智能电网中的分布式拒绝服务攻击综述

于信芳[1] 张添夫[1] 于 航[1] 毛伯星[1] 孙成烨[1]
YU Xinfang ZHANG Tianfu YU Hang MAO Boxing SUN Chengye

摘 要 智能电网系统由于其复杂的架构和多样化的设备，面临着严重的安全威胁，尤其是分布式拒绝服务（DDoS）攻击。该研究旨在回顾和分析针对威胁先进计量基础设施（AMI）可用性的 DDoS 攻击的仿真、检测和缓解技术。采用了最新的仿真方法、检测机制和防护策略，通过实验与技术评估，研究了多种缓解方案的有效性。结果表明，综合运用流量监控、异常检测及防御技术，可以显著提高智能电网对 DDoS 攻击的防护能力。针对 AMI 系统的 DDoS 攻击防护仍需不断优化技术手段，分析技术有助于智能电网系统免受 DDoS 攻击，以保障电力系统的稳定性与可靠性。

关键词 分布式拒绝服务攻击；智能电网；网络安全；物联网

doi：10.3969/j.issn.1672-9528.2024.12.043

0 引言

智能电网（SG）是一种综合了物联网（IoT）技术的电力系统，它结合了信息与通信技术（ICT），涵盖了能源生产、传输、变电、配电和消费的双向智能网络。这种系统的设计旨在实现可持续性、安全性、可靠性、韧性和经济效益 [1-5]。

从 2017 年到 2023 年，智能电网的全球价值增加一倍多。智能电网的一个关键模块是双向电力流与通信和控制的集成 [6-7]。智能电网使用智能双向设备，如智能电表、传感器和致动器，覆盖从电力生产到消费的整个过程 [8]。该系统采用监控和数据采集（SCADA）架构，以高精度和细粒度实时控制，使每个设备的稳定性 [9]。作为关键基础设施，智能电网对攻击者具有很大吸引力，因为监控和控制是通过互联网协议与消费者操作进行的 [10]。

即使在智能电网兴起之前，电网也容易发生故障，在破坏平衡的同时会导致一连串故障。2015 年 12 月，因受电网攻击，导致某国长时间断电，造成巨大的经济损失 [11]。因物联网和互联电网系统的兴起增加了攻击点，使攻击者更容易对它们进行有针对性的攻击，从而加剧了这一全球性问题。2016 年，Mirai 僵尸网络攻击表明了物联网设备的巨大负面可能性 [12]。剑桥大学在近期研究中描述了对美国电网灾难性但可行的网络攻击，这可能会切断 100 万人的电力并造成 1 万亿美元的经济损失 [13]。

将过去的电网适当转换为未来的智能电网需要实现保密性、完整性和可用性（CIA 三要素）等安全目标。因此，有必要检查智能电网基础设施中的现有漏洞和潜在威胁 [14]。

1. 中国科学院沈阳计算所新技术开发有限公司 辽宁沈阳 110168

在众多智能电网威胁中，分布式拒绝服务（DDoS）是针对 CIA 三要素可用性的主要攻击。当攻击者试图使其目标用户无法访问系统或网络基础设施时，就会发生这种情况。根据 2019 年第 14 届全球基础设施安全年度报告显示，分布式拒绝服务（DDoS）攻击占服务提供商面临的实际危险的 95%。根据 NIST 的智能电网网络安全指南 [15]，可用性被视为智能电网的关键安全目标。

CIA 三要素的可用性传统上被描述为“确保及时准确的信息访问和使用”。然而，从智能电网的角度来考虑也应包含“保证充足的电力供应”。关于这一点，Huseinovic 等人 [16] 扩大了智能电网对 DDoS 攻击的描述，包括以下提到的维度。

（1）拒绝服务针对资源与电力的获取能力进行攻击。

（2）拒绝保密针对数据完整性与数据操纵进行攻击。

（3）拒绝授权针对设备间通信进行攻击。

因此，研究智能电网系统以上描述问题至关重要。

1 智能电网概念模型

智能电网的基础设施是广泛的，包括一些分布式能源（DER）、智能电子设备（IED）、电器和设施。通过实现有效的操作、维护以及优化资产利用率，降低了功耗和投资费用。智能电网是一个电力市场，客户可以在其中产生、存储和转移负载。由于智能电网应用需要实时监控和通信，因此必须具有一致的数据流。智能电网通信框架是实时和双向的，客户将获得同步数据流 [17]。智能电网系统可以通过利用自动控制设备、及时检测和增强的传感器系统来自愈故障。智能电网系统通过自动控制设备、实时检测和先进传感器来实现故障自愈。它为各种应用带来了新的商品、服务和市场。面向消费者的智能电子设备（IED）可以由授权服务提供商

或用户远程管理电力使用，保持发电与消费的平衡。同时，智能电网建设还需确保安全、可靠、实时和低延迟的通信，以有效应对网络攻击、中断和物理损害 [18-19]。

2 智能电网 DDoS 攻击技术

DDoS 攻采用 7 种不同的策略来危害智能电网中的设备或应用。干扰是用于减缓或限制物理层信息或功率的 DDoS 攻击之一。洪泛是指以不受限制的方式分配流量，以使网络过载并消耗一定程度的内存、电池或电源资源 [20]。另一种 DDoS 攻击形式是加密 DDoS 攻击，这种攻击利用了消息认证码（MAC），虽然这些 MAC 的设计目的是为了保护数据的安全 [21]。篡改数据可能被用作 DDoS 攻击的切入点。

