以数据为核心的安全泛在微电网智能管理平台

张 捧,陈艺琳,易传佳,王 园,夏萍萍,左黎明
(华东交通大学 理学院,江西 南昌 330013)

摘 要:随着电网系统软硬件建设的快速发展,大数据、人工智能和物联网技术在电网系统中得到广泛应用,泛在电力物联网技术正在快速发展,以分布式能源为基础的泛在微电网研究成为一个热门课题。针对泛在微电网中存在海量数据的集中管理困难、电网融合平台传输协议中缺乏安全认证以及数据完整性保护等安全问题,提出一个以数据为核心的安全泛在微电网智能管理平台,重点分析了平台中格式化数据封包的处理机制,并设计了一个基于数字签名的安全服务协议。最后,模拟用户申请窃漏电用户识别服务,实现了数据封包在整个平台中的统一处理和安全认证,可以有效解决海量数据管理以及数据完整性保护和可靠性认证问题,为大数据技术在泛在微电网的应用提供了技术支撑。

关键词:泛在微电网;智能管理平台;安全;大数据;数字签名
中图分类号:TP181;TP399 **文献标识码**:A **文章编号**:1673-629X(2020)10-0143-06
doi:10.3969/j.issn.1673-629X.2020.10.026

Data-centric Security Ubiquitous Micro-grid Intelligent Management Platform

ZHANG Peng,CHEN Yi-lin,YI Chuan-jia,WANG Yuan,XIA Ping-ping,ZUO Li-ming
(School of Science,East China Jiaotong University,Nanchang 330013,China)

Abstract:With the rapid development of software and hardware construction of power grid system,big data,artificial intelligence and internet of things have been widely applied in power grid system. Ubiquitous power internet of things technology is developing rapidly,and the research of ubiquitous micro-grid based on distributed energy has become a hot topic. Aiming at the ubiquitous micro-grid's centralized management of massive data and many security issues in the fusion ubiquitous network platform transmission protocol,We propose a data-centric security ubiquitous micro-grid intelligent management platform. We focus on the processing mechanism of formatted data packets in the platform and design a digital signature-based security service protocol. Finally,the simulated user application for the stolen electricity user identification service realizes the unified processing and security authentication of the data packet in the whole platform,which can effectively solve the problems of massive data management,data integrity protection and reliability certification,and provides technical support for the application of the big data technology in the ubiquitous micro-grid.

Key words:ubiquitous micro-grid;intelligent management platform;security;big data;digital signature

0 引 言

微电网是由分布式电源、储能装置和用电负荷组成的一种微型供电网络,具备并网、脱网等多种运行模式,是分布式电源接入电网的一种新型手段,在解决偏远地区缺电和无电问题,以及就地消纳分布式清洁能源,降低分布式发电大规模接入对大电网的冲击等方面具有一定优势。2016 年,葛磊蛟等[1]提出一种大数据存储的三层管理框架设计方案,为智能配用电大数据技术的应用提供基础支撑作用。2017 年,周小平等[2]针对多个交、直流子网的互联系统的复杂结构,设计了一种自主调控的微网群架构。2018 年,郑琨琪等[3]提出一种基于数据驱动系统架构的实现。同年,Harmon 等[4]介绍了一种基于云的混合无线网状通信框架,用于网络微电网集群的双分布式优化。另一方面,这种半开放性的泛在微电网也带来了数据安全和隐私保护问题,委内瑞拉因网络攻击引起大规模停电、乌克兰电力系统因恶意代码攻击造成多个电力区域破坏[5-6]等安全事件,使大数据安全和隐私保护问题[7-9]受到了广泛关注。2017 年,戚湧等[10]指出电网融合泛在网平台主要存在隐私信息泄露、非法访问、认证授权

收稿日期:2019-12-14 **修回日期**:2020-04-15
基金项目:2018 国家级大学生创新创业训练计划项目(201810404003);江西省学位与研究生教育教学改革研究项目(JXYJG-2018-095)
作者简介:张 捧(1999-),女,软件工程师,研究方向为网络信息系统、网络环境下智能信息处理与自动化数据采集;左黎明,副教授,硕士,CCF 会员(E20-0013632M),研究方向为信息安全、大数据分析。

