文章编号:1671-4598(2019)04-0240-05 DOI:10.16526/j.cnki.11—4762/tp.2019.04.052 中图分类号:TN915.08 文献标识码:A

基于联盟区块链的 V2G 网络跨域认证技术研究

刘冬兰[1],刘 新[1],陈剑飞[2],于 淼[1],张 昊[1]
(1. 国网山东省电力公司 电力科学研究院,济南 250003;2. 国网山东省电力公司,济南 250001)

摘要:针对车辆到电网(Vehicle—to—Grid,V2G)网络所面临的安全威胁,分析了 V2G 多域网络架构,给出了一个适用于该架构的网络信任模型;基于联盟区块链提出一种 V2G 网络跨管理域认证方案,通过本域用户与外地域服务器以及外地域服务器与其域内用户的认证实现域间用户双向认证;该方案利用区块链所具有的不易篡改特性,在数字身份验证环节采用哈希算法减少方案中的签名与验证次数,提高了方案的效率和可扩展性;该认证方案中的签名采用基于身份的密码算法 SM9,在适应性选择消息攻击下具有存在性不可伪造安全。

关键词:智能电网;电动汽车加入电网;联盟区块链;跨域认证

A Cross—Domain Authentication Technology Based on Consortium Blockchain in V2G Networks

Liu Donglan[1], Liu Xin[1], Chen Jianfei[2], Yu Hao[1], Zhang Hao[1]
(1. State Grid Shandong Electric Power Research Institute, Jinan 250003, China;
2. State Grid Shandong Electric Power Company, Jinan 250001, China)

Abstract: In view of the security threats faced by the vehicle—to—grid (V2G) network, this paper analyzes the V2G multi—domain network architecture and presents a network trust model suitable for the architecture. Based on the consortium blockchain, a cross—domain V2G authentication scheme is proposed, which achieves inter—domain user mutual authentication through the authentication between the domain user and the foreign domain server, and between the foreign domain server and its intra—domain users. The scheme utilizes the non—tampering characteristic of the blockchain, and adopts a hash algorithm in the digital identity verification to reduce the number of signatures and verifications in the scheme, thereby improving the efficiency and scalability of the scheme. The signature in the authentication scheme adopts the identity—based cryptographic algorithm SM9, and has the existence of unforgeable security under the adaptive selection message attack.

Keywords: smart grid; vehicle—to—Grid; consortium blockchain; cross—domain authentication

0 引言

随着全球电动汽车的迅猛发展,车辆到电网(Vehicle—to—Grid,V2G)已被视为智能电网的重要组成,受到产业界和学术界越来越多的关注[1-2]。V2G 技术可以根据电力系统的供应和需求灵活地充电或放电,既能缓解电动汽车规模发展面临的充电压力,又可将其作为移动的、分布式储能单元,旋转备用,削峰填谷,使可再生能源更好地整合,增强电网稳定性。但 V2G 同时具有电流和信息流的实时双向性,在交互过程中也不可避免地面临着各种安全威胁[3-4]。考虑电动汽车具有快速移动特性,因此,研究安全高效的跨域认证协议对 V2G 具有重要的意义。

学术界目前对 V2G 网络认证主要关注于用户身份的隐私保护。2011 年,Yang 等人首次提出使用假名技术实现 V2G 匿名认证[5]。随后一些学者提出了基于假名的 V2G 匿名认证方案[6-7],但这些方案需要对假名进行定期更换,维持假名数据库,系统开销比较大。基于群签名、盲签名和签密的 V2G 网络匿名认证方案也先后被提出[8-10]。这些方案都需要大量的通信和计算开销,要么需要高额的管理费用,要么在操作上有所限制,很难用于实际,尤其是大群组应用场景。考虑 V2G 中车辆可移动的特点,Vaidya 等人最早提出 V2G 网络的多域网络架构[11],该方案构建了一个基于混合公钥基础设施的模型,通过域内和域间数字身份建立节点间信任关系,支持点对点的跨域认证。此后陆续有一些具有隐私保护特性的 V2G 跨域认证方案被提出[12-13]。

