DOI:10.12158/j.2096-3203.2021.05.007

基于区块链的配电物联网数据安全防护方法

王海，曾飞，杨雄
（国网江苏省电力有限公司电力科学研究院，江苏 南京 211103）

摘 要：针对配电物联网中海量数据易受网络攻击的问题，提出一种基于区块链的配电物联网数据安全防护方法。首先，构建一种协作式安全防护架构，通过自适应流量监测设计异常流量识别机制。其次，采用改进实用拜占庭共识（PBFT）算法建立信任机制，实现配电云主站与每个配电边缘代理装置攻击检测模型共享。然后，基于区块链智能合约实现攻击检测模型动态更新，采用深度强化学习训练各攻击检测模型并进行融合，得到攻击检测融合模型。最后，基于 Mininet 搭建仿真平台并对所提方法进行实验论证，结果表明，所提攻击检测模型综合性能优于集中式和分布式模型。

关键词：区块链；配电物联网；数据安全防护；实用拜占庭共识（PBFT）；深度强化学习；攻击检测
中图分类号：TM769 **文献标志码**：A **文章编号**：2096-3203（2021）05-0047-07

0 引言

随着信息和通信技术的发展以及传感器技术的普及，物联网已广泛应用于医疗、智慧城市和智能电网等各个领域，可实现高效状态感知与资源管理[1]。近年来，随着配电物联网建设的推进，新型智能配电网的结构和功能明显优化，除具备基本电能传输和分配功能外，还兼具全景状态采集、数据分布式存储转发与分析管理、电能交易、主动控制等功能[2—3]。物联网技术在运行方式、拓扑形态等方面对配电网的建设具有很好的支撑作用，但配电网运行环境复杂，既要基于物联网技术实现泛在物联和全景感知，又要面临物联网灵活多样的接入方式以及数量庞大的装置带来的配电网结构动态多变和数据安全风险增大的问题。另一方面，配电物联网的分布式特性使其更难监视海量装置的历史数据，因此建立安全攻击检测机制变得更有挑战性[4]。在此背景下，亟需开展攻防结合、里外兼顾、多维融合的配电物联网信息安全防护方法研究[5]。

随着大规模分布式电源、新型负荷以及边缘层各类型装置的快速增长，配电物联网的信息数据类型逐步多样化，不同类型数据交互方式也存在差异[6]。因此，如何设计安全防护机制保证配电网数据的真实性、可靠性以及时效性是支撑配电网高效稳定运行的关键[7—9]。文献[10]针对能源互联网环境下配电网通信接入网的安全问题，提出基于多种技术融合的电网信息安全模型，并针对配电网业务设计了与模型相关的三层安全访问架构，但是攻击检测的准确性有待提升[11]。文献[12]提出一种面向物联网的分布式学习算法，该算法基于交替方向乘子法（alternating direction multiplier method，ADMM）将弹性网络回归目标优化问题分解为多个能够由边缘节点利用本地数据进行独立求解的子问题，该算法无需物联网节点将隐私数据上传至服务器进行训练，从而减少了计算开销，但需要经过多轮迭代获得最终结果，增加了攻击缓解时间。文献[13]提出一种滑动窗口区块链（sliding window blockchain，SWBC）架构，通过修改传统区块链架构并应用于物联网中，提高了安全性，较大程度减少了内存开销，但由于需要物联网节点对滑块窗口及时更新和备份，对系统存储限制较多[14]。文献[15]提出一种双重组合布鲁姆滤波器（dual combination bloom filter，DCOMB），将比特币挖掘的计算能力转换为查询的计算能力，并使用 DCOMB 方法构建基于区块链的物联网数据查询模型，保障数据的安全性。另一方面，软件定义网络（software defined networking，SDN）支持远程自适应动态管理数据[16]。文献[17]为了满足基于区块链的物联网计算量需求，提出一种协同计算的能效感知集成架构，采用几何编程获得最佳功率和资源分配，通过 SDN 将数据转发决策的执行与逻辑集中控制器分开，可协助数据收集和分析，以便更快响应攻击检测[18]。

由此可见，区块链支持无信任的解决方案，其数据以分布式的形式存储于网络节点中，与配电物联网的数据存储、应用和处理方式较为契合。在配电物联网中，每个配电边缘代理装置都可以使用区块链进行交易，而无需依赖配电云主站。另外，区