等安全问题,但并未给出具体的技术实现。该文针对泛在微电网当前管理与控制中存在的数据安全问题,提出一个以数据为核心的微电网智能计算管理平台,重点分析了安全数据封包的处理机制及其技术方案。

1 当前泛在微电网信息管理中存在的问题

泛在微电网数据量大,数据类型复杂。在实现微电网的智能调度、实时监测及电力企业的信息化管理过程中,包含设备状态监控数据、设备检修维护日志、设备仿真数据结构化数据及信息化系统的半结构化数据等。电力企业市场营销数据又包括售电、用电客户、电价交易等方面的数据[11]。这些数据包括二维数据流、图像数据、波形数据、文本数据等。其次,这些数据作为系统的运行状态的多个维度的刻画,系统需要利用各种大数据分析与预测算法快速处理和分析这些数据[12],然后将其转换成可以指导电网运行的决策信息,从而实现对电网的智能管理和实时调度[13]。

当前泛在微电网的多种运行模式与控制机制非常复杂[14-16],缺乏可靠的数据安全传输与认证保障。微电网在并网运行的情况下,既可以与外部电网并网运行,也可以脱网运行;在独立运行的情况下,不与外部电网连接,能够实现电力电量的自我平衡。这种复杂的运行模式,促进了分布式电源所产生电能合理分配的同时,避免了微电网与主电网直接连接所带来的弊端,但是对微网集群之间高效协作产生了更高的要求。由于微网之间的业务数据相互隔离,同一协作微网集群的业务需要按业务的关联性在多个微网集群间共享。此外,微电网多网群协作需要复杂的控制和调度,当前研究主要集中在协作机制和策略研究上,较少涉及数据安全传输与认证保障。由于微电网的控制单元分布式部署,无法集中保护,因此易于受到各种类型的攻击,例如篡改和伪造控制指令恶意联网、恶意脱网等。

2 以数据为核心的安全泛在微电网智能管理平台

2.1 管理平台架构与核心功能分析

为解决当前泛在微电网信息管理中存在的问题,如图 1 所示,提出了一种面向协作微电网群并且能够处理海量大数据的安全泛在微电网智能管理平台架构,该架构核心包括感知中心、数据中心、计算中心、应用中心和安全服务中心。