去同步攻击是另一种类型的 DDoS 攻击，在保护先进计量基础设施（AMI）连接的 TLS 握手中断控制数据包 [22]。一些 DDoS 攻击，如虫洞、黑洞和女巫攻击，是值得注意的基于路由的攻击，与智能电网领域直接相关 [23]。反射式攻击向一系列服务器发出伪造请求，这些服务器将响应发送到伪造地址 [24-25]。

在传统的拒绝服务（DoS）攻击中，洪泛数据包来自单一受感染的主机。而在分布式拒绝服务（DDoS）攻击中，这些数据包则来源于多个被攻击者控制的主机（僵尸），对智能电网系统造成严重破坏。智能电表中的安全漏洞可能被中间人（MitM）攻击利用，注入恶意数据，导致各种攻击，这在家域网（HAN）中尤其脆弱。智能电网中 DDoS 攻击如图 1 所示。由于智能电网依赖双向数据传输与转发，DDoS 攻击成为了有效的网络攻击工具和潜在威胁。

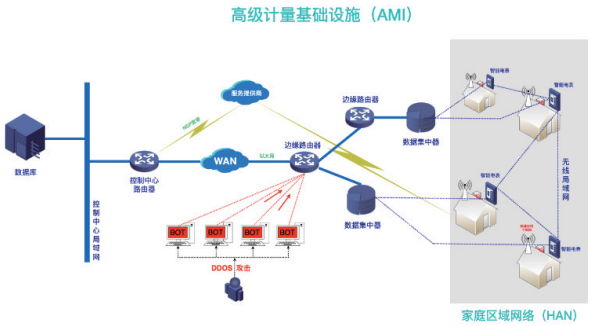

图 1 智能电网中的 DDoS 攻击示意图

3 智能电网漏洞与影响

智能电网采用多级数据收集和监控设备，如智能仪表、智能应用、可编程逻辑控制器（PLC）、相量测量单元（PMU）、数据聚合器和远程终端单元（RTU）。数据集中器（DC）负责收集信息。然后，数据通过在中间的数据中心发送到中央数据中心。这些数据收集系统与互联网的设计基本相同，存在大量漏洞，并且曾被具有欺骗性和产生灾难性后果的 DDoS 攻击利用过。

表 1 列出了智能电网漏洞和 DDoS 攻击影响的 3 个不同角度的表格分类。

表 1 智能电网漏洞与后果

视角	安全漏洞	结果	受影响的设备或通信协议
维度	电动汽车汽车网络通信系统设计中的安全漏洞 [26]	车辆停用作为攻击中的一部分	电动汽车
	PMU 和 PDC 中信息通信的安全漏洞 [27]	通讯与发电中拒绝访问 PMU 或 PDU 的测量数据	PMU 和 PDU
通信协议	SV 和 GOOSE（IEC 61850）等变电站自动化系统协议中的安全漏洞，包括 IED[28]	访问间隔层上的设备，如 PMU 和 IED	PMU 和 IED/ IEC 61850
	ANSI C12.22 继承了影响 IP 网络的相同安全漏洞，这些漏洞包括跟踪服务、解析服务和紧急流量 [29]	智能电表不可用，获取电表通道	智能电表和 ANSI C12.22
	IEEE C37.118 协议不支持任何认证方法，如 SSL 或 IPSEC 功能，以确保 PMU 和 PDC 的保密性 [30]	系统可见性丧失，中断反馈控制环路并停止同步向量测量传递，PMU 与 PDU 无响应	IEEEC37.118，PMU 和 PDC
	攻击者利用 DNP3 协议中的漏洞 [31]	失陷伪造数据聚合器产生自发响应洪泛，中继无响应	DNP3 和数据聚合器
	SCADA 中 RTU 通信系统的安全漏洞 [32]	定位到处理环境中的失陷 RTU	RTU 和 SCADA
层面	RTU 到控制中心的物理层通信信道存在漏洞 [33]	通信干扰产生丢包和控制中心无法访问	RTU 和控制中心
	MAC（媒体访问控制）层 ARP（地址解析协议）容易受到希望通过执行 ARP 欺骗攻击来修改参数的攻击者的攻击 [34]	ARP 欺骗导致 DDoS 攻击，阻断数据集中器和智能表间的信息	智能电表和数据集中器
	欺骗数据包 IP 地址的能力是 DDoS 在网络层攻击和发送过载 DNP 数据包时利用的核心漏洞 [35]	IP 欺骗中断变电站控制中心	变电站 IED 设备
	传输层使用 IEC-104 协议的 SCADA 系统中的安全漏洞被缓冲区溢出利用 [36]	中断源与目的的通信	IEC-104