以上 V2G 跨域认证方案均采用中心化模式,随着设备数量的增加,海量设备接入时汇聚效应将造成认证服务器拥塞,形成信令数据风暴,导致认证时延急剧增加。区块链技术具有去中心化、可追溯性、公开透明、不可篡改、交易匿名、共识机制等特点[14],与 V2G 的移动、分布式特点相吻合。区块链技术的引入可以在去中心化、可信任方向上发挥重要作用[15-16],其在认证上的应用开始受到学者关注[17-19]。本文将基于联盟区块链和 SM9 数字签名算法[20]提出一种 V2G 网络跨管理域认证方案,进一步改善 V2G 认证的效率和可扩展性。

收稿日期:2019-02-10; **修回日期**:2019-02-24。
基金项目:国网山东省电力公司科技项目(52062617002V)。
作者简介:刘冬兰(1987-),女,云南宣威人,硕士,高级工程师,主要从事网络安全,大数据,区块链等技术方向的研究。

1　联盟区块链及 V2G 网络架构

1.1　联盟区块链的概念及应用

区块链是一个去中心化的分布式数据库，依据访问以及管理的权限，区块链可以分为公有链、私有链、联盟链。联盟区块链又称共同体区块链，简称“联盟链”。联盟链指的是在共识的过程当中受制于预选节点的区块链，简单来说就是有若干个机构共同参与管理的区块链，每个机构都运行着一个或多个节点，其中的数据只允许系统内不同的机构进行读写和发送交易，并且共同来记录交易数据。

目前，世界上各行各业开始密切关注区块链技术，并且不少金融企业基于区块链可以减少成本、提升效率的优点，把其运用到各企业的发展当中，但是在金融企业的某些场景中由于区块链数据的完全公开透明，不能直接应用全网记账的公有链技术，因此，以联盟链为目标的区块链项目不断涌现。一些专家学者表示，整个社会中，联盟区块链其实更有前景，因为它更好的发挥互联网的互联互通，共享信息的作用，它的意义在于让大家达成了共识，同时促成更快的建立生态联盟，更好的利用区块链技术去改变工作模式和生活模式。并且，联盟链可以使交易数据及隐私得到保护。

联盟区块链技术作为新兴的分布式数据库技术，在未来的能源互联网中应用潜力很大[21-24]。在能源互联网行业，联盟区块链主要应用于智能电网数据安全存储与共享、分布式能源交易认证、大用户直购电等方面，通过联盟区块链技术实现了安全、有效的数据存储与共享，提高了分布式能源交易数据安全性、信息透明度和自动化认证水平。

1.2　V2G 网络架构

V2G 技术通过专门设计的双向充电站工作，这些充电站允许电动车辆所有者为他们的汽车充电，同时还便于车辆电池的放电。我们将充电站按地理区域进行划分，每个区域有一个密钥生成中心（Key Generation Center，KGC），用于建立管理域内或域间的信任关系，并使用 KGC 来传递消息。为解决多个管理域内或域间的跨域身份认证问题，本文提出一种跨域环境下的 V2G 网络信任模型。假定这样的应用场景：归属地是陕西省的电动汽车 U_A 对应的管理域为 A，到达山东省接入电网时，需要在山东省的管理域 B 内进行身份认证。陕西省电网和山东省电网分属于两个域（A 和 B），本文关注于跨域认证的系统模型，该信任模型如图 1 所示。

图 1 中不同域的 KGC 由矩形框表示，而域内用户则由 EV（电动汽车，Electric Vehicle）表示。为实现跨域身份认证，本地域和外地域间不同域的 KGC 经过许可后便加入联盟链，构成联盟链的验证节点 VP（Vaildating Peer，VP）。

在本文中，利用联盟区块链不易篡改的特性和哈希算法高效的签名验证方法，基于联盟区块链提出一种 V2G 网络跨管理域认证方案。本方案中，加入联盟链的密钥生成中心 KGC 是可信的，为验证节点 VP 生成区块链数字身份，

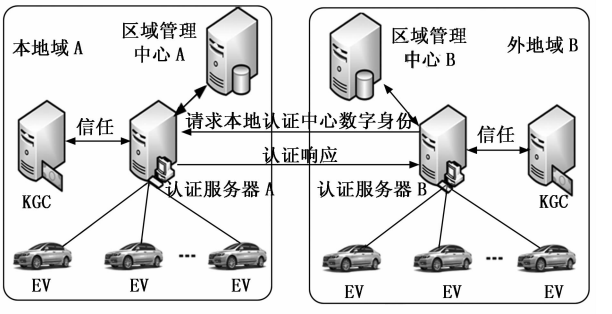

图 1　V2G 网络跨域信任模型

并将数字身份进行哈希计算后存储到不易被篡改的区块链内，并将哈希值作为各管理域的信任身份凭证。如果一个管理域不可信或者不需要跨域需求，则撤销加入该联盟链的许可，实现盟员的退出。在图 1 中，联盟链上有 2 个不同区域的 KGC，分别记为本地域 KGC_A、外地域 KGC_B，它们作为联盟链的验证节点。

