一种适用于园区微电网的安全控制协议

陈艺琳,罗娇燕,胡逸芳,易传佳,左黎明
(华东交通大学 理学院,江西 南昌 330013)

摘 要:随着微电网技术的快速发展,微电网的控制研究成为当前的研究热点。针对当前园区微电网控制系统在数据交互过程中存在数据来源可靠性和数据完整性保护等问题,提出一种消息可恢复式数字签名方案。该方案与一般的数字签名方案相比具有能够减少通信量、降低通信代价的优点,适用于带宽有限,计算能力弱的应用场景中,可以有效地应用到园区微电网的控制系统中,并保持微电网运行的高效性。园区微电网的控制是保障园区稳定供电的重要组成部分,针对园区微电网控制系统的网络安全问题,以消息可恢复式的数字签名方案为基础,进一步提出一种适用于园区微电网的安全控制协议。最后通过 C#轻量级密码术包对安全控制协议的交互过程进行实验与仿真,实验结果表明该方案的签名过程耗时短,表明该安全控制协议在控制器端运行效率较高,可以有效提高园区微电网控制系统的安全性,可以为园区微电网的安全稳定运行提供有力保障。

关键词:园区微电网;微电网控制;消息恢复;数字签名;安全协议
中图分类号:TP309.2 **文献标识码**:A **文章编号**:1673-629X(2022)03-0120-06
doi:10.3969/j.issn.1673-629X.2022.03.020

A Security Control Protocol for Microgrid in Park

CHEN Yi-lin,LUO Jiao-yan,HU Yi-fang,YI Chuan-jia,ZUO Li-ming
(School of Science,East China Jiaotong University,Nanchang 330013,China)

Abstract:With the rapid development of microgrid technology,the research of microgrid control has become a hot topic. Aiming at the problems of data source reliability and data integrity protection in the process of data interaction in the current park microgrid control system,a digital signature scheme with message recovery is proposed. Compared with the general digital signature scheme,this scheme has the advantages of reducing communication traffic and communication cost,which is suitable for the application scenarios with limited bandwidth and weak computing power. Therefore,it can be applied to the efficient microgrid in the park and maintain the high efficiency of the operation of the microgrid. The microgrid control is an important part to ensure the stable power supply in the park. Aiming at the network security problem of the control system of the micromigrid and based on the signature scheme with message recovery,a security control protocol is proposed for the microgrid control system in the park. Finally,the security control protocol is simulated by Csharp lightweight cryptography package. Experimental results show that the security control protocol has the advantages of shorter time in scheme signature process and higher operation efficiency in the controller,which can improve the security of the microgrid control system in the park effectively,and can provide a strong guarantee for the security and stable operation of the microgrid in the park.

Key words:microgrid in the park;microgrid control;message recovery;digital signature;security protocol

0 引 言

随着风能、太阳能、天然气等清洁能源开发技术的不断突破,分布式电源[1]逐渐得到发展。分布式电源可以较好地避免集中供电技术存在的环境破坏和资源浪费问题。随着分布式电源并入到配电网中,为了有效提高分布式电源的利用效率,微电网[2-5]的概念被提出。微电网系统可以促进可再生能源的开发与利用,为负荷提供稳定可靠的电能。在微电网技术快速发展的背景下,面向园区的微电网[6-8]建设也在快速发展。稳定可靠的电力供应是园区正常生产和运营的重要保障,园区微电网的安全控制是保障园区正常运转的关键。微电网的控制成为近年来的研究热点[9-12],文献[13]针对微电网控制器成本高、集成度低等问题提出一种基于嵌入式系统的园区微电网中央

收稿日期:2021-02-25 **修回日期**:2021-06-28
基金项目:2021 国家级大学生创新创业计划训练项目(1500421076);国家自然科学基金项目(11761033);江西省科学技术计划项目(20192BBHL80004);江西省研究生创新项目(YC2019-S263);江西省教育厅科技项目(GJJ180323)
作者简介:陈艺琳(2000-),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,硕导,CCF 会员(E20-0013632M),研究方向为信息安全、大数据分析。