收稿日期：2021-02-18；修回日期：2021-05-22
基金项目：国家重点研发计划资助项目（2018YFB0904700）

块链的应用能够在很大程度上避免配电物联网数据集中处理时的高延迟、计算开销大等问题。为此，文中提出一种基于区块链的配电物联网数据安全防护方法。其主要创新点为：针对集中式攻击检测模型计算开销大、检测延时长，而分布式攻击检测模型准确率不高的问题，设计协作式配电物联网数据安全防护模型，并结合动态流量规则减少可疑流量的影响；采用改进实用拜占庭共识（practical Byzantine fault tolerance，PBFT）算法建立信任机制，提高攻击检测效率；利用智能合约动态更新攻击检测模型，通过融合各检测模块实现攻击检测。

1 配电物联网数据安全防护方法

传统配电网中的安全攻击检测大多依赖集中式或分布式架构。在集中式架构中，攻击检测模型部署在配电云主站上，通过攻击检测模型对整个网络收集的海量数据进行分析和检测[19]。然而集中式攻击检测架构的配电云主站计算开销大，需占用大量的通信带宽，检测延时较长。在分布式攻击检测架构中，攻击检测模型部署在配电边缘代理装置中，数据分析和检测处理均局限在配电边缘代理装置中进行，且装置中的检测模型以分布式的方式进行数据训练，不与其他装置和配电云主站共享，这样能够降低通信带宽需求，减少计算开销和检测延时。然而每个配电边缘代理装置都需要足够数量的数据训练才能保证攻击检测的准确决策，而与单一装置关联的传感设备和数据量较少，导致攻击检测的准确率较低[20—21]。

1.1 配电物联网协作式安全防护架构

为了解决集中式和分布式攻击检测架构存在的问题，提出一种协作式配电物联网数据安全防护模型，其架构如图 1 所示。在该架构中，每个单独的配电边缘代理装置都控制自身的攻击检测模型，并基于区块链的智能合约技术与其他配电边缘代理装置以及配电云主站进行共享和更新，确保足够的数据可用性。

协作式安全防护模型包括 3 个层次：感知层，边缘层和云层。感知层由海量配电智能终端和分布广泛的传感单元组成，可监视配电网线路和设备的各种电气量和状态量数据，并转发至边缘层。边缘层由配电边缘代理装置构成，每个配电边缘代理装置均配置低功耗高性能数据聚合器，每个数据聚合器都链接本地的多个配电智能终端和传感器，监测和分析来自配电智能终端和传感器的数据，处理分类并传至配电云主站的接入控制器（access controller，AC），每个 AC 与数据聚合器集群相关联，负责

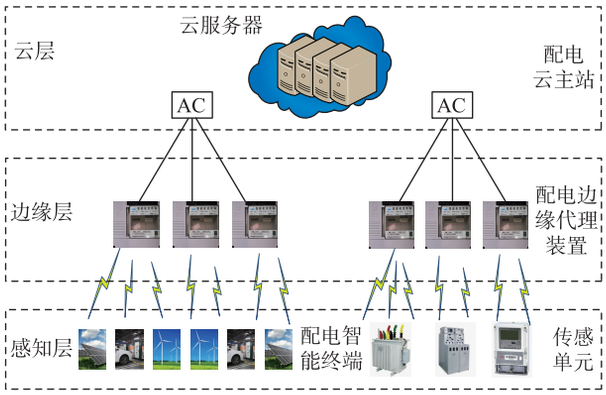

图 1 协作式安全防护架构

Fig.1 Collaborative security protection architecture

分析处理数据以及识别异常数据。基于识别出的异常，AC 更新和管理各自数据聚合器的流量规则和攻击检测模型。此外，每个 AC 都会向云服务器上送数据处理结果，并监视更大范围和长周期的攻击。

1.2 异常流量识别与流量规则

配电边缘代理装置中的数据聚合器会连续监视感知层上与其连接的配电智能终端和传感器节点的流量，并将监视的流量跟踪报告给对应配电边缘代理装置。流量跟踪由 AC 学习和分析，用于识别来自配电智能终端和传感器节点的恶意流量。AC 利用流量的历史行为，如已知的攻击模式和攻击方，识别流量是恶意还是正常[22]。执行分析后，将在 AC 中设置数据聚合器的流量规则。然后，AC 动态地将流量规则下发至各自的数据聚合器。数据聚合器根据流量规则对来自配电智能终端和传感器的流量执行相应操作，如对异常流量进行限流甚至截断。此外，配电边缘代理装置若检测到异常模式或事件，会定期更新配电云主站 AC 的攻击检测模型。AC 具有来自所有配电边缘代理装置的异常事件和模式信息，易于发现来自任何装置的攻击，并提供对应的防护决策[23]。因此，AC 可以从配电边缘代理装置集群中查找互相关联或者相似的安全事件，并作出全局的攻击检测决策。