2　基于联盟链的认证协议设计

本节给出一种基于联盟区块链的智能电网中 V2G 跨域认证协议，该协议假定这种情况：由于联盟链的身份准入机制，加入联盟链的域是可信的，以 A、B 两域为例作跨域认证。

本协议设计中用到的数字签名方案为国密标准 SM9，相关参数设置标准详见文献[20]。SM9 是我国国家密码管理局于 2016 年 3 月发布的一种基于身份的密码标准，对应的标准为“GM/T 0044－2016 SM9 标识密码算法”。SM9 包括数字签名算法、密钥协商协议以及密钥封装机制和公钥加密算法。下文中出现的主要符号含义如表 1 所示。

表 1　符号含义

符号	含义
G_1，G_2	阶为素数 N 的加法循环群
G_T	阶为素数 N 的乘法循环群
e	$G_1 \times G_2 \rightarrow G_T$ 的双线性映射
P_1	群 G_1 的生成元
P_2 群 G_2 的生成元	
$H_1(\cdot)$，$H_2(\cdot)$	由密码杂凑函数派生的密码函数

电动汽车 U_A 在接入电网前，先在归属地 A 的认证服务器注册个人信息并获得相应的公私钥对 PK_A 和 SK_A。U_A 将身份信息 ID_A、公钥 PK_A、时戳 t_A 和有效期 T（设为比特串 $m_A = ID_A \| PK_A \| t_A \| T$），以及对 m_A 的签名发送给区域管理中心 R_A，R_A 包含该区域的密钥生成中心 KGC_A。R_A 验证 U_A 身份的合法性，并为 U_A 计算用户的签名主公钥 P_{pub-sA} 和签名私钥 ds_A，计算过程如算法 1 所示。

算法 1：用户签名公私钥的计算算法

输入：(N, P_2, ID_A, H_1)，输出：(P_{pub-sA}, ds_A, hid)

1：随机产生随机数 $ks \in [1, N-1]$；

2：计算群 G_T 中的元素 $P_{pub-sA} = [ks] P_2$；

3：选择函数识别符 hid，计算有限域 F_N 中的元素 $t_1=H_1(ID_A\|\|hid,N)+ks$；

4：若 $t_1=0$ 返回至步骤 1，否则进入步骤 5；

5：计算 $t_2=ks\cdot t_1^{-1}\bmod N$；

6：计算 $ds_A=[t_2]P_1$；

7：结束。

区域管理中心 R_A 将 U_A 的区块链数字身份 $BID_{U_A-CA_A}$ 以及 U_A 的签名主公钥 P_{pub-sA} 和签名私钥 ds_A 发给 U_A，并将相应的身份信息和 $BID_{U_A-CA_A}$ 存于区块链和数据库中。用户 U_A 在 A 域接入电网时，区域管理中心 R_A 在区块链上查询 Hash（$BID_{U_A-CA_A}$）的值，当查询结果为 $issue$ 时，允许 U_A 接入电网。U_A 在接入 B 域电网前需先向 B 域认证服务器 S_B 发出访问 S_B 的请求，S_B 收到用户 U_A 的请求后，向 A 域用户 U_A 发送随机数 M 和时戳 t_B，用户 U_A 对随机数 M、数字身份 $BID_{U_A-CA_A}$ 和时戳 t_B 进行签名得到签名值 (h,S)，计算过程如算法 2 所示。