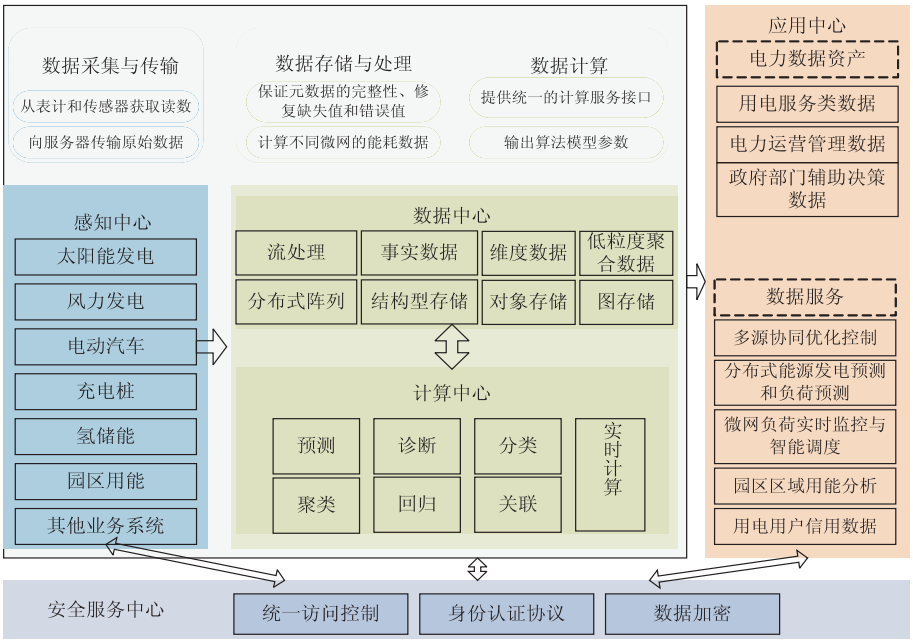

图 1 以数据为核心的安全泛在微电网智能管理平台

感知中心用于元数据的采集与管理。感知中心采集泛在微电网产生的各种结构化和非结构化数据,以格式化数据封包的形式交由数据中心进行统一处理。数据中心根据封包的类型,分别对不同类型的数据进行处理,如对流式数据、事实数据、高维度数据和低粒度聚合数据分别采用不同的方式进行拆分、预处理和计算,然后将其存储于分布式阵列、结构型存储、对象存储、图存储等不同的数据结构之中。

数据中心作为资源集中管理的核心,管理与存储来自感知中心的元数据,为计算中心提供泛在微电网多维度的数据,为应用中心提供原子化的数据服务,与各个中心的交互采用统一的格式化数据封包。

计算中心解析来自数据中心的格式化数据封包,调用算法插件输出训练后的算法参数,然后将算法参数进行本地备份后,打包处理成格式化数据封包发送给数据中心进行结构化存储。计算中心通过实时计算

和离线计算的方式,为数据中心提供预测、分类、回归、聚类、诊断、关联的数据分析功能,其中实时计算用于处理简单的计算逻辑,主要响应用户的在线需求,离线计算用于处理复杂的计算模型,如神经网络参数的训练,其基于多种开源的大数据计算框架。

应用中心,作为数据服务和数据资产输出端,实时响应用户请求,灵活编排以数据为核心的服务。

安全服务中心提供数据的统一访问控制、身份认证协议、数据加密等功能,主要通过解析格式化数据封包中的身份信息、请求的服务信息等进行权限的控制、用户身份的认证和安全访问等。

2.2　以数据封包为核心的数据处理机制

在电网融合的泛在微电网应用架构中,主要参与对象由人、各类软件和硬件设备构成,其中人包括微电网系统的管理员、服务使用者、服务提供者和普通用户,应用软件包括应用软件、系统软件、通讯转发和控制组件、服务中间件、数据库、身份认证中心等,硬件设备包括各种类型的计算机、网络设备、安全设备、物联网设备等,是一个综合的集成化和智能化服务平台。每一个参与对象之间的通讯十分复杂,包含人与人、人与硬件、人与软件、硬件与硬件、硬件与软件、软件与软件之间,所涉及的交互信息复杂多变,包括各种类型的数据、网络控制指令和命令、身份验证协议数据,若采用传统的消息和数据处理方法进行管理是难以实现的,为了实现便捷统一管理和快捷处理,设计了一种基于 PACKET 数据封包(如表 1 所示)的消息处理机制和以格式化封包数据为核心的程序开发方法。

表 1　PACKET 数据封包的格式

符号	说明
SID	封包发送者的身份信息
DID	封包接收者的身份信息
MTYPE	消息类型序列号
PTYPE	协议序列号
ATYPE	动作序列号
DATALEN	业务数据长度
DATA	业务数据

平台中的交互均以一个完整的 PACKET 封包格式进行,其格式包括表 1 中消息发送者的身份信息(SID),封包接收者的身份信息(DID),消息类型序列号(MTYPE,标识消息的类型)、协议序列号(PTYPE,标识所执行的协议)、动作序列号(ATYPE,标识所执行动作和操作)、业务数据长度(DATALEN)、业务数据(DATA),其中业务数据表示需要处理或立即返回的数据,可以是嵌套的 PACKET 数据封包格式或加密密文。

