基于区块链的信息物理融合系统的信息安全保护框架

丁庆