算法 2：用户签名算法

输入：$(M,t_B,P_{pub-sA},BID_{U_A-CA_A},ds_A)$，输出：$(h,S)$

1：计算群 G_T 中的元素 $g=e(P_1,P_{pub-sA})$；

2：产生随机数 $r\in[1,N-1]$；

3：计算 $w=g^r\in G_T$，转换 w 比特串；

4：计算整数 $h=H_2(M\|t_B\|BID_{U_A-CA_A}\|w,N)$；

5：计算 $l=(r-h)\bmod N$，若 $l=0$ 跳回步骤 2，否则转入步骤 6；

6：计算 $S=[l]ds_A\in G_1$；

7：结束。

A 域用户 U_A 响应 B 域认证服务器 S_B 的请求，把签名主公钥 P_{pub-sA}、随机数 M、数字身份 $BID_{U_A-CA_A}$、时戳 t_B 和签名(h,S) 作为消息发送给 B 域认证服务器 S_B。S_B 接收到消息后根据算法 3 验证签名 (h,S)，以确定随机数 M 是否有效。

算法 3：签名验证算法

输入：$(M,t_B,ID_A,P_{pub-sA},BID_{U_A-CA_A},hid,(h,S))$，

输出：(○，⊥)

1：检查 $h\in[1,N-1]$ 是否成立，若失败输出⊥，跳转至步骤 11；否则转入步骤 2；

2：对 S 进行数据类型转换，映射为椭圆曲线上的点，判断是否有 $S\in G_1$。若为否则输出⊥，跳转至步骤 11；否则转入步骤 3；

3：计算群 G_T 中的元素 $g=e(P_1,P_{pub-sA})$；

4：计算群 G_T 中的元素 $t=g^h$；

5：计算 $h_1=H_1(ID_A\|\|hid,N)$；

6：计算群 G_2 中的元素 $P=[h_1]P_2+P_{pub-sA}$；

7：计算群 G_T 中的元素 $u=e(S,P)$；

8：计算群 G_T 中的元素 $w'=u\cdot t$，将 w' 的数据类型转换为比特串；

9：计算整数 $h_2=H_2(M\|\|t_B\|\|w',N)$；

10：检验 $h_2=h$ 是否成立，若成立输出○；否则输出⊥；

11：结束。

B 域认证服务器 S_B 在签名验证算法输出为○时向 A 域认证服务器 S_A 发送请求和随机数 n，申请得到 A 域信任锚 KGC_A 的区块链数字身份 BID_{KGC_A}。S_A 收到请求及随机数 n，将 A 域信任锚 KGC_A 的区块链数字身份 BID_{KGC_A} 和随机数 n 作为消息发送给 S_B。S_B 随后根据算法 4(表 5) 生成跨域区块链数字身份，并发送给用户 U_A。A 域对 B 域的认证同样可以利用算法 4 完成，达到双向认证。

算法 4：跨域数字身份生成算法

输入：(n，BID_{KGC_A}，$BID_{U_A-CA_A}$)，输出：(○，⊥)

1：检查随机数 n 是否依然有效，若无效输出⊥，跳转至步骤 7，否则转入步骤 2；

2：在区块链上查询 Hash（BID_{KGC_A}）的值；

3：（1）若在区块链上查询哈希值的结果为空，即 Hash（BID_{KGC_A}）=null，则由于本地域 A 域认证服务器提供的信任锚 KGC_A 区块链数字身份不正确，认证失败，输出⊥，进入步骤 7；

（2）若在区块链上查询哈希值的结果为 revoke 和 issue，即 Hash（BID_{KGC_A}）=revoke and issue，则由于 A 域信任锚 KGC_A 的区块链数字身份已经变成撤销状态，认证失败，输出⊥，进入步骤 7；

（3）若在区块链上查询哈希值的结果只有且仅有 issue，即 Hash（BID_{KGC_A}）=issue，则 A 域信任锚 KGC_A 的区块链数字身份为已发布状态，认证成功，输出○，进入步骤 4；

4：向 B 域信任锚 KGC_B 发送用户 U_A 的数字身份 BID_{CA_A}；

5：KGC_B 解析 BID_{CA_A}，生成 U_A 的跨域区块链数字身份 $BID_{U_A-CA_A\cdot CA_B}$，发送给 S_B，并记入区块链；

6：发送域区块链数字身份 $BID_{U_A-CA_A\cdot CA_B}$ 给用户 U_A；

7：结束。

需要指出的是，为确保安全当 U_A 再次进入 B 域时需要重新认证。如果此时的区块链数字身份 $BID_{U_A-CA_A\cdot CA_B}$ 在有效期内，用户 U_A 将跨域区块链数字身份 $BID_{U_A-CA_A\cdot CA_B}$ 直接发给 B 域认证服务器 S_B，由 S_B 作哈希运算，并查询区块链数字身份值，进而对数字身份有效性进行验证。