各个中心都包含一个 PACKET 数据封包处理组件,其包括:接收器、转发器、消息分发处理器、协议分发处理器、协议插件、封包处理类,各个组件相互协作,保证各个中心交互的稳定性。如图 2 所示的 PACKET 数据封包处理流程中,用户的身份信息交由封包接收器认证,认证失败则将封包交由转发器负责转发,转发器根据当前计算网络的状态和各节点负载情况进行封包路由的智能选择与优化,然后将封包转发给下一层。若认证成功,则将封包发给消息分发处理器,消息分发处理器根据消息类型再将封包发给协议分发处理器,协议分发处理器根据协议序列号将封包发给对应的协议插件,协议插件根据动作号调用合适的业务对象方法提取对应的业务数据完成处理后,再次将结果以封包形式逐级返回。这种基于 PACKET 数据封包的交互机制,使得各中心之间通过封包传递数据解耦,实现了以数据为驱动的服务。

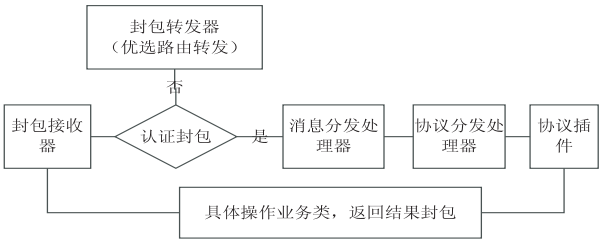

图 2　PACKET 数据封包处理流程

2.3　安全数据服务协议

基于 PACKET 数据封包的交互机制中,存在伪造攻击、重放攻击、恶意篡改和拒绝服务等安全威胁,如以智能移动终端为跳板入侵内部网络[17]、监控电网设备数据传输安全[18]、调度控制系统的远方操作安全[19]等问题,因此数据封包交互协议中引入安全认证机制来保证数据的完整性、机密性、不可否认性、身份认证、授权和访问控制。

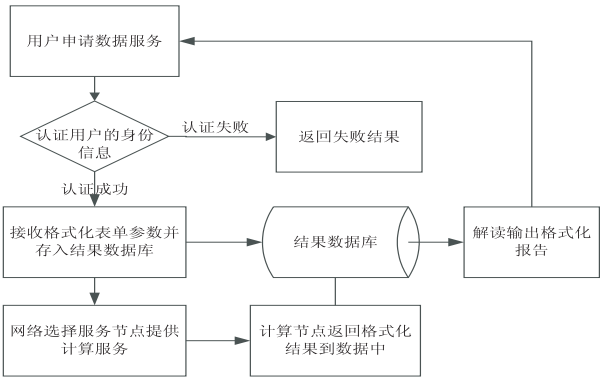

图 3　数据服务协议交互流程

为进一步描述数据服务协议过程,以下将每个参与的对象称为节点。如图 3 中所示的安全服务协议交互流程中,用户在服务登记节点注册服务请求,登记节点提交含有签名信息的服务申请表单,计算网络选择合适节点提供计算服务,服务节点提交含有签名信息的结果表单到服务结果数据库,最后登记节点查询、解

读结果并给出可视化结果。采用这种以数据为核心的模式的优点在于用户只需要提供格式化表格(如 XML、UML、JSON、YAML 等)、返回结果的格式和个人信息,无需了解计算网络的处理过程和算法的计算细节,可视化结果输出后可通过登记节点进行查询,或由计算网络平台直接推送至用户终端。该模式适用于需要多阶段处理的复杂的数据,如需要各种高级算法支持的计算模型,需要多节点配合作业的分布式计算,另外还有耗时较长的计算服务,其具体计算过程如下:

假设 C 为请求服务的用户,W 为登记服务节点,(U1,U2,U3)为计算节点,"|"表示字符串连接,用户 C 请求一项基于神经网络算法的数据挖掘服务,ID 为用户 C 的身份信息,ServiceNum11 为服务号,ServiceRecordNum11 为服务记录号,Sig 为数字签名。

(1) C→W:用户 C 发送服务请求 PACKET 封包给登记服务节点 W,其封包格式为 DATA = ID | ServiceNum11 | Sig(ID,H(ServiceNum11),Time),然后验证用户 C 的身份;