控制器,并验证了中央控制器的功能和能量管理策略具有较好的实用性。微电网的控制系统依赖于大量的数据采集与交互,在网络攻击层出不穷的互联网环境下,微电网的正常运营面临着网络攻击的威胁。2015 年和 2016 年末乌克兰曾发生由黑客组织进攻导致的大面积停电事故,2019 年 3 月委内瑞拉电网遭到网络攻击,导致全国 18 个州范围电力中断超过 24 小时。此类停电事故造成了巨大的经济损失,为避免此类事故的发生,相关网络安全研究者和电网机构开始对电网和微电网的安全性进行研究[14-16]。园区微电网的控制系统中,包含有园区大量电力设备的用电数据,攻击者一旦通过网络攻击手段窃取或篡改微电网数据,很可能使园区微电网以及其他生产设备发生故障,从而导致园区产生重大安全事故和经济损失。针对园区微电网控制系统中可能存在的信息安全问题,该文提出一种消息可恢复数字签名方案,并基于该方案设计一种适用于园区微电网的安全控制协议,在保证通信效率的前提下,有效保障微电网控制系统数据交互的安全性,保障园区微电网稳定运行。

1　相关基础

1.1　园区微电网控制系统

园区微电网是一个可以实现自我控制、保护和管理的自治系统,主要为商业园区或工业园区提供电能服务。

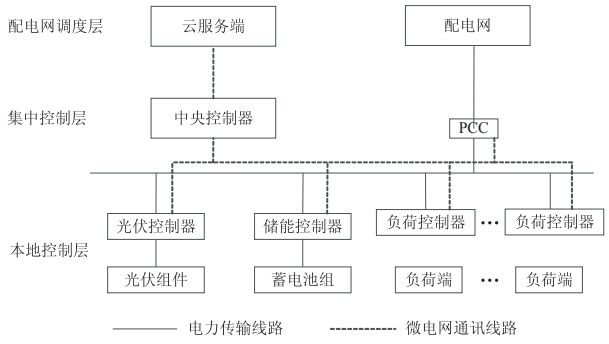

图 1　园区微电网系统结构

如图 1 所示,园区微电网主要包括光伏电源、储能装置、电力负荷等设备。园区微电网通过公共连接点(point of common coupling,PCC)与配电网连接,PCC 处的静态开关可以实现微电网在孤网和并网两种运行状态间的平滑切换。在该文所描述的园区微电网中,分布式能源为太阳能,光伏电源和储能装置负责对多个负荷端提供电能和电压支撑,这样可以有效节约从大电网购买电力而产生的经济成本,同时也有效降低了电力传输的负担。在大电网发生突发故障或电能质量不达标时,PCC 处的静态开关断开与配电网的连接,园区微电网从并网模式平滑切换至孤网模式独立运行,这种方式有效降低了由于主网故障带来的影响,提高了园区供电的可靠性与安全性,园区的正常运营也得到有效保障。

园区微电网的控制系统是整个园区微电网系统的核心部分,是维持园区微电网安全、稳定、高效运行的重要组成部分。目前主流的微电网控制系统为三层控制结构,分别为配电网调度层、集中控制层、本地控制层。控制系统由各部分控制装置组成,可实现分布式电源控制、储能装置控制、孤网并网切换控制、微电网电能管理以及微电网实时监控等。

(1)配电网调度层。

配电网调度层是一个云服务端,可以实时采集各个控制装置的数据,并将数据进行计算和分析。实时数据和计算分析结果可以在云服务端以图表等形式实时显示。云服务端根据计算分析结果给各个控制装置下达控制指令,同时也能接受上级配电网的调节控制指令,从微电网安全、经济运行的角度协调和调度微电网。

(2)集中控制层。

集中控制层是微电网的控制中心,也是整个微电网控制系统的核心部分,主要控制装置为中央控制器。中央控制器对分布式电源、储能装置、各个负荷的运行数据进行实时采集,对它们的运行状态进行实时监控,并对采集的数据进行计算与分析,得出微电网的实时运行状态。中央控制器可以接受配电网调度层的控制指令给出相应的控制动作。中央控制器根据实时运行状态,实时优化控制策略,控制分布式电源、储能装置、负荷的启动和停止,实现微电网并网状态、孤网状态的平滑切换,保障微电网稳定运行。