智能电网容易受到与互联网基本协议相同的攻击媒介、漏洞攻击，从而产生不利影响。因此，准确检测安全风险和漏洞可以确定适当的对策。干扰攻击只能通过利用 RTU 到控制中心的物理层通信信道中的漏洞来进行。此外，安全性主要是智能电网领域中的保护层。在许多电力公司中，PMU 电路不被视为重要的网络基础设施 [37]。尽管损害单个设备可能会导致一系列事件，导致电力服务中断 [38]。

4 缓解针对智能能源系统的 DDoS 攻击的已知框架

攻击者可以通过多种方式有效地破坏智能电网的服务或其中一部分。但没有一种通用的方法来防御所有类型的 DDoS 攻击。可用的 DDoS 对策集中在预防、检测或响应上。最好的防御形式是预防，但预防并不总是可行的。下面从 3 个方面讨论了现有潜在的智能电网 DDoS 攻击解决方案。

4.1 基于认证的解决方案

可用性和完整性是传统网络安全方法中的两个不同目标。当涉及到网络物理系统时，攻击者可能会通过插入错误的数据和指令间接中断服务，密码学是检测和拒绝第三方插入的恶意通信的强大工具 [39]。传统的加密模型，如高级加密标准（AES）、Rivest-Shamir 和 Adleman（RSA）以及数据加密标准（DES），在具有高处理能力和内存的系统上运行，但它们在计算能力有限的嵌入式设备和传感器系统上运行不佳。轻量级密码模型旨在解决与传统加密相关困难。基于智能电网的物联网轻量级密码学算法列表如图 2 所示。

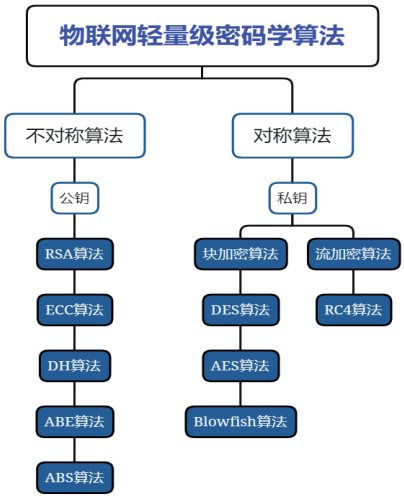

图 2 物联网轻量级密码学算法

如文献所述，大约 18% 的 AES、42% 的椭圆曲线密码学（ECC）和 17% 的基于属性的加密（ABE）算法是广泛使用的方法 [40]。由于所需的计算能力、能源和内存等资源较少，ECC 最适合需要轻量级加密的系统。ECC 使用 160 位的安全级别与 RSA 的 1024 位安全级别相似。ECC 是一种非对称密码学算法，可用于在受限设备中实现高度保护。与使用中的其他非对称算法相比，ECC 需要更少的密钥并可确保更高的安全性。

在理想情况下，如果终端没有损坏，并且所有通信参与者及其数据包都经过加密验证，则可以避免部分 DDoS 攻击。基于多项式的轻量级验证技术和公钥基础设施（PKI）被用作广域安全系统中密钥管理、签名和证书验证的可行选择。尽管它在满足可用性、隐私和可扩展性标准方面存在一些挑战。另一方面，认证机构（CA）等第三方提供商将参与颁发数字证书，对系统构成隐私威胁 [41]。在计划中的智能电网中，大量智能计算设备需要相互验证。因此，在大量实体中应用 PKI 存在一些可扩展性问题 [42]。

Abood 等人 [43] 解决了会话密钥和通信密钥上的额外漏洞问题，研究人员创建了一种独特的密钥管理解决方案，该方案结合了 ECC 公钥技术和基于 Needham-Schroeder 认证协议的对称密钥方法，通过构建链接的信任流来克服前面提到的可扩展性问题。单个单词的算法加密时间比较如图 3 所示。

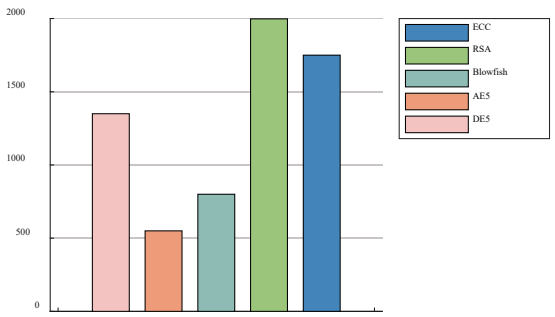

图 3 轻量级密码学算法加密时间

根据研究结果，AES、Blowfish 和 DES 等算法在加密速度方面与 ECC 具有竞争力。然而，这些算法不符合表 II 所示的安全标准。表 2 展示的是如果黑客每秒生成一百万个密钥，破解算法所需的时间。

表 2 破解算法来获得单个单词所需时间

算法	密钥长度 /bit	破解算法所需时间 /s
DES	64	1.054 18e+18
RSA	1024	681 427 599
Blowfish	32 448	22 597.2
AES	128 192 256	6.336 4e+37
ECC	160	7.458 9e+40