(2) W→C:查询计算服务中心所有应用提供的服务号,检索是否存在 ServiceNum11 服务,若存在,则添加 ServiceNum11 服务到服务表备案,然后返回格式化信息和服务记录号 ServiceRecordNum11 给 C;

(3) C→W:用户 C 提交参数 PACKET 封包给登记服务节点 W,其封包 DATA 部分的格式为 DATA = ID | ServiceNum11 | ServiceRecordNum11 | XMLParam | Sig(ID,H(ServiceNum11),XMLParam);

(4) W→(U1,U2,U3):登记服务节点 W 分别给计算节点(U1,U2,U3)发送 PACKET 封包,其封包 DATA 部分的格式为 DATA = ID | ServiceNum11 | ServiceRecordNum11 | XMLParam | Sig(ID,H(ServiceNum11),XMLParam);

(5)(U1,U2,U3)→DATABASE:计算节点(U1,U2,U3)分别将其计算结果封包(PACKET1,PACKET2,PACKET3)存入结果数据库中;

(6) W→DATABASE:登记服务节点 W 获取结果封包 XMLAnswer = PACKET1 | PACKET2 | PACKET3,并分析和解读结果,并对结果可视化封装,存入数据中心,存入数据中心的 PACKET 封包的 DATA 部分的格式为 DATA = ID | ServiceNum11 | ServiceRecordNum11 | XMLParam | XMLAnswer | Sig(ID,H(ServiceNum11),XMLAnswer);

(7)用户 C 提供服务记录号 ServiceRecordNum11 访问结果,并个性化视图输出结果。

2.4 数据安全传输与控制协议

数据服务协议的过程中,首先需要通过数字签名认证用户的身份信息,认证失败则返回错误信息,否则将数据封包交由下一个节点进行处理。其数字签名认证协议如图 4 所示,图中 C 为服务请求方,W 为服务响应方,ID 为用户的身份信息(如手机号、身份证号、email 地址、学号等),m 为消息,RandParams 为随机值,H 为杂凑函数,Sig 为数字签名算法,Verify 为验证签名算法。具体的交互过程如下:

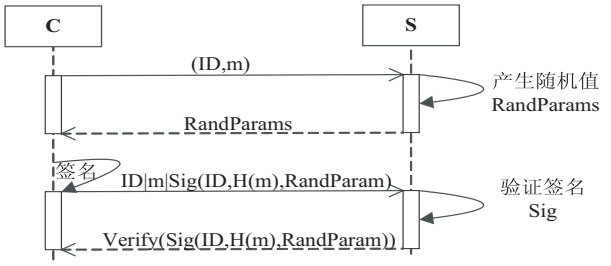

图 4 数字签名认证协议

(1) C→S:服务请求方 C 发送(ID,m)给服务响应方 S,并请求一个随机值 RandParams;

(2) S→C:服务响应方 S 将随机值 RandParams 发送给服务请求方 C;

(3) C→S:服务请求方 C 调用算法 sig(ID,H(m),RandParams)进行签名,并将签名发送给服务响应方;