(3)本地控制层。

本地控制层由分布式电源控制器、储能控制器、负荷控制器等控制设备组成,接受集中控制层的控制指令,同时通过分布式电源控制器调节分布式电源,通过储能控制器实现储能装置的充放电控制,通过负荷控制器实现对负荷的控制。

在园区微电网的运行过程中,配电网调度层、集中控制层和本地控制层自上而下通过通信向下发送控制指令。在这个过程中存在网络攻击威胁的根源主要在于数据来源缺乏安全认证,该文提出的适用于园区微电网的安全控制协议基于消息可恢复签名方案,可以通过数字签名对数据来源进行安全认证,保障数据传输的可靠性。

1.2　消息可恢复签名方案

消息可恢复的签名方案由系统初始化、密钥生成、签名和验证签名四个算法组成,具体描述如下:

(1)系统初始化:给定安全参数,输出系统参数,

公开系统参数。

(2)密钥生成:根据公开的系统参数,生成用户的私钥,并计算系统公钥。

(3)签名:输入系统参数和用户私钥,输出签名,并发给验证者。

(4)验证签名:输入系统参数、签名,输出验证结果,“TRUE”或者“FALSE”,输出恢复的完整消息。

在园区微电网控制系统中,云服务端为签名验证者,中央控制器可以生成私钥并定期更新私钥。中央控制器发送数据封包时,先对数据封包进行签名,然后发送给云服务端,当云服务端对签名信息进行验证,验证成功则输出恢复的完整消息,验证失败则发出警告信息。

2 消息可恢复签名方案构造

基于椭圆曲线上离散对数问题的难解性,提出一种消息可恢复签名方案。为了方便方案描述,首先给出一些常用符号,符号对照如表 1 所示。

表 1 符号说明

符号	意义
$a \mid\mid b$	表示 a 和 b 两个字符串的连接
$\oplus$	表示二进制系统中的异或运算
$\{0,1\}^n$	表示长度为 n 的二进制串
$\{0,1\}^*$	表示任意长度二进制串
$[\alpha]_L$	表示 α 的最低 L 比特
$[\alpha]_R$	表示 α 的最高 R 比特

下面给出方案的详细描述,方案主要由四个算法构成,具体描述如下:

(1)系统初始化。

给定一个安全参数 k,选择椭圆曲线上 q(q 为大素数)阶循环群 G,其中 P 是 G 的生成元。选择一个安全的抗碰撞的哈希函数:$H:\{0,1\}^* \rightarrow Z_q^*$。公开参数 params = $\{k,G,P,H\}$。

(2)密钥生成。

用户随机选取 $x_1,x_2 \in Z_q^*$,计算 $y_1 = x_1P$,将(x_1,y_1)作为私钥,然后计算 $y_2 = x_2P$,将(x_2,y_2)作为公钥。

(3)签名。

对任意给定的消息 $m \in \{0,1\}^n$ 进行签名,随机选择 $r \in Z_q^*$,依次计算:

$$K = x_1y_2 \tag{1}$$

$$R = rP \tag{2}$$

$$h_1 = H(m) \mid\mid H(H(m)) \oplus m \tag{3}$$

$$h_2 = H(K,R) \tag{4}$$

$$s = h_1 \oplus h_2 \tag{5}$$

$$e = sx_1 + r \bmod q \tag{6}$$

则(e,s)为消息 m 的签名。

(4)签名验证。

对给定消息 m 的签名(e,s),验证签名的过程如下:

①依次计算:

$$R = eP - sy_1 \tag{7}$$

$$K = x_2y_1 \tag{8}$$

$$h_2' = H(K,R) \tag{9}$$

②计算 $h_1' = h_2' \oplus s$,分离 $h_1' = [h_1']_L \mid\mid [h_1']_R$,得到两个二进制串 $[h_1']_L$ 和 $[h_1']_R$,恢复消息 $m' = H([h_1']_L) \oplus [h_2']_R$。