结果表明，ECC 算法是结合 Needham-Schroeder 认证协议的最安全的算法，必须使用 PKI 作为密钥管理和证书验证的最佳选择。未来的研究应侧重于将各种非对称算法与 PKI 相结合的实际实现，以增加密码学的复杂性，这是防止智能电网资源入侵的一种很好方法。

4.2 基于陷阱的解决方案

蜜罐是一种基于陷阱的安全机制，它模拟攻击并吸引攻击者攻入。攻击者可以利用有意被攻陷的计算机系统中的漏洞，帮助其了解攻击者的行为模式。例如，Stuxnet 攻击突显了网络安全的必要性，并使 PLC 等控制系统组件的问题引起了安全界的注意。Crysys PLC 蜜罐（CryPLH）技术旨在区分针对工业控制系统的 PLC 攻击 [44]。Honeyd 是最早的开源有限交互蜜罐项目之一，能够模拟各种 TCP/IP 服务。HoneydV6 也是一个低交互蜜罐，它经过改进，可以处理与 Honeyd 相同的 IPv6[45]。Conpot[46] 是一个低交互蜜网项目，是一个专注于 ICS 设备建模的工业蜜罐。ShaPe[47] 是一个低交互率的模拟变电站自动化系统的蜜罐。

CockpitCI[48] 项目使用 Modbus 创建了一个可供入侵者访问并由安全适配器控制的高交互蜜罐。中间交换机通过将所有 PLC 流量直接镜像到实现事件监视程序模块的安全适配器来执行监视。Wang 等人 [49] 在使用 OPNET 工具模拟的高级计量基础设施中引入了蜜罐来对拓扑进行建模，并通过蜜罐博弈实现了攻击者和防御者之间的几个贝叶斯纳什均衡。根据模拟数据，博弈方法降低了能耗，将检测率提高了 85%，远高于其他监控模型，但它缺乏对许多重要协议的支持。

Conpot 蜜罐能够支持许多智能电网用例，因为它支持许多流行的工业协议，如表 3 所示。它是一个开源项目，研究界可以为开发其他模板做出贡献。然而，模拟真实世界的智能电网行为是困难的，这限制了智能电网蜜罐安装的优点。未来，有必要将蜜罐置于工业物联网基础设施和智能电网网络的网际互连协议（IP）范围内，以获取真实的情报数据。

表 3 智能电网蜜罐模型

智能电网蜜罐模型	交互层级	模拟的服务	模拟的设备
Honeyd	低	FTP、SMTP、Telnet、IIS、POP	不适用
HoneydV6	低	FTP、SMTP、Telnet、IIS、POP	不适用
CryPLH	高	HTTP(S)、SNMP	PLC
SHaPe	低	IEC 61850、HTTP、FTP	变电站
CockpitCI	高	FTP、SNMP、Modbus	PLC
Honeygame	高	FTP、SNMP、Modbus	AMI
Conpot	低	IEC 60870-5-104、BACnet、FTP Ethernet/IP、Modbus、HTTP S7comm、SNMP、TFTP、IPMI	RTU 设备

4.3 基于入侵检测与防御的解决方案

入侵检测系统是检查整个数据包（包括报头和内容）的设备或应用程序，并在检测到可疑网络事件时发送警报。当与自动响应和对策结合使用时，这些系统可以被视为一种入侵防御系统，通过实时识别和防止潜在的安全漏洞来改进加密操作。

一般来说，有 3 种类型的入侵检测技术：基于特征的、基于异常的和基于行为的。基于特征的检测将计算机系统中发生的活动与一组指定的渗透模式（称为特征）进行比较。如果其中一个特征与操作的规范匹配，则发出匹配的警报。它的弱点是无法检测到没有特征的攻击。基于异常的技术将异常行为识别为入侵。经常在各种数据集中使用统计分析过程、神经网络、马尔可夫模型、贝叶斯网络和分类算法等机器学习技术来检测有害行为。与基于特征的方法相比，这种检测准确率较低。然而，它有检测以前未发现的网络威胁的好处。基于行为的方法采用一组既定的规则来描述系统的通常行为。规范是用于描述这些规定的术语。它可以识别可能的异常，以及检测未知的攻击。

表 4 分析了每种检测方法，突出了它们最重要的特征，如曲线下面积（AUC）、准确率、误报率（FPR）和实报率（TPR）。根据它们的监测目标、检测策略和效率，对入侵检测与防御系统进行了比较。目标系统可以是以下任何一个：一是完整的智能电网环境，二是 AMI，三是 SCADA 网络，四是变电站，五是同步相量。基于特征的方法通常会提供良好的结果。因此，为预料之外的威胁创建攻击特征是一个繁琐的过程。另一方面，基于异常的方法可以识别 0day 攻击，但误报率更高。

最后，基于行为的入侵检测与防御系统结合了前两种方法的优点，但在智能电网这样的环境中，频繁更改和更新是常见的，这些规则必须定期修订。入侵检测与防御系统都没有分析检测延迟和资源利用率。由于智能电网中使用了各种通信协议，无法监测和分析来自多个来源的数据。检测技术的结合可以解决上述问题，因此，不断发展的混合入侵检测与防御系统的解决方案更有前景。综上所述，建议智能电网的理想入侵检测与防御系统使用混合方法，包括特征和规范规则以及异常检测过程。