3 安全性与效率分析

3.1 安全性分析

在本文中，用户在归属的管理域内可通过域内认证的方式完成用户和归属认证服务器之间的双向身份认证。在多个管理域间联盟区块链的架构下，认证服务器通过发起请求来获得待认证域的根 KGC 区块链数字身份，通过计算 Hash 值，并对区块链内已保存的信任凭证进行查询，对比 Hash 值是否相同来确定信任关系，进而可实现本地用户与外地域的服务器的双向身份认证。因此，本文的方案支持的认证类型包括本地域用户与外地域服务器间的认证、外

地域服务器与其域内用户间的认证，从而达到两个管理域间用户的跨域双向身份认证。

本文方案将对各个管理域内用户的数字身份进行哈希运算，再将数字身份的哈希值存入联盟区块链中，同时提交哈希值存储至区块链的对应时间信息与有效期，为数字身份文件的存在性与所有权提供证明。哈希函数具有单向性和抗碰撞性，能够使任何区块链节点匿名和安全地存储信任凭证。方案中的签名和认证中采用了 SM9 国密密码算法，可提供身份认证、抗否认性、完整性和保密性，在基于身份的适应性选择消息攻击下满足存在性不可伪造[20]。依照 SM9 算法标准中推荐的参考曲线，其安全强度等效于 RSA－3072bit。根据评估，理论上破解系统的复杂度相当于 2500 亿台电脑 10 亿年的计算量[25]。

联盟区块链使用时间戳和数字密码技术，把传递的消息记载在按时间序列组成的数据区块中，并使用共识机制把数据存储到分布式数据库中，从而生成了永久保存、不可逆向篡改的唯一数据记录，达到不依靠任何中心机构而实现可信交易的目的。本文方案在传递消息时附加了一个随机数，保存在询问服务器内，各个管理域内的电动汽车用户在验证对方的反馈信息之前，通过验证本地域用户接收到的随机数与原服务器保存的随机数的一致性达到抗重放攻击的目的。在验收消息时，由于时戳在传递的消息中无法被篡改，如果网络攻击者利用截获的消息去验证电动汽车用户的身份时，由于时戳失效导致消息验证失败，所以本文方案能够很好地抵抗重放攻击。通过在认证协议中设置有效期，在认证之前首先核对信息是否在有效期内，起到防止拒绝服务攻击的效果。本地域用户和外地域用户在交互时，由于双方用户都是使用自己的私钥进行签名验证消息，若攻击者对传递的消息进行篡改，则发送方的签名信息不能通过接收方用户的验证，这样就能够起到抵抗中间人攻击的效果。

由于单一签名算法或加密算法不能保证安全通信，本文采用联盟区块链的 V2G 网络跨域认证方法，通过采用签名和加密技术相结合的方式，在传递消息过程中通信认证结合签名和加密算法，能够更好地满足通信时的安全性需求。单一的签名算法、加密算法，以及本文使用的签名加密结合算法在应用过程中的安全性对比分析如表 2 所示。从表 6 中可以看出，本文方案的签名加密结合算法，具有很好的保密性、认证性以及安全性。

表 2　签名加密算法的安全性对比分析

算法	保密性	认证性	安全性
签名算法	否	是	否
加密算法	是	否	否
签名加密结合算法	是	是	是

3.2　效率分析

本文提出的基于联盟区块链的 V2G 网络跨域认证方法，通过采用分布计算方式，盟员的增加将不会导致两方跨管理域认证时使用公钥算法次数的增加。使用哈希算法将数字身份的 Hash 值存放在联盟区块链中进行查找，由于哈希 Hash 算法的计算速度比公钥算法速度快很多倍，所以即使在多域联盟的环境下，本方案实现跨域认证的效率比普通公钥密码算法高很多。目前，本文方案中采用的 SM9 算法是公开密钥算法，该算法具有较好的安全性，在大数据环境中非常适合海量用户的安全交互通信[25]。通过对陕西省电网 A 域和山东省电网 B 域之间电动汽车跨管理域认证进行初步分析发现，随着域内用户设备数量的增加，本方案的安全性和实用性也相对比较高。