③验证等式 $[h_1']_L = H(m')$,若等式成立,则接受签名(e,s) 以及可恢复消息 m'。正确情况下,$[h_1']_L = H(m)$,$[h_1']_R = H(H(m)) \oplus m$。

整个签名验证和消息恢复过程正确性证明如下:

$$R = eP - sy_1 = sx_1P + rP - sx_1P = rP \tag{10}$$

$$K = x_2y_1 = x_2x_1P = x_1y_2 \tag{11}$$

$$h_1' = h_2' \oplus s = h_2' \oplus h_1 \oplus h_2 \tag{12}$$

由于 $h_2' = h_2 = H(K,R)$,故:

$$h_1' = h_1 = H(m) \mid\mid H(H(m)) \oplus m \tag{13}$$

$$[h_1']_L = H(m) \tag{14}$$

$$[h_1']_R = H(H(m)) \oplus m \tag{15}$$

$$m' = H([h_1']_L) \oplus [h_1']_R = H(H(m)) \oplus H(H(m)) \oplus m = m \tag{16}$$

3 安全控制协议设计

3.1 安全控制系统结构

在微电网系统中,中央控制器与云服务端的安全控制架构如图 2 所示。在中央控制器中集成了数据采集模块、数据处理模块和签名模块,云服务端由身份认证模块、信息处理模块组成。

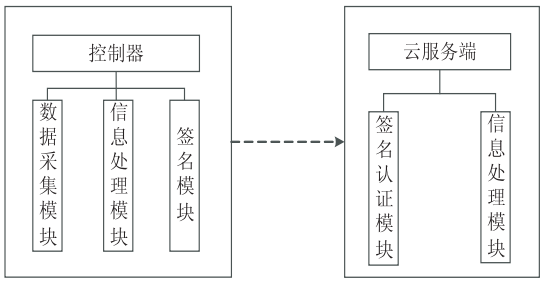

图 2 微电网安全控制系统结构

在中央控制器中,数据采集模块负责微电网数据的采集,信息处理模块负责数据格式的处理,将数据处理为规范的消息封包,签名模块负责对消息封包进行签名。在云服务端,信息处理模块负责对接受到的消息封包进行解析,签名验证模块负责对中央控制器发

送过来的签名进行验证及消息恢复。

3.2　安全协议设计

安全协议的交互过程如图 3 所示。

步骤 1:数据采集模块采集实时数据,得到数据系列 data1,data2,data3 等。

步骤 2:数据采集模块将采集的数据系列 data1,data2,data3 发送到信息处理模块。

步骤 3:信息处理模块接收到数据后,将数据处理成 data1 * data2 * data3 的封包格式,然后发送到签名模块。

步骤 4:签名模块接收到消息封包后,调用签名算法得到签名 Sig。

步骤 5:签名模块将签名结果 Sig 发送到云服务端。

步骤 6:云服务端接收到消息封包后,签名验证模块调用签名验证算法对消息封包进行签名验证,验证通过则恢复消息,并把消息发送到信息处理模块,验证不通过则发出警告信息。