(4) S→C:服务响应方 S 调用算法 Verify(Sig(ID,H(m),RandParams))进行验证签名,最后将验证结果返回给服务请求 C。

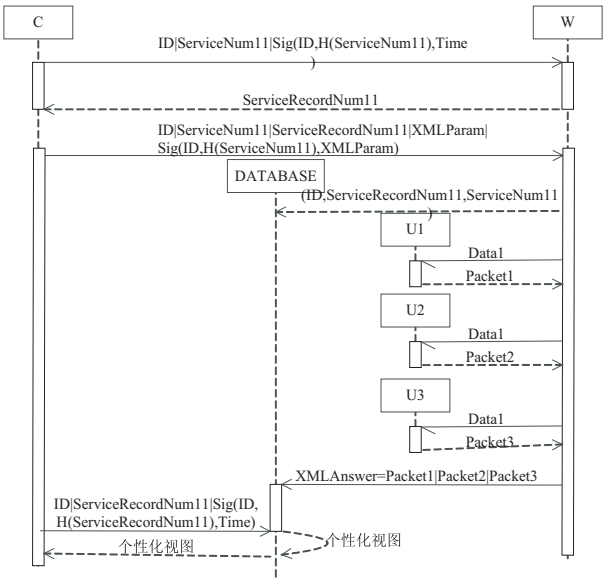

图 5 泛在微电网管理平台的数据安全传输与控制协议

基于 2.3 节中的数据服务协议和 2.4 节中的数字签名认证协议,以数据为核心的泛在微电网管理平台的数据安全传输与控制协议如图 5 所示。在交互的过程中,每一个数据封包都包含了请求方的身份信息、请求的服务信息、随机值和签名信息,服务接收方都需要先解析封包中的信息,然后验证其签名的合法性,中心节点一方面作为接收方验证上一节点的请求,另一方

面作为请求方,将服务请求转发给下一个节点,通过这种机制,来保证数据在这个链路中的安全传输与控制。

3　安全性分析

(1)抗明文泄露攻击。

该文提出的安全数据服务协议中,隐私数据通过加密的数据封包进行传输,保证了数据的机密性。若恶意攻击者想从加密的数据封包中获得明文,就必须先计算加密密钥。若想获得加密密钥,则须先获得数据封包发送节点的私钥,而恶意的攻击者获得私钥的过程中面临解离散对数问题,因此加密密钥的获得是困难的,从而无法恢复出密文。因而各节点的交互过程中保证了数据的机密性,防止了泛在微电网系统中隐私数据的泄露。

(2)抗篡改攻击。

该文提出的数据安全传输与控制协议中,数字签名过程中的杂凑函数 H 用于产生消息摘要,为要签署的消息增加一个可以验证的冗余,使得此杂凑消息包含可以识别的信息,消息的接收节点可以验证该消息确实是来自所声称的消息发送节点(消息源),且在 PACKET 数据封包传输的过程中未收到未授权方式的篡改,保证了消息在各个节点交互过程中的完整性。

(3)抗身份冒充攻击。

各个节点在响应服务请求之前,需先认证数据封包发送节点的身份,认证过程中数据封包发送节点产生数字签名,数字签名中引入了随机值 RandParams,保证了数据的新鲜性,数据封包接收节点验证签名,防止数据封包发送节点身份被恶意攻击者冒充。

4　数据安全传输与控制实验仿真

在进行实验仿真的过程中,为实现图 6 中的仿真实验节点部署结构,配置环境:服务器端操作系统为 Ubuntu Linux for ARM,客户端操作系统为 Windows XP 64-Bit Edition,利用包管理器安装. NET Core,用以支持 C#开发环境。基于 C/S 架构,采用多 Agent 模式,实现基于 WinForm 程序的用户客户端 C#开发,数据库版本为 SQL Server 2008 R2。

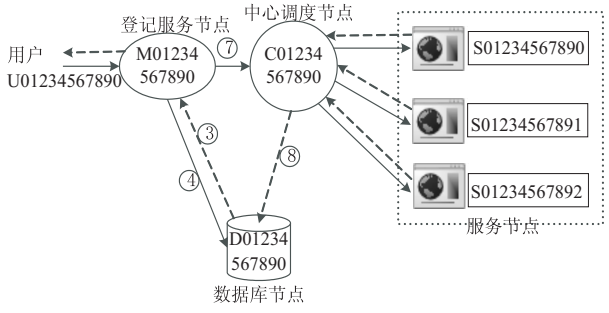

图 6　仿真实验节点部署结构

将图 6 中的登记服务节点、中心调度节点、数据节点和服务节点均部署在服务器端,用户节点、应用节点均部署在客户端。实验中模拟用户 U01234567890 申请一项电力窃漏电用户自动识别的服务,服务号为 SN0123456789。协议中的数字签名算法为 RSA 签名算法,杂凑函数为 MD5 算法,安全服务协议的交互封包如下所示:

(1)用户 U01234567890 向登记服务节点 M01234567890 发送封包的 DATA 格式如下:

U01234567890 | SN0123456789 | 5LkWxCDDeb8Y8VzkX6xjCxpvfJKt6VaPV3gofjfnnSAgVNVQv86ChEFfKr0VuUbulk1L7c6YER6ZwM6fsfxm91961cMxPO49e CQWgevOtoYBu5 UkqaUt-LoiLIBXMkac+9LGt3MtWEw==

(2)登记服务节点 M01234567890 生成一个服务记录号 SRN0123456789,然后将该服务记录号返回给用户 U01234567890,并备案在数据库节点 D01234567890 中。

(3)用户 U01234567890 接收到服务记录号 SRN0123456789 后,输入表 2 中的元数据,转换成 XML 的形式(XMLParams),并提交封包,该封包 DATA 部分如下:

表 2　某企业大用户终端报警数据

电量趋势下降指标 DeclineIndex	线损指标 LineLossIndex	告警类指标 WarningIndex	是否窃漏电 IsLeakage
4	1	1	1
4	0	4	1
2	1	1	1

U01234567890 | SN0123456789 | SRN0123456789 | XMLParams | rWaQKyDsyd60oy7qbynsffZ + Kxo70uci9hp9kJMQzLg8pQHmkxLUn9FrI2pgDaf ChBWYzw 6NV8dAD3 + MEUoI8P2d9Awhyr KhNWIc9ElMI1mjKiVo4WU3taDCfrt/ZpQqK Dal3fleA==

封包中 XMLParams 的 XML 格式如下:

```
<? xml version="1.0" encoding="UTF-8" ? >
<0>
<DeclineIndex>4</DeclineIndex>
<LineLossIndex>1</LineLossIndex>
<WarningIndex>1</WarningIndex>
<IsLeakage>1</IsLeakage>
</0>
<1>
<DeclineIndex>4</DeclineIndex>
<LineLossIndex>0</LineLossIndex>
<WarningIndex>4</WarningIndex>
<IsLeakage>1</IsLeakage>
</1>
<2>
<DeclineIndex>2</DeclineIndex>
```

<LineLossIndex>1</LineLossIndex>
<WarningIndex>1</WarningIndex>
<IsLeakage>1</IsLeakage>
</2>
<3>
<DeclineIndex>9</DeclineIndex>
<LineLossIndex>0</LineLossIndex>
<WarningIndex>0</WarningIndex>
<IsLeakage>0</IsLeakage>
</3>

(4)登记服务节点 M01234567890 提交封包向 CART 决策树计算服务节点 U1、U2、U3 申请分布式计算服务,其封包的 DATA 为步骤(3)中的 DATA;

(5)计算节点(U1,U2,U3)返回计算结果封包(PACKET1,PACKET2,PACKET3)给服务登记节点,其中 PACKET1 = PACKET2 = PACKET3,封包中 DATA 的 XML 格式如下:

<? xml version = "1.0" encoding = "UTF-8" ? >
< ModelParms >
DecisionTreeClassifier(class_weight = None, criterion = ′gini′,
max_depth = None, max_features = None, max_leaf_nodes = None,
min_samples_leaf = 1, min_samples_split = 2, min_weight_fraction
_leaf = 0.0,
presort = False, random_state = None, splitter = ′best′)
</ModelParms>

(6)登记服务节点 M01234567890 获取结果封包 XMLAnswer = PACKET1 | PACKET2 | PACKET3,并分析和解读结果,并对结果可视化封装,存入数据中心,存入数据中心的 PACKET 封包的数据部分(DATA)如下:

U01234567890 | SN0123456789 | SRN0123456789 | XMLParams | XMLAnswer | rWaQKyDsyd60oy7qbynsffZ + Kxo70uci9hp9kJMQz | Lg8pQHmkxLUn9FrI2pg DafChBWYzw6 NV8dAD3 + MEUoI8P2 d9AwhyrKhNWIc9ElMI1mjKiVo4WU3ta DCfrt/ZpQqKDal3fleA = =