4　结语

区块链可以促进电网和新能源的发展，最终创造一个更加去中心化的电网。本文针对 V2G 网络中电动汽车跨管理域接入电网的问题，基于联盟区块链和 SM9 算法提出了一种 V2G 中电动汽车跨域认证方案。该方案在不改变基于身份的密码认证模型的前提下，将经过许可的域加入联盟区块链之中，实现用户在多域之间的跨域认证。该方案在适应性选择消息攻击下满足存在性不可伪造，可抵抗重放攻击、拒绝服务攻击和中间人攻击。通过采用签名加密技术结合的算法，能够更好地满足电动汽车跨管理域接入电网过程中的通信安全需求，实现跨域认证的效率较高，可扩展性较强。

联盟区块链技术在能源领域的应用还处于起步阶段，未来的电网将由亿万交互的终端组成，包括微电网、光伏、智能设备、分布式计算系统与能源管理软件等。联盟区块链在构建下一代分布式微电网体系中的潜力巨大，会产生数千万甚至上亿个去中心化节点，这些节点能够交换信息并完成交易，能够极大地推动分布式能源方面的投资活动，还会对电力市场收入进行再分配。结合区块链技术与物联网技术，将使分布式能源交易的协商机制成为可能。在能源运输行业里，联盟区块链可以为电动车辆（EV）充电提供协调服务，如果在两个管理域间建立联盟区块链微电网，每个电站的电价可以由电网和住宅电力供应商共同建立，可以有效促进更大、更高效的充电网络，能够大力推动电动汽车的普及。

参考文献：

[1] Yilmaz M, Krein P T. Review of the impact of vehicle－to－grid technologies on distribution systems and utility interfaces [J]. IEEE Transactions on Power Electronics, 2013, 28 (12): 5673－5689.

[2] Liu K T, Wu C D, Gao S. Opportunities and Challenges of Vehicle－to－Home, Vehicle－to－Vehicle, and Vehicle－to－Grid Technologies [A]. Proceedings of the IEEE [C]. http://ieeexplore. ieee. org/stamp/stamp. jsp? tp = &arnumber=6571224.

[3] Liu J, Xiao Y, Li S, Liang W, etal. Cyber Security and Privacy Issues in Smart Grids [J]. IEEE Commun. Surveys Tuts,

2012，14 (4)：981－997.
[4] Chaudhry H，Bohn T. Security concerns of a plug－in vehicle [A]. Innovative Smart Grid Technologies (ISGT) [A]. 2012 IEEE PES [C]. IEEE，2012：1－6.
[5] Yang Z，Yu S，Liu C. P2：Privacy－preserving communication and precise reward architecture for V2G networks in smart grid [J]. IEEE Trans. Smart Grid，2011，2 (4)：697－706.
[6] Nicanfar H，Hosseininezhad S，TalebiFard，P，et al. Robust privacy－preserving authentication scheme for communication between electric vehicle as power energy storage and power stations [A]. Proceedings of the IEEE INFOCOM [C]. Turin，Italy，2013：3429－3434.
[7] Abdallah A，Shen X M. Lightweight authentication and privacy－preserving [A]. IEEE Transactions on Vehicular Technology [C]. 2017，66 (3)：2615－2629.
[8] Braeken A. Efficient anonym smart card based authentication scheme formulti－server architecture [J]. Int J Smart Home，2015，9 (9)：177－184.
[9] Touhafi A B A. AAA－autonomous anonymous user authentication and its application in V2G [J]. Concurrency and Computation：Practice and Experience，2018，30 (12).
[10] Saxena N，Choi BJ. Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks [J]. IEEE Trans Inf Forensics Secur. 2016，11 (7)：1438－1452.
[11] Vaidya B，Makrakis D，Mouftah H T. Security mechanism for multi－domain vehicle－to－grid Infrastructure [A]. Proc. IEEE Global Telecommun. Conf. GLOBECOM [C]. 2011.
[12] Chen J，Zhang Y，Su W C. An anonymous authentication scheme for plugin electric vehicles joining to charging/discharging station in vehicle－to－grid (V2G) Networks [J]. China Communications，2015：10－20.
[13] Vaidya B，Makrakis D，Mouftah H T. Multi－domain Public key Infrastructure for Vehicle－to－Grid network [C]. MILCOM 2015：1572－1577.
[14] 唐文剑. 区块链将如何重新定义世界 [M]. 北京：机械工业出版社，2016.
[15] Mengelkamp E，Notheisen B，Beer C，et al. A blockchain－based smart grid：towards sustainable local energy markets [J]. Computer Science － Research and Development，2018，33 (1/2)：207－214.
[16] Gao J B，Asamoah K O，Sifah E B. GridMonitoring：secured sovereign blockchain based monitoring on smart grid [J]. IEEE Access (Volume：6)，2018，9917－9925.
[17] Yu R G，Wang J R，Xu T Y，et al. Authentication with block－chain algorithm and text encryption protocol in calculation of social network [J]. IEEE Access，2017，5：24944－24951.
[18] Mann C，Loebenberger D. Two－factor authentication for the Bitcoin protocol [J]. Int. J. Inf. Secur.，2017，16：213－226.
[19] 周致成，李立新，李作辉. 基于区块链技术的高效跨域认证方案 [J]. 计算机应用，2018，38 (2)：316－320.
[20] 袁 峰，程朝辉. SM9 标识密码算法综述 [J]. 信息安全研究，2016，2 (11)：1008－1027.
[21] 余 维，杨晓宇，胡 跃，等. 基于联盟区块链的分布式能源交易认证模型 [J]. 中国科学技术大学学报，2018，48 (4)：307－313.
[22] 吴振铨，梁宇辉，康嘉文，等. 基于联盟区块链的智能电网数据安全存储与共享系统 [J]. 计算机应用，2017，37 (10)：2742－2747.
[23] 欧阳旭，朱向前，叶 伦，等. 区块链技术在大用户直购电中的应用初探 [J]. 中国电机工程学报，2017，37 (13)：3737－3745.
[24] 杨德昌，赵肖余，徐梓潇，等. 区块链在能源互联网中应用现状分析和前景展望 [J]. 中国电机工程学报，2017，37 (13)：3664－3671.
[25] 更加安全易用的国产密码体系——SM9 算法 [J/OL]. 网域前沿，2016 (06)：85－86.