步骤 7:信息处理模块对消息封包进行解析,获得原始数据。

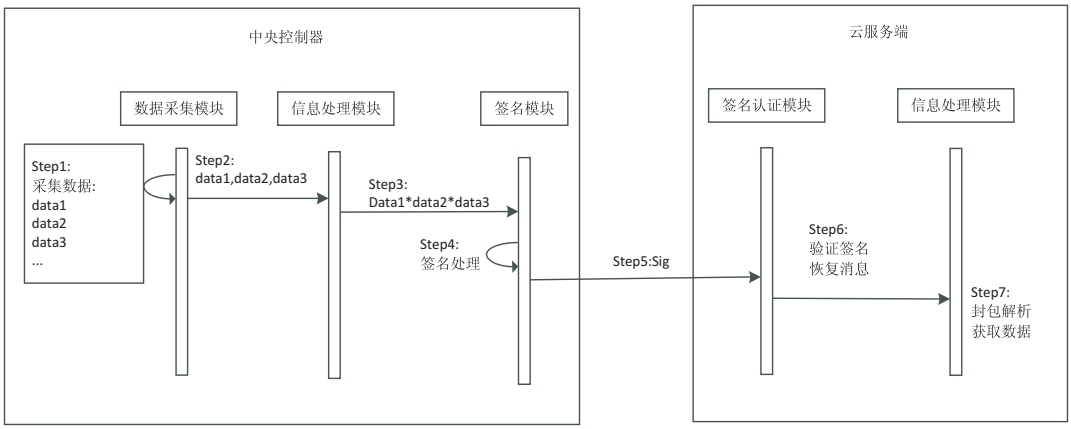

图 3　协议交互流程

4　安全性分析

4.1　数据机密性

当控制器与云服务端进行通信时,攻击者可以对通信数据进行监听。当通信数据以明文数据传输时,攻击者可以窃取通信双方的通信具体内容。在安全控制协议中,控制器会先将通信数据进行签名处理再发送签名,云服务端对签名进行验证,然后通过签名进行消息恢复。通信的报文内容只含有签名数据,不包括原始消息,原始消息不会暴露在通信过程中,从而保证了数据的机密性。

4.2　数据完整性

信息的完整性是指在存储或传输信息的过程中,原始的信息不能允许被随意更改。篡改攻击是破坏数据完整性最常见的方法之一,篡改攻击是指攻击者对拦截到的报文进行篡改,将篡改后的报文进行发送达到攻击目的。在安全控制协议中,当攻击者对报文进行篡改并发送到服务端后,由于报文已经被篡改,服务端进行签名验证时会验证失败,无法对消息进行恢复。从而使得协议可以抵抗篡改攻击,确保数据的完整性。

4.3　数据不可否认性保护

在网络通信中,攻击者常常利用冒充、伪造等方法向接收方发送报文,在安全控制协议中,采用了消息可恢复式签名技术,服务端可以根据公开参数签名者公开的公钥对接收到的报文进行签名验证,可以有效地保障数据来源的可靠性。

5　实验仿真

在 Windows7 64 位操作系统 Microsoft Visual Studio 2012 微软平台下,采用 C#轻量级密码术包(bouncy castle)实现了文中方案。实验结果显示该方案签名所消耗时间为 0.010 秒,验证所消耗时间为 0.219 秒。实现结果如图 4 所示。

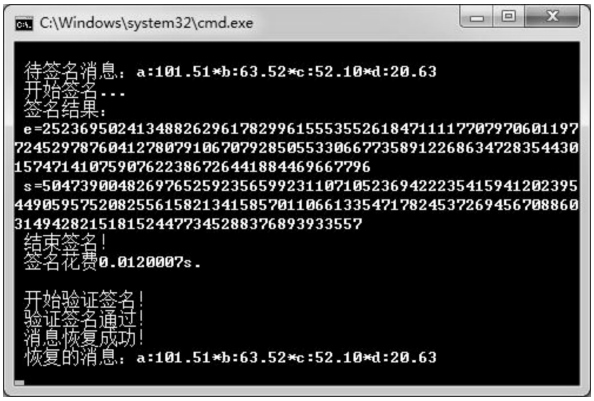

图 4　实验结果

5.1　签名生成过程

在中央控制器中,首先对采集的数据进行封包处理,然后通过该签名方案对数据封包进行签名处理,核心代码如下:

```
ecc myecc=new ecc();
ECPoint y1=myecc.ecc_point_g.Multiply(x1);
ECPoint y2=myecc.ecc_point_g.Multiply(x2);
ECPoint K=y2.Multiply(x1);
ECPoint R=myecc.ecc_point_g.Multiply(r);
hash myhash=new hash();
byte[] hm=myhash.TanGetDigestByteArray(m);
//计算 H(H(m))
byte[] hhm=myhash.TanGetDigestByteArray(hm);
//计算 H(H(m))⊕m
byte[] hmxor=HexXorByte(hhm, m);
//计算 h1
byte[] h1=new byte[64];
Array.Copy(hm, 0, h1, 0, 32);
Array.Copy(hmxor, 0, h1, 32, 32);
//计算 h2
string KK=K.X.ToBigInteger().ToString()+K.Y.ToBigInteger().ToString();
string RR=R.X.ToBigInteger().ToString()+R.Y.ToBigInteger().ToString();
string KR=KK+RR;
byte[] h2=myhash.TanGetDigestByteArray512(KR);
//计算 s=h1⊕h2
byte[] ss=HexXorByte(h1, h2);
//计算 e
BigInteger s=new BigInteger(ss);
BigInteger sx1=s.Multiply(x1);
BigInteger e=sx1.Add(r.Mod(myecc.ecc_n));
```