5 结语

智能电网系统正成为分布式拒绝服务（DDoS）攻击的主要目标，这种攻击不仅带来严重的安全威胁，还可能导致国家经济损失。网络安全技术是检测和防范这些攻击的关键，但智能电网面临许多挑战，尤其是在入侵检测和防御系统方面。加密数据包的检测是一个难点，这一领域仍在积极研究中。由于准确特征的开发困难，混合检测技术被提出作为解决方案。然而，许多智能电网的检测机制没有考虑检测延迟

表 4 入侵检测与防御系统在智能电网环境中检测 DDoS 的总结

文献编号	目标单元	检测方法	表现	数据集	模拟工具
[50]	完整的智能电网	基于异常	AUC=0.994 51	KDD CUP 1999	Protégé
[51]	完整的智能电网	基于异常	ACC=99.7%	NSL-KDD	MatLab
[52]	AMI	基于异常	ACC=94.67%，FPR=3.31%	KDD CUP 1999	MOA
[53]	AMI	基于异常	ACC>90%，TPR=89.2，TNR=93.4	ADFA-LD	MatLab
[54]	AMI	基于异常	准确率 =99.70% TPR=99.60%	ISCX2012	WEKA
[55]	SCADA	基于异常	准确率 =90%，TPR=0.846，AUC=0.905	IEC-104 数据集	WEKA
[56]	SCADA	基于异常	TPR=95.12	蜜罐获取的数据	Python
[57]	SCADA	基于异常	ACC=97.387 9%	模拟数据	Wireshark、WEKA
[58]	SCADA	基于特征	不适用	不需要	Snort
[59]	AMI	基于行为	理论分析	不需要	MatLab
[60]	变电站	基于行为	FPR=0%，TPR=98.9%，准确率 =100%	变电站中的真实数据	Wireshark
[61]	变电站	基于行为	FPR=1.61×10^{-4}	不需要	Wireshark、NMap
[62]	同步向量	基于行为	FPR = 0%	不需要	Nmap、hping

或时间敏感操作的需求。此外，加密保护下的公钥管理的可扩展性也未得到充分重视。为了确保长期安全，需要开发能够升级和修改的智能电网协议。蜜罐技术在现实世界中难以模仿，因此部署受到限制。机器学习和深度学习技术在检测和防御方面展现出潜力，但许多文献中的解决方案未能解决智能电网系统中的物理设备问题。考虑到 DDoS 攻击可能对物理设备造成严重损害，建议基于模拟结果的解决方案在实际环境中进行验证，并结合硬件和家庭能源系统中的电器负载，未来可计划实施基于物理参数的入侵检测方案。

参考文献：

[1] 鞠平，周孝信，陈维江，等．“智能电网 +”研究综述 [J]. 电力自动化设备 ,2018,38(5): 2-11.

[2] 岳芳，王雪珍，姜山．智能电网的网络安全风险及应对策略 [J]. 科技导报 , 2024, 42(9): 6-16.

[3]BHALAJI N. Cluster formation using fuzzy logic in wireless sensor networks[EB/OL].(2021-03-09)[2024-09-01].https://www.semanticscholar.org/paper/Cluster-Formation-using-Fuzzy-Logic-in-Wireless-Bhalaji/e6c39801f730e5132ed05f319e7e74d83aa2f803.

[4]MUGUNTHAN S R. Wireless rechargeable sensor network fault modeling and stability analysis[J].Journal of soft computing paradigm, 2021, 3(1): 47- 54.

[5]MCDANIEL P, MCLAUGHLIN S. Security and privacy challenges in the smart grid[J] .IEEE security & privacy, 2009, 7(3): 75–77.

[6] 祝恩国，窦健．用电信息采集系统双向互动功能设计及关键技术 [J]. 电力系统自动化 , 2015(17): 62-67.

[7]KOTUT L, WAHSHEH L A. Survey of cyber security challenges and solut ions in smart grids[C/OL]//2016 Cybersecurity Symposium (CYBERSEC). Piscataway:IEEE, 2016[2024-04-12].https://ieeexplore.ieee.org/abstract/document/7942422.

[8]AHMED S, GONDAL T M, ADIL M, et al.A survey on communication technologies in smart grid[C/OL]//2019 IEEE PES GTD Grand International Conference and Exposition Asia(GTD Asia). Piscataway: IEEE,2019[2024-02-19].https://ieeexplore.ieee.org/abstract/document/8715993.

[9] 应杰耀．基于物联网技术的智能电网数据安全问题研究进展 [J]. 电子科技 ,2023,36(3): 76-80.

[10]LIANG G Q, WELLER S R, ZHAO J H,et al. The 2015 ukraine blackout: Implications for false dat a inject ion at t acks[J]. IEEE transactions on power systems, 2016, 32(4): 3317-3318.

[11] 赵俊华，梁高琪，文福拴，等．乌克兰事件的启示：防范针对电网的虚假数据注入攻击 [J]. 电力系统自动化 , 2016(7): 149-151.