封包中 XMLParams 与步骤(3)中的 XMLParams 格式相同。

5 结束语

针对泛在微电网海量数据的统一管理问题,和复杂的脱网、并网运行模式中的数据安全传输与认证问题,提出一个以数据为核心的泛在微电网智能管理平台。主要设计了该平台中以 PACKET 数据封包为核心的处理机制及数据安全服务协议,并分析了将该服务协议应用于泛在微电网管理平台中以抵抗明文泄露攻击、篡改攻击和身份冒充攻击,最后通过仿真实验分析了数据封包在各个节点之间的安全传输与控制过程,一定程度上解决了数据集中管理与安全传输问题。但是 PACKET 数据封包在传输过程中还存在复杂的路由调度机制,未来还需进一步研究。

参考文献:

[1] 葛磊蛟,王守相,瞿海妮. 智能配用电大数据存储架构设计[J]. 电力自动化设备,2016,36(6):194-202.

[2] 周小平,陈燕东,周乐明,等. 一种微网群架构及其自主协调控制策略[J]. 电工技术学报,2017,32(10):123-134.

[3] 郑琨琪,王治华,范 帅,等. 电网信息物理系统的数据驱动架构设计及应用[J]. 电网技术,2018,42(10):3116-3127.

[4] HARMON E,OZGUR U,CINTUGLU M H,et al. The internet of microgrids:a cloud-based framework for wide area networked microgrids[J]. IEEE Transactions on Industrial Informatics,2018,14(3):1262-1274.

[5] 童晓阳,王晓茹. 乌克兰停电事件引起的网络攻击与电网信息安全防范思考[J]. 电力系统自动化,2016,40(7):144-148.

[6] 丁坚勇,周 凯,田世明,等. 基于大数据技术的重要用户供电安全分析[J]. 电网技术,2016,40(8):2491-2495.

[7] 龚钢军,高 爽,陆 俊,等. 地市级区域能源互联网安全可信防护体系研究[J]. 中国电机工程学报,2018,38(10):2861-2873.

[8] 魏三强,任 环,杨 威. 保护隐私的智能电网大数据分析挖掘技术[J]. 广西大学学报:自然科学版,2015,40(3):714-721.

[9] 陈居勤. 智能电网隐私保护方法的研究[D]. 长沙:湖南大学,2016.

[10] 戚 湧,郭诗炜,李千目. 电网融合泛在网信息平台设计及安全威胁分析[J]. 计算机科学,2017,44(3):150-152.

[11] 崔立真,史玉良,刘 磊,等. 面向智能电网的电力大数据存储与分析应用[J]. 大数据,2017,3(6):42-54.

[12] 周念成,廖建权,王强钢,等. 深度学习在智能电网中的应用现状分析与展望[J]. 电力系统自动化,2019,43(4):180-191.

[13] 邓炜瑛. 智能电网大数据处理技术现状与挑战[J]. 中外企业家,2015(6):126.

[14] 徐晓宁,周雪松. 微网脱/并网运行模式平滑切换控制策略[J]. 高电压技术,2018,44(8):2754-2760.

[15] 赵文会,祁 宇,范韩璐. 区域电网的主从博弈调度[J]. 控制理论与应用,2018,35(5):644-652.

[16] 杨欢红,刘书洲,王西瑶,等. 多场景多模式独立微电网经济运行研究[J]. 高压电器,2018,54(3):174-180.

[17] 王 晋,喻 潇,刘 畅,等. 智能电网环境下一种基于 SDKey 的智能移动终端远程证明方案[J]. 信息网络安全,2018(7):1-6.

[18] 余 容,黄 剑,何朝明. 基于 SM4 并行加密的智能电网监控与安全传输系统[J]. 电子技术应用,2016,42(11):66-69.

[19] 林静怀,米为民,李泽科,等. 智能电网调度控制系统的远方操作安全防误技术[J]. 电力系统自动化,2015,39(1):60-64.