(上接第 221 页)

[3] Jayaram U，Jayaram S，Shaikh I，et al. Introducing quantitative analysis methods into virtual environments for real－time and continuous ergonomic evaluations [J]. Computers in Industry，2006，57 (3)：283－296.
[4] 杨新红，高 峰，王国富，等. 基于 TESIS DYNAware 的车辆巡航虚拟试验研究 [J]. 机械工程学报，2011，47 (20)：165－170.
[5] 邹 俞，晁建刚，杨 进. 航天员虚拟交互操作训练多体感融合驱动方法研究 [J]. 图学学报，2018，39 (4)：742－751.
[6] 崔庆春，李星新，郝建平. 基于 WiseGlove 数据手套的维修手势仿真研究与实现 [J]. 计算机测量与控制，2014，22 (2)：594－597.
[7] 李文峰，王 琦. 虚拟设计环境建立与 OpenGL 和 VRML 的研究开发 [J]. 图学学报，2000，21 (2)：1－5.
[8] 刘 佳，刘 毅. 虚拟维修技术发展综述 [J]. 计算机辅助设计与图形学学报，2009，21 (11)：1519－1534.
[9] 冯桂珍，池建斌，邢海军，等. 基于 Unity3D 的减速器虚拟拆装实验 [J]. 图学学报，2018，39 (2).
[10] 刘钡钡，田 凌，杨宇航. 航空虚拟维修系统关键技术 [J]. 计算机集成制造系统，2012，22 (1)：47－57.
[11] 姚凡凡，梁 强，许仁杰，等. 基于 Vega Prime 的三维虚拟战场大地形动态生成研究 [J]. 系统仿真学报，2012，24 (9)：154－158.
[12] 杨 远，蒋 明，闫 勇. 基于 EON Studio 和 Visual Studio 输油挂车泵模拟器设计 [J]. 后勤工程学院学报，2012 (5)：77－82.
[13] 唐爱军，黄振全，何 云. 基于 Virtools 的火炮液压装置虚拟装配设计 [J]. 信息系统工程，2017 (1)：90－91.
[14] Gerbaud S，Mollet N，Ganier F，et al. GVT：a platform to create virtual environments for procedural training [A]. Virtual Reality Conference，2008. VR '08. IEEE [C]. IEEE，2008：225－232.
[15] 焦玉民，王 强，徐 婷. 军用工程机械保障虚拟训练体系研究 [J]. 计算机工程与应用，2013，49 (8)：253－256.