[12]HOSSAIN E, HAN Z, POOR H. Smart grid communication networks [EB/OL].(2021-01-19)[2024-08-11].https://www.cambridge.org/us/universitypress/subjects/engineering/wireless-communications/smart-grid-communications-and-networking.

[13]NETSCOUT SYSTEMS INC. NETSCOUT releases 14th annual worldwide infrastructure security report[EB/OL]. (2019-03-20)[2024-07-23].https://www.netscout.com/press-releases/netscout-releases-14th-annual-worldwide-infrastructure.

[14] 白开峰，赵宏斌，张芸，等 . 电网异常业务数据检测方法综述 [J]. 计算机与现代化 , 2023(3): 79-83+89.

[15]HUSEINOVIĆ A, MRDOVIĆ SAŠA, BICAKCI K, et al. A survey of denial-of-service attacks and solutions in the smart grid[J]. IEEE access , 2020,8:177447-177470.

[16]DELGADO-GOMES V, MARTINS J F,LIMA C,et al. Smart grid security issues[C/OL] //2015 9th International Conference on Compatibility and Power Electronics (CPE).Pi scataway:IEEE,2015[2024-08-10].https://ieeexplore.ieee.org/document/7231132.

[17]B RAWAT D,BAJRACHARYA C.Cyber security for smart grid systems: Status, challenges and perspectives [C/OL] South east Con 2015. Piscataway:IEEE,2015[2024-02-19]. https://ieeexplore.ieee.org/abstract/document/7132891.

[18] 王明俊 . 智能电网与智能能源网 [J]. 电网技术 , 2010, 34(10): 1-5.

[19] 余贻鑫 , 栾文鹏 . 智能电网述评 [J]. 中国电机工程学报 , 2009, 29(34): 1-8.

[20] 王印玺 , 黄华雪 . DDoS 攻击的发展与防御综述 [J]. 现代计算机 , 2021(2): 51-56.

[21] 张永铮 , 肖军 , 云晓春 , 等 . DDoS 攻击检测和控制方法 [J]. 软件学报 , 2012,23(8): 2058-2072.

[22]ALMAS M S, VANFRETTI L, SINGH R S, et al.Vulnerability of synchrophasor-based WAMPAC applications' to time synchronization spoofing[J]. IEEE transactions on smart grid, 2017, 9(5): 4601-4602.

[23]WANG X D, YI P. Security framework for wireless communications in smart distribution grid[J] .IEEE transactions on smart grid, 2011,2(4):809-818.

[24]GROCHOCKI D, HUH J H, BERTHIER R, et al.AMI threats, intrusion detection requirement s and deployment recommendations [C/OL]// 2012 IEEE Third International Conference on Smart Grid Communications (Smart Grid Comm). Piscataway:IEEE,2012[2024-04-16].https://ieeexplore.ieee.org/document/6486016.

[25]MENG W X, MA R, CHEN H H. Smart grid neighborhood area networks: a survey[J]. IEEE network, 2014,28(1):24-32.

[26]AHMED S, DOW F M. Elect ricvehicle technology as an exploit for cyber-attacks on t he next generation of electric power systems [C/OL]//2016 4th International Conference on Control Engineering & Information Technology (CEIT). Piscataway: IEEE, 2016[2024-05-10].https://ieeexplore.ieee.org/abstract/document/7929019.

[27]ISLAM S N, BAIG Z, ZEADALLY S.Physical layer security for the smart grid: vulnerabilities, threats, and count ermeasures[J].IEEE transactions on industrial informatics, 2019, 15(12):6522-6530.

[28]HONG J H, LIU Q C,GOVINDARASU M. Detect ion of cyber intrusions using network-based multicast messages for substation automat ion[C/OL]//ISGT 2014. Piscataway: IEEE, 2014[2024-07-11].https://ieeexplore.ieee.org/document/6816375.

[29]RANA S, ZHU H Y, LEE C W, et al. The not-so-smart grid: preliminary work on identifying vulnerabilities in ANSI C12.22[C]//2012 IEEE Globecom Workshops. Piscataway: IEEE, 2012:1514-1519.

[30]MORRIS T H, PAN S Y,ADHIKARI U.Cyber security recommendations for wide area monitoring, protect ion, and control systems[C/OL]//2012 IEEE Power and Energy Society General Meeting.Piscataway:IEEE, 2012[2024-07-14]. https://ieeexplore.ieee.org/document/6345127.

[31]JIN D, NICOL D M, YAN G H. An event buffer flooding attack in DNP3 controlled SCADA systems[C/OL]// Proceedings of the 2011 Winter Simulation Conference (WSC). Piscataway:IEEE, 2011[2024-03-28]. https://ieeexplore.ieee.org/document/6147969.

[32]GOGIC D, JELACIC B, LENDAK I. Simulation-based evaluation of DDoS against smart grid SCADAs[C]// Computer Security. Cham, Switzerland: Springer, 2020:86-97.

[33]PROANO A, LAZOS L. Selective jamming at tacks in wireless networks [C/OL]//2010 IEEE International Conference on Communications. Piscataway: IEEE, 2010[2024-06-11].https://ieeexplore.ieee.org/abstract/document/5502322.