5.2 签名验证过程

在云服务端,接收到中央控制器发送过来的数据封包后,根据该签名方案的签名验证算法对签名进行验证,核心代码如下:

```
ECPoint ep=myecc.ecc_point_g.Multiply(e);
ECPoint sy1=y1.Multiply(s);
ECPoint R1=ep.Subtract(sy1);
ECPoint K1=y1.Multiply(x2);
string KK1=K1.X.ToBigInteger().ToString()+K1.Y.ToBigInteger().ToString();
string RR1=R1.X.ToBigInteger().ToString()+R1.Y.ToBigInteger().ToString();
string KR1=KK1+RR1;
byte[] H2=myhash.TanGetDigestByteArray512(KR1);
byte[] H1=HexXorByte(H2, ss);
byte[] H1L=new byte[32];
byte[] H1R=new byte[32];
Array.Copy(H1, 0, H1L, 0, 32);
Array.Copy(H1, 32, H1R, 0, 32);
byte[] HL=myhash.TanGetDigestByteArray(H1L);
//恢复消息 m
byte[] m1=HexXorByte(HL, H1R);
byte[] left=H1L;
byte[] right=myhash.TanGetDigestByteArray(m1);
if (ByteEquals(left,right))
{
    Console.WriteLine("验证签名通过!");
    Console.WriteLine("消息恢复成功!");
    Console.WriteLine("恢复的消息:{0}", Encoding.UTF8.GetString(m1));
}
else
{
    Console.WriteLine("验证签名失败! 消息恢复失败!");
}
```

5.3 协议性能分析

在 Windows7 64 位操作系统 Microsoft Visual Studio 2012 微软平台下,采用 C#轻量级密码术包(bouncy castle)运行文献[16-20]中方案对应的协议,分别运行 100 次,计算签名过程与验证签名的平均耗时并进行比较,各协议签名过程与验证签名的平均耗时如图 5 所示。

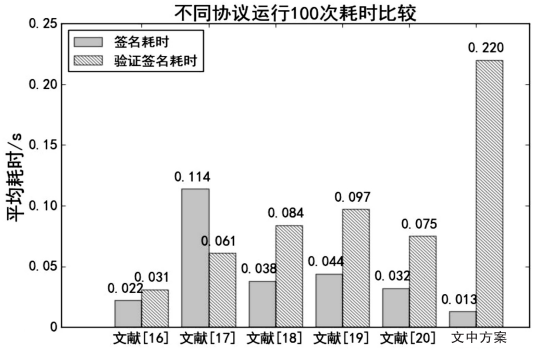

图 5 不同协议运行 100 次平均耗时比较

在签名过程中,文献[16]对应协议的签名过程平均耗时 0.022 秒,文献[17]平均耗时 0.114 秒,文献[18]平均耗时 0.038 秒,文献[19]平均耗时 0.044 秒,文献[20]平均耗时 0.032 秒,文中方案签名过程平均耗时为 0.013 秒。相比其他协议,文中方案的安全控制协议在签名效率方面存在优势。

在验证签名过程中,文中方案的验证签名过程平均耗时为 0.22 秒,相比文献[16-20]的验证签名过程平均耗时都要高,这是由于验证签名的过程不仅需要签名的验证,而且需要消息的恢复,其计算复杂程度高于签名过程。

综合来看,文中方案协议的签名过程运行效率较高,适合在计算能力差的设备上运行,验证签名过程运行效率一般,需要在计算能力高的设备上运行。在安全控制协议中主要针对的是中央控制器的性能,在中央控制器上进行的为签名过程,验证签名在云服务端