异常流量识别动态监测来自不同配电智能终端和传感器的流量并收集流量模式，包括流量的数据包和流量级别、功能等，比如正常情况下不同时间间隔的设备利用率、带宽利用率等。此外，异常流量识别模组还监测设备存在的漏洞，并负责准备攻击检测模型，用于分类配电边缘代理装置处的攻击流量。

另一方面，整个网络的流量规则需要动态更新，所提方法通过 AC 动态设置流量规则，以便在发生异常事件时通知配电边缘代理装置的数据聚合

器执行操作。流量规则设置为:(1) 如果攻击检测模型将流量分类为正常流量,则 AC 通知数据聚合器不间断业务流;(2) 当检测到异常流量时,AC 通知数据聚合器立即截断异常流量,并将攻击源列为黑名单,AC 更新列入黑名单的攻击者,并在更大范围应用黑名单,防止攻击者影响配电物联网中的其他设备;(3) 当攻击检测模型未检测到流量模式时,需要对流量进一步调查,AC 指示数据聚合器限制流量,减少可疑流量的影响。通过设置的任务能够减小存储限制和计算延迟。

1.3 基于区块链的攻击检测模型

配电物联网中,攻击会严重损耗网络中各装置和系统的计算开销,影响配电网正常业务开展。文中所提方法采用信任模型实现攻击检测,针对配电物联网中海量电气量、状态量数据以及配电边缘代理装置有限计算能力的现状,采用改进 PBFT 算法建立信任模型,PBFT 算法具有效率高、计算复杂度低的优势,能够兼顾配电物联网各类型终端设备的安全和处理能力。信任模型用来计算每个节点的信任值,而信任值由共识过程中节点的行为决定,信任模型作为共识算法的一部分,可以在每个参与共识的节点中执行。改进后,设定的信任值是 0~1 的实数,信任值越大,可信度越高。新增共识节点初始信任值通常设定为 0.5,根据配电云主站与配电边缘代理装置之间不同的共识行为,分以下 2 种情况讨论。

情况一:在 t 轮共识建立程序中,生成的新区块将增大配电云主站的信任值,并且信任值增大的速度会随着共识轮次的增多而降低,但其最大值小于 1。若无新区块生成,配电云主站信任值将降低,降低的速度由系数 α 决定。设第 t 轮共识后节点 S_i 的信任值为 $R_i(t)$,则 $R_i(t+1)$ 为:

$$R_i(t+1)=\begin{cases}\min\{1,R_i(t)[1+1/(t+1)]\} & \text{有新区块产生}\\ \alpha R_i(t) & \text{无新区块产生}\\ 0 & \text{向不同节点发送不同的信息列表}\end{cases} \tag{1}$$

情况二:在 t 轮共识过程中,若配电边缘代理装置发送同样的消息列表到其他节点,并核实到各节点投票结果一致,则配电边缘代理装置信任值增加。但若配电边缘代理装置未参加共识过程,则其信任值降低,降低速度由 α 确定。若配电边缘代理装置参加共识过程,但各节点投票结果不一致,则其信任值降低,降低速度由系数 β 确定。若某共识节点发送不同的消息列表,则判定其为攻击节点,将其信任值降为 0,并删除。此时,$R_i(t+1)$ 为:

$$R_i(t+1)=\begin{cases}\min\{1,R_i(t)[1+1/(t+1)]\}\\ \text{节点发送相同的信息列表并同意}\\ \alpha R_i(t) \quad \text{节点在本轮未发送信息}\\ \beta R_i(t) \quad \text{多数节点在本轮表示不同意}\\ 0 \quad \text{向不同节点发送不同的信息列表}\end{cases} \tag{2}$$

式中:$0<\beta<\alpha<1$。

在信任模型中,所有正常参与共识的节点信任值均根据每次的共识过程慢慢提升。随着时间推移,共识次数变多,整个系统的决策权越来越集中在正常的共识节点中。另外,可在系统中融合奖赏机制,正常节点获取更多的信任值和决策权,同时得到更多奖励。反之,若节点的信任值太低,则获得很少或无法获得奖励,严重时则从共识节点信息列表中剔除。