[34]PREMARATNE U K, SAMARABANDU J, SIDHU T S, et al. An intrusion detection system for IEC 61850 automated substations[J]. IEEE transactions on power delivery ,2010,25 (4): 2376-2383.

[35]KNAPP E D, SAMAMI R. Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure[EB/OL].(2013-02-26)[2024-04-16]. https://www.semanticscholar.org/paper/Applied-Cyber-Security-and-the-Smart-Grid%3A-Security-Knapp-Samani/576a314fa555732f136a9eb47bea712c5d440561#:~:text=The%20purpose%20of%20this%20review%20paper%20is%20

to,ecosystem%20and%20potential%20cybersecurity%20solutions%20to%20smart%20gr.

[36]WANG W Y, XU Y, KHANNA M. A survey on the communication architectures in smart grid[J] .Computer networks, 2011, 55 (15): 3604 -3629.

[37]MOUSSA B, DEBBABI M, ASSI C. A detection and mitigat ion model for PTP delay at tack in an IEC 61850 substation[J]. IEEE transactions on smart grid, 2016, 9(5): 3954-3965.

[38]RISBUD P, GATSIS N, TAHA A. Vulnerability analysis of smart grids to GPS spoofing[J].IEEE transactions on smart grid, 2018, 10(4): 3545-3548.

[39] MOUSAVI S K, GHAFFARI A, BESHARAT S. Security of internet of things based on cryptographic algorithms: a survey [J]. Wireless networks ,2021,27(1):1515-1555.

[40]HE D J, CHEN W, ZHANG Y, et al. An enhanced public key infrastructure to secure smart grid wireless communication networks[J]. IEEE network, 2014, 28(1):10-16.

[41] SMITH S W. Cryptographic scalability challenges in the smart grid[C]//2012 IEEE PES Innovative Smart Grid Technologies(ISGT). Piscataway:IEEE, 2012:1-3.

[42]WU D P, ZHOU C. Fault-tolerant and scalable key management for smart grid [J].IEEE transactions on smart grid, 2011, 2(2):375-381.

[43]ABOOD O G, ELSADD M A, GUIRGUIS S K. Investigation of cryptography algorithms used for security and privacy protection in smart grid infrastructures[C/OL]//2017 Nineteenth International Middle East Power Systems Conference (MEPCON). Piscataway: IEEE, 2017[2024-07-12].https://ieeexplore.ieee.org/abstract/document/8301249.

[44]BUZA D I, JUHÁSZ F, MIRU G, et al. CryPLH: protecting smart energy systems from targeted attacks with a PLC honeypot[J].Smart grid secur, 2014, 8814(1): 181–192.

[45]SCHINDLER S, SCHNOR B, KIERTSCHER S, et al. HoneydV6: a low-interaction IPv6 honeypot[C/OL]//2013 International Conference on Security and Cryptography (SECRYPT).Piscataway:IEEE, 2015[2024-01-10].https://ieeexplore.ieee.org/document/7223158.

[46]PLIATSIOS D, SARIGIANNIDIS P, LIATIFIS T,et al.A novel and interactive industrial control system honeypot for critical smart grid infrastructure [C/OL]// 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD).Piscataway:IEEE,2019[2024-06-26].https://ieeexplore.ieee.org/document/8858431.

[47]KOLTYS K, GAJEWSKI R R. Shape: a honeypot for electric power ′substation[EB/OL]. (2015-12-30)[2024-05-16].https://www.semanticscholar.org/paper/SHaPe%3A-A-Honeypot-for-Electric-Power-Substation-Koltys-Gajewski/ace0f0c1271874feffded6a6230965aeb6af0331.

[48]SIMÕES P, CRUZ T, PROENÇA J, et al. Specialized honeypots for SCADA systems[J]. Cyber security: analytics, technology and automation, 2015,78(1):251-269.

[49]WANG K, DU M, SUN Y F, et al. Strategic honeypot game model for distributed denial of service attacks in the smart grid[J].IEEE transactions on smart grid, 2017,8(5):2474-2482.

[50]ZHANG Y C, WANG L F, SUN W Q, et al. Artificial immune system based intrusion detection in a distributed hierarchical network architecture of smart grid [C/OL]// 2011 IEEE Power and Energy Society General Meeting.Piscataway:IEEE,2011[2024-04-27].https://ieeexplore.ieee.org/abstract/document/6039697.

[51]FAISAL M A, AUNG Z, WILLIAMS J R, et al.Data-stream based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study [J].IEEE systems journal, 2014,9(1):31-44.

[52] VIJAYANAND R, DEVARAJ D, KANNAPIRAN B. Support vector machine based intrusion detection system with reduced input features for AMI of smart grid[C/OL]//2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS).Piscataway: IEEE, 2017[2024-06-26].https://ieeexplore.ieee.org/document/8014590.

[53] PETR M. Description and analysis of IEC 104 protocol[R/OL].(2017-12-07)[2024-01-19].https://www.fit.vut.cz/research/publication/11570/.en.

[54]WANG P H, LIAO Y H, GAO G F, et al.An intrusion detection method based on log sequence clustering of honeypot for modbus TCP protocol [C/OL] //2018 IEEE International Conference on Applied System Invention (ICASI). Piscataway: IEEE, 2018[2024-05-25].https://ieeexplore.ieee.org/document/8394581.