进行。在微电网控制系统的结构中,中央控制器受限于设备本身,在中央控制器运行的协议需要较高的运行效率,而云服务端采用的服务器集群,计算能力很高。因此,文中方案的签名过程运行在中央控制器,验证签名过程运行在云服务端,可以保障协议的安全高效运行。

6　结束语

针对当前园区微电网控制系统在数据交互过程中存在安全性认证和数据完整性保护问题,提出了一种消息可恢复的数字签名方案,并进一步设计了一种适用于园区微电网的安全控制协议。对安全控制协议进行了实验与仿真,结果表明该方案在控制器端的效率较高。该方案应用到园区微电网的控制系统中,可以提高系统的安全性,保障园区微电网的安全稳定运行。

参考文献:

[1] 罗　迪,田新首,刘　超,等. 分布式清洁电源接入配电网研究综述[J]. 电网与清洁能源,2017,33(8):101-108.

[2] LASSETER R H. Microgrids[C]//Proceedings of IEEE power engineering society winter meeting. New York,USA: IEEE,2002:305-308.

[3] OLIVARES D E, MEHRIZI-SANI A, ETEMADI A H,et al. Trends in microgrid control[J]. IEEE Transactions on Smart Grid,2014,5(4):1905-1919.

[4] 鲁宗相,王彩霞,闵　勇,等. 微电网研究综述[J]. 电力系统自动化,2007,31(19):100-107.

[5] 孟　明,陈世超,赵树军,等. 新能源微电网研究综述[J]. 现代电力,2017,34(1):1-7.

[6] 刘敦楠,徐尔丰,许小峰. 面向园区微网的"源-网-荷-储"一体化运营模式[J]. 电网技术,2018,42(3):681-689.

[7] 张世翔,吕帅康. 面向园区微电网的综合能源系统评价方法[J]. 电网技术,2018,42(8):2431-2438.

[8] 田　军,刘征宇,舒　军,等. 适用于工业园区的微电网系统能量管理[J]. 电力自动化设备,2016,36(11):45-50.

[9] 陈　新,姬秋华,刘　飞. 基于微网主从结构的平滑切换控制策略[J]. 电工技术学报,2014,29(2):163-170.

[10] 窦春霞,李　娜,徐晓龙. 基于多智能体系统的微电网分散协调控制策略[J]. 电工技术学报,2015,30(7):125-134.

[11] 顾　伟,薛　帅,王　勇,等. 基于有限时间一致性的直流微电网分布式协同控制[J]. 电力系统自动化,2016,40(24):49-55.

[12] 王成山,李　微,王议锋,等. 直流微电网母线电压波动分类及抑制方法综述[J]. 中国电机工程学报,2017,37(1):84-97.

[13] 丁　明,程　清,李　林,等. 一种基于嵌入式系统的园区微电网中央控制器设计[J]. 电力系统保护与控制,2019,47(6):158-165.

[14] 马　良,许　刚. DoS 攻击下基于自触发一致性的微电网电压无功控制[J]. 计算机工程,2020,46(9):298-305.

[15] 席　禹,邹俊雄,蔡泽祥,等. 基于报文识别与流量管控的智能变电站保护控制信息安全防护方法[J]. 电网技术,2017,41(2):624-629.

[16] 左黎明,张梦丽,丁仕晗,等. 微电网 SCADA 系统中具有消息恢复的身份认证协议[J]. 电网技术,2019,43(12):4299-4305.

[17] LI M, FANG T. Provably secure and efficient ID-based strong designated verifier signature scheme with message recovery[C]//2014 17th international conference on network-based information systems. Salerno, Italy: IEEE Computer Society,2017:287-293.

[18] VERMA G K,SINGH B B,SINGH H. Provably secure message recovery proxy signature scheme for wireless sensor networks in e-healthcare[J]. Wireless Personal Communications,2018,99(1):539-554.

[19] SARDEP P,BANERJEE A. A secure id-based proxy signature scheme from bilinear pairing[J]. International Journal of Computer Applications,2015,124(9):1-4.

[20] KARATI A,ISLAM S H,KARUPPIAH M. Provably secure and lightweight certificateless signature scheme for IIoT environments[J]. IEEE Transactions on Industrial Informatics,2018,14(8):3701-3711.