此外,通过在信任模型中加入预提交阶段,进一步减少配电网中各装置节点间的通信次数。通过信任值评估,检测区块链中的攻击,工作流程如下。

(1) 配电云主站广播预准备信息至各配电边缘代理装置;

(2) 配电边缘代理装置收到配电云主站广播的信息,首先根据信任值对其进行有效性验证,通过验证后再根据预准确信息收集下游的配电智能终端和传感器数据,更新本地业务信息共识状态,返回预提交信息给配电云主站;

(3) 当配电边缘代理装置收到的预准备信息来自其他配电边缘代理装置,同样根据信任值对其进行验证,如果确认大于信任值阈值,则收集下游的配电智能终端和传感器数据,更新本地业务信息共识状态,并发送预提交信息给其他配电边缘代理装置和配电云主站;

(4) 配电云主站比对预提交信息,根据信任模型更新每个节点信任值和共识节点信息列表,并反馈至配电智能终端、传感单元和配电边缘代理装置。

1.4 攻击检测模型更新与融合

为了动态更新配电物联网中的攻击检测模型,实现数据安全防护,设计基于区块链的攻击检测模块。基于区块链的攻击检测包括 2 个实体:配电云主站 AC 和配电边缘代理装置。AC 定义了用于攻击检测的数据驱动任务,提供测试数据集,验证来自每个配电边缘代理装置的攻击检测模型。配电边缘代理装置负责处理协作式攻击检测模型的实体,使用深度强化学习算法训练本地数据,准备攻

击检测模型[24]。同时,配电边缘代理装置也负责验证准备好的攻击检测模型,配电边缘代理装置之间基于智能合约中的多数表决确定相应的贡献。每个代理装置都会从 AC 获得贡献值,AC 启动攻击检测,配电边缘代理装置通过对本地数据执行深度强化学习训练来准备攻击检测模型,将配电网业务数据以哈希值的形式记录,并发布该模型给链上其他代理装置。当其他代理装置收到广播的攻击检测模型,对其进行评估,通过智能合约给出评估结果。最后,AC 将各个攻击检测模型进行融合,获得融合攻击检测模型。

由于早期融合可将原始数据空间转换为高维特征空间,占用较少的计算和内存开销[25—26],因此,所提方法采用早期融合用于攻击检测模型的融合。基于早期融合的攻击检测模型,将攻击检测任务通过深度强化学习进行分类,即每个代理装置根据 AC 赋予的攻击检测任务设计分类模型,且代理装置使用智能合约中代理指定的属性一致的数据。给定用于攻击检测模型 A_k 的未标记数据集 $a=\{a_1,a_2,\cdots,a_n\}$,其中模型 A_k 第一层输入卷积神经元的编码过程为:

$$h_1=f_{\text{th}}\left(\frac{\sigma_1 a-b_1}{\sigma_1 a+b_1}\right) \tag{3}$$

式中:$f_{\text{th}}(\cdot)$ 为激活函数;σ_1 为激活参数;b_1 为输入层和卷积层之间的偏差参数。

深度强化学习具有深度及强化学习的训练和参数逼近优势,在深度卷积神经网络中,卷积层特征输出 g_1 为下一层卷积层特征输出 g_2 的输入,用于训练参数 σ_2, b_2。重复训练过程,直到得到给定第 N 层卷积层特征输出 g_N 的网络参数 σ_N , b_N。为便于说明,使用 $\sigma=\{\sigma_1,\sigma_2,\cdots,\sigma_N\}$ 和 $b=\{b_1,b_2,\cdots,b_N\}$ 代表攻击检测模型 A_k 的第 N 个卷积层上的网络参数集合。

在连续训练状态下,深度卷积神经网络参数 φ 需要较长的时间才能收敛,文中采用强化学习的 Q 函数逼近方式进行快速收敛。

$$\varphi_{t+1}=\varphi_t+u[r_{t+1}+\gamma\max_a Q(s_{t+1},d_{t+1},\varphi)-Q(s_t,d_t,\varphi)]\nabla\varphi Q(s_t,d_t,\varphi) \tag{4}$$

式中:u 为学习率;r 为奖励;γ 为折扣因子;s 为系统状态;d 为动作策略。

训练网络时,使用均方差定义参数偏差。

$$L(\varphi)=E((r_{t+1}+\gamma\max_a Q(s_{t+1},d_{t+1},\varphi)-Q(s_t,d_t,\varphi))^2) \tag{5}$$

式中:$L(\cdot)$ 为损失函数;$E(\cdot)$ 为期望。

计算参数偏差在 φ 上的梯度,并以随机梯度下降的方式更新参数。

使用上述过程训练攻击检测模型 A_k,从每个模型最后一个卷积层 g_N 中提取模型特征 $(f_1,f_2,\cdots,f_k,\cdots,f_m)$,$m$ 为模型的数量。基于提取的特征,得到所有攻击检测模型 $(A_1,A_2,\cdots,A_k,\cdots,A_m)$ 的早期融合。

为了融合 m 个攻击检测模型,首先,将每一组攻击检测模型的第 k 个特征量 f_k 进行级联运算,获得级联特征 f_{c_k}。然后,计算级联特征 f_{c_k} 的加权和,通过权重矩阵 $\boldsymbol{\omega}_1$,$\boldsymbol{\omega}_2$ 分别计算卷积层输出 $\boldsymbol{G}_k$ 和最终输出 $\boldsymbol{Y}$,使用卷积神经网络算法寻优获得该 2 个矩阵的最佳值。其中卷积层输出为:

$$\boldsymbol{G}_k=\sum_{k=1}^{m}(\boldsymbol{\omega}_1\vartheta f_{c_k}) \tag{6}$$

式中:ϑ 为权值参数。

使用逻辑斯谛函数计算 $\boldsymbol{Y}$ 为:

$$\boldsymbol{Y}=\frac{\boldsymbol{\omega}_2^{\mathrm{T}}\boldsymbol{G}_k}{K+\mathrm{e}_{k=1}^{\sum m}(\boldsymbol{\omega}_2^{\mathrm{T}}\boldsymbol{G}_k)} \tag{7}$$

式中:K 为终值。

2 实验仿真与结果

基于 Mininet 仿真环境,对配电物联网各功能节点进行仿真。在 Linux 服务器上,使用 22 台服务器设置 Mininet,配置均为 128 GB RAM 和 Intel i7 中央处理器(central processing unit,CPU)。目前配电物联网中主流厂家的配电边缘代理装置配置为 1~2 GB RAM。在实验仿真中对其中 20 台服务器均设置 60 台虚拟配电边缘代理装置,2 台服务器均设置虚拟 AC。其中每个代理装置包含 700 个不同的训练数据和 700 个测试数据。实验中,α , β 分别取 0.6,0.4。

2.1 数据量对检测性能的影响分析

在所提协作式检测架构中,每个配电边缘代理装置的攻击检测模型都通过区块链技术进行动态更新,提高了配电边缘代理装置的安全防护性能。其中数据量的增大对攻击检测时间和精度影响较大,其变化情况分别如图 2、图 3 所示。

由图 2 可知,随着数据量增加,3 种架构的检测时间均在不断增加。与分布式和集中式架构相比,协作式架构的检测时间进一步缩短。在协作式架构中,配电边缘代理装置汇集本地数据流量,定期更新数据聚合器中的流量规则,以便更适应配电智能终端和传感器的攻击检测。同时改进 PBFT 算法建立信任模型,减低计算复杂度,提高检测效率。

由图 3 可知,数据量的不断增加为攻击检测提

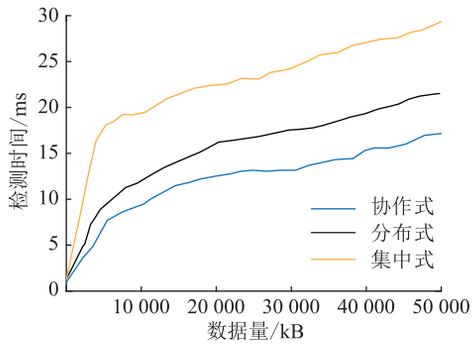

图 2 数据量变化对不同架构检测时间的影响

Fig.2 The impact of data volume change on detection time of different architectures

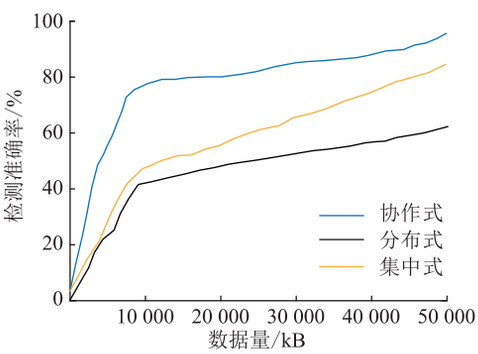

图 3 数据量变化对不同架构检测准确率的影响

Fig.3 The impact of data volume change on detection accuracy of different architectures

供了更多数据,使得 3 种架构的攻击检测准确率不断提高。然而,协作式架构使用区块链技术动态更新配电边缘代理装置的攻击检测模型,使得攻击检测比分布式和集中式架构更精确。协作式架构在配电物联网安全防护方面的表现优于集中式和分布式架构,这表明基于区块链技术的协作式安全防护方法是配电物联网中检测攻击的有效方法。

2.2 攻击类型对攻击缓解时间的影响

为了评估所提方法攻击缓解的性能,将 3 种常见的攻击作为应用场景:因特网控制消息协议(Internet control message protocol,ICMP)洪泛攻击;分布式拒绝服务(distributed denial of service,DDoS)攻击;女巫攻击(SYBIL)。在 3 种不同的攻击场景中,不同架构减少攻击缓解的时间如表 1 所示。

表 1 不同架构的攻击缓解时间

Table 1 Attack mitigation time of different architectures ms

攻击类型	集中式	分布式	协作式
ICMP	122	92	86
DDoS	135	78	54
SYBIL	186	116	76

由表 1 可知,相比集中式和分布式攻击检测架构,基于区块链的协作式攻击检测架构的攻击缓解时间较短。由于其使用区块链技术动态更新配电边缘代理装置的攻击检测模型,可在数据聚合器中快速、准确地更新流量规则以缓解攻击。与分布式和集中式架构相比,减少了预提交阶段节点间的通信次数,缓解攻击的时间得以缩短。

2.3 区块链运行开销

与集中式和分布式架构相比,区块链技术的引用增加了所提方法的额外运行开销,其内存和 CPU 开销对比如表 2 所示。

表 2 区块链运行开销

Table 2 Operational expenses of blockchain

项目	运行开销/%	
	有区块链	无区块链
内存	8.3	6.5
CPU	6.9	5.1

由表 2 可知,配电边缘代理装置在区块链操作期间,对配电业务流量数据的打包和交互消耗了较多的内存和 CPU 资源。所提方法在准确性和检测时间方面均优于集中式和分布式架构,因此可允许稍多的运行开销。

2.4 性能评价

为了进一步论证文中所提方法的性能,将其与文献[12]、文献[13]、文献[15]从平均检测准确率、Mathew 相关系数和工作特性曲线下面积(area under the receiver operating characteristic,AUC)指标进行对比评估,结果如图 4 所示。

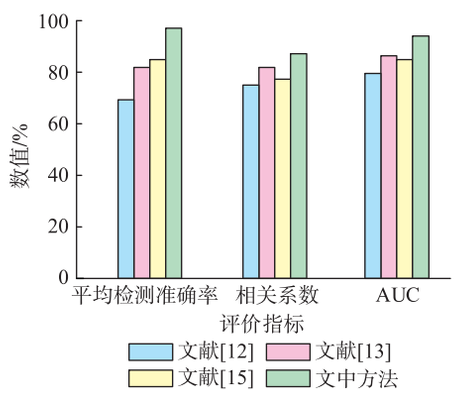

图 4 不同架构的性能比较

Fig.4 Performance comparison of different architectures

由图 4 可知,所提方法相对其他方法整体性能最佳。文献[12]提出一种基于 ADMM 的分布式算法实现隐私数据的传输与存储,不适于处理大量数据,整体性能不佳。文献[13]提出一种 SWBC 架构,优化了传统的区块链架构,提高了数据安全性,

但计算开销较大，且模型易受网络攻击，因此平均检测准确率较低，但 Mathew 相关系数和 AUC 稍高于文献[15]。文献[15]提出一种 DCOMB 方法，构建基于区块链的数据查询模型，保障了数据的安全性。文中所提方法基于协作式架构并融入区块链技术，整体性能优于文献[15]方法，平均检测准确率高于 95%。

3 结语

随着配电网规模不断扩大、网架结构日益复杂、全景监控和分布式能源交易等新型业务大幅增加，亟需研究配电物联网动态安全防护架构。为此，文中提出一种基于区块链的配电物联网数据安全防护方法。基于协作式安全防护模型，结合数据自适应动态管理特性，为配电边缘代理装置提供最佳攻击检测模型。并且在配电边缘代理装置处配置区块链技术实现协作式攻击检测，其中使用早期融合将各攻击检测模块融合。此外，基于 Mininet 搭建仿真平台对所提方法进行实验论证，结果表明，数据量越多，攻击检测的准确率越高，并且所提方法平均检测准确率超过 95%。虽然加入区块链技术对 CPU 和内存的消耗稍大，但总体而言，所提方法提升了配电物联网的数据安全防护水平。

所提方法虽然考虑攻击缓解时间和检测时间，但未深入分析生成区块的时延，因此，在接下来的研究中将重点聚焦生成区块的时延，实现更高效的安全防护。

参考文献：

[1] 王乾同，季振东，张锦涛，等. 应用于配电物联网的高压直流固态变压器启动策略研究[J]. 供用电，2020，37(1)：30-36.
WANG Qiantong，JI Zhendong，ZHANG Jintao，et al. Research on start-up strategy of HVDC solid-state transformer applied to distribution internet of things[J]. Distribution & Utilization，2020，37(1)：30-36.

[2] 孙浩洋，张冀川，王鹏，等. 面向配电物联网的边缘计算技术[J]. 电网技术，2019，43(12)：4314-4321.
SUN Haoyang，ZHANG Jichuan，WANG Peng，et al. Edge computation technology based on distribution Internet of Things[J]. Power System Technology，2019，43(12)：4314-4321.

[3] 李洪全，张冀川，丁浩，等. 基于 IPv6 的配电物联网通信单元设计[J]. 供用电，2020，37(1)：21-29.
LI Hongquan，ZHANG Jichuan，DING Hao，et al. Design of IoT communication unit based on IPv6[J]. Distribution & Utilization，2020，37(1)：21-29.

[4] PAL S，RABEHAJA T，HILL A，et al. On the integration of blockchain to the Internet of Things for enabling access right delegation[J]. IEEE Internet of Things Journal，2020，7(4)：2630-2639.

[5] 吴超，刘元安，吴帆，等. 移动性受限物联网应用中基于图论的高效数据采集策略[J]. 浙江大学学报(工学版)，2018，52(8)：1444-1451，1460.
WU Chao，LIU Yuan′an，WU Fan，et al. Efficient data gathering scheme in mobility-constrained Internet of Things with graph theory[J]. Journal of Zhejiang University (Engineering Science)，2018，52(8)：1444-1451，1460.

[6] 乔蕊，曹琰，王清贤. 基于联盟链的物联网动态数据溯源机制[J]. 软件学报，2019，30(6)：1614-1631.
QIAO Rui，CAO Yan，WANG Qingxian. Traceability mechanism of dynamic data in Internet of Things based on consortium blockchain[J]. Journal of Software，2019，30(6)：1614-1631.

[7] 潘旭，王金丽，赵晓龙，等. 智能配电网多维数据质量评价方法[J]. 中国电机工程学报，2018，38(5)：1375-1384.
PAN Xu，WANG Jinli，ZHAO Xiaolong，et al. Multi dimensional data quality evaluation method for intelligent distribution network[J]. Proceedings of the CSEE，2018，38(5)：1375-1384.

[8] CAI J Y，HUANG C，LI Y，et al. Data standard interface of distribution network equipment inspection automation system[J]. IOP Conference Series：Materials Science and Engineering，2018，452(2)：181-190.

[9] 徐美强，高志远，王伟，等. 基于区块链技术的智能变电站配置版本管理[J]. 电力系统保护与控制，2020，48(2)：60-67.
XU Meiqiang，GAO Zhiyuan，WANG Wei，et al. Smart substation configuration version management based on blockchain technology[J]. Power System Protection and Control，2020，48(2)：60-67.

[10] LI Y X，ZHU W G，PENG H D，et al. Network power-grid information security architecture model for intelligent distribution communication network[C]//Proceedings of the 2nd International Conference on Telecommunications and Communication Engineering. 2018：348-351.

[11] 孟仕雨，孙伟卿，韩冬，等. 支持现货市场的分布式电力交易机制设计与实现[J]. 电力系统保护与控制，2020，48(7)：151-158.
MENG Shiyu，SUN Weiqing，HAN Dong，et al. Design and implementation of decentralized power transaction mechanism to spot market[J]. Power System Protection and Control，2020，48(7)：151-158.

[12] 方维维，刘梦然，王云鹏，等. 面向物联网隐私数据分析的分布式弹性网络回归学习算法[J]. 电子与信息学报，2020，42(10)：2403-2411.
FANG Weiwei，LIU Mengran，WANG Yunpeng，et al. A distributed elastic net regression algorithm for private data analytics in Internet of Things[J]. Journal of Electronics & Information Technology，2020，42(10)：2403-2411.

[13] KOSHY P，BABU S，MANOJ B S. Sliding window blockchain architecture for Internet of Things[J]. IEEE Internet of Things Journal，2020，7(4)：3338-3348.

[14] 朱超平，任继平. 基于智能优化算法的物联网异构数据融合方法[J]. 吉林大学学报(理学版)，2019，57(3)：627-632.

ZHU Chaoping, REN Jiping. Heterogeneous data fusion method of Internet of Things based on intelligent optimization agorithm [J]. Journal of Jilin University (Science Edition), 2019, 57(3): 627-632.

[15] REN Y J, ZHU F J, SHARMA P K, et al. Data query mechanism based on hash computing power of blockchain in Internet of Things[J]. Sensors, 2020, 20(1): 207-228.

[16] 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.

[17] FU S, FAN Q L, TANG Y J, et al. Cooperative computing in integrated blockchain-based Internet of Things[J]. IEEE Internet of Things Journal, 2020, 7(3): 1603-1612.

[18] LYU Z, SONG H B. Mobile Internet of Things under data physical fusion technology[J]. IEEE Internet of Things Journal, 2020, 7(5): 4616-4624.

[19] KADAM S B, JOHN S K. Blockchain integration with low-power Internet of Things devices[J]. Handbook of Research on Blockchain Technology, 2020: 183-211.

[20] LIU Y Q, WANG K, LIN Y, et al. A lightweight blockchain system for industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3571-3581.

[21] WEI H X, FENG W, ZHANG C, et al. Creating efficient blockchains for the Internet of Things by coordinated satellite-terrestrial networks[J]. IEEE Wireless Communications, 2020, 27(3): 104-110.

[22] MATHANE V, LAKSHMI P V. Multi-layer attestation for Internet of Things using blockchain[J]. International Journal of Engineering and Advanced Technology, 2020, 9(3): 995-1000.

[23] KARATAS F, KORPEOGLU I. Fog-based data distribution service (F-DAD) for Internet of Things (IoT) applications[J]. Future Generation Computer Systems, 2019, 93: 156-169.

[24] 朱文广,熊宁,钟士元,等. 基于区块链的配电网电力交易方法[J]. 电力系统保护与控制,2018,46(24):165-172.
ZHU Wenguang, XIONG Ning, ZHONG Shiyuan, et al. Power-trading method for distribution network based on block chain [J]. Power System Protection and Control, 2018, 46(24): 165-172.

[25] CRAM W A, PROUDFOOT J G, D'ARCY J. Organizational information security policies: a review and research framework [J]. European Journal of Information Systems, 2017, 26(6): 605-641.

[26] 王鸿玺,唐如意,吴一敌,等. 基于 HPLC 的智能抄表技术在客户侧泛在电力物联网中的研究及应用[J]. 电力系统保护与控制,2020,48(3):92-98.
WANG Hongxi, TANG Ruyi, WU Yidi, et al. Research and application of smart meter reading technology based on HPLC in customer side universal power Internet of Things[J]. Power System Protection and Control, 2020, 48(3): 92-98.

作者简介:


王海

王海(1976),男,硕士,高级工程师,从事电力信息通信等技术研究工作;

曾飞(1984),男,硕士,高级工程师,从事智能配电网、新能源及储能等技术研究工作(E-mail:zeng_nj2021@126.com);

杨雄(1983),男,博士,高级工程师,从事配电自动化、配电物联网、交直流配电网、新能源发电、储能技术等工作。

Blockchain-based data security protection for distribution Internet of Things

WANG Hai, ZENG Fei, YANG Xiong

(State Grid Jiangsu Electric Power Co., Ltd. Research Institute, Nanjing 211103, China)

Abstract: Aiming at the problem that massive data in distribution Internet of Things is vulnerable to network attack, a data security protection method of distribution Internet of Things based on blockchain is proposed. Firstly, a collaborative security protection architecture is constructed, and the abnormal traffic identification mechanism is designed through adaptive traffic monitoring. Secondly, the improved practical Byzantine fault tolerance (PBFT) is used to establish a trust mechanism to share the attack detection model between the distribution cloud master station and each distribution edge agent. Then, based on the blockchain smart contract, the attack detection model is dynamically updated, and the deep reinforcement learning is used to train and fuse each attack detection model to obtain the attack detection fusion model. Finally, a simulation platform based on Mininet is built to demonstrate the proposed method. The results show that the comprehensive performance of the proposed attack detection model is better than that of centralized and distributed models.

Keywords: blockchain; distribution Internet of Things; data security protection; practical Byzantine fault tolerance (PBFT); deep reinforcement learning; attack detection

(编辑 吴楠)