[55]LI Z C, HUANG Y N, DAI B C, et al.Using data mining methods to detect simulated intrusions on a modbus network [C/OL]//2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2).Piscataway: IEEE, 2017[2024-03-11].https://ieeexplore.ieee.org/document/8315369.

[56]LI H, LIU G J, JIANG W W, et al. Designing snort rules to detect abnormal DNP3 network data[C/OL]//2015 International Conference on Control, Automation

and Information Sciences (ICCAIS). Piscataway: IEEE, 2015[2024-01-19].https://ieeexplore.ieee.org/document/7338690.

[57]JOKAR P, LEUNG V C M. Intrusion detection and prevention for ZigBee-based home area networks in smart grids [J]. IEEE transactions on smart grid, 2016,9(3):1800-1811.

[58] KWON Y J, KIM H Y, LIM Y H, et al. A behavior-based intrusion detection technique for smart grid infrastructure[C/OL]//2015 IEEE Eindhoven PowerTech.Piscataway: IEEE, 2015[2024-07-01].https://ieeexplore.ieee.org/document/7232339.

[59]HONG J H, LIU C Q, GOVINDARASU M. Detection of cyber intrusions using network-based multicast messages for substation automation [C/OL]// ISGT 2014.Piscataway: IEEE, 2014[2024-02-12].https://ieeexplore.ieee.org/document/6816375.

[60]YANG Y, GAO L, YUAN Y B, et al.Intrusion detection system for IEC 61850 based smart substations [C/OL]//2016 IEEE Power and Energy Society General Meeting (PESGM). Piscataway: IEEE, 2016[2024-03-27].https://ieeexplore.ieee.org/document/7741668.

[61]YANG Y, MCLAUGHLIN K, SEZER S, et al. Intrusion detection system for network security in synchrophasor systems [C/OL]//IET International Conference on Information and Communications Technologies (IETICT 2013). London: IET, 2013[2024-06-10].https://ieeexplore.ieee.org/document/6617502.

[62]HONG J H, LIU C Q, GOVINDARASU M. Detection of cyber intrusionsusing network-based multicast messages for substation automation[C/OL]// ISGT 2014.Piscataway: IEEE, 2014[2024-04-19].https://ieeexplore.ieee.org/document/6816375.

【作者简介】

于信芳（1984—），男，辽宁辽阳人，本科，研究方向：网络信息安全、电力系统。

（收稿日期：2024-09-10）

（上接第 188 页）

[4] PENG Y X, QI J W, YUAN Y X. CM-GANs: Cross-modal generative adversarial networks for common representation learning[J]. ACM transactions on multimedia computing, communications, and applications (TOMM), 2019, 15(1): 1-24.

[5] LI C L, LI X, WANG X P, et al. FG-AGR: Fine-grained associative graph representation for facial expression recognition in the wild[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2023,34(2):882-896.

[6] YOU Q, LUO J, JIN H, et al. Joint visual-textual sentiment analysis with deep neural networks[C]//Proceedings of the 23rd ACM international conference on Multimedia. New York: ACM, 2015: 1071-1074.

[7]CHEN M H, WANG S, LIANG P P, et al. Multimodal sentiment analysis with word-level fusion and reinforcement learning[C]// Proceedings of the 19th ACM International Conference on Multimodal Interaction. New York: JMLR.org, 2017: 163-171.

[8] DAI W L, LIU Z H, YU T Z, et al. Modality-transferable emotion embeddings for low-resource multimodal emotion recognition[DB/OL].(2020-10-7)[2024-02-11].https://doi.org/10.48550/arXiv.2009.09629.

[9] HU G M, ZHAO Y, LU G M,et al. Unimse: Towards unified multimodal sentiment analysis and emotion recognition[DB/OL]. (2022-11-21)[2023-12-06].https://doi.org/10.48550/arXiv.2211.11256.

[10] LL J N, LI D X, XIONG C M, et al. Blip: Bootstrapping language-image pre-training for unified vision-language understanding and generation[DB/OL].(2022-02-15)[2024-03-16].https://doi.org/10.48550/arXiv.2201.12086.

[11] LIU S T, ZHANG X, YANG J F. SER30K: A large-scale dataset for sticker emotion recognition[EB/OL].(2022-10-10)[2024-01-13].https://www.semanticscholar.org/paper/SER30K%3A-A-Large-Scale-Dataset-for-Sticker-Emotion-Liu-Zhang/1d2baaf2489328baba2c4db93d44257059ded3d7.

[12] KHAN Z, FU Y. Exploiting BERT for multimodal target sentiment classification through input space translation[DB/OL].(2021-08-05)[2023-08-16].https://doi.org/10.48550/arXiv.2108.01682.

【作者简介】

李伟（1999—），男，湖北襄阳人，硕士研究生，研究方向：多模态情感分析。

王东娟（1977—），女，陕西咸阳人，博士，副教授、硕士生导师，研究方向：信息管理与电子商务、大数据应用等。

（收稿日期：2024-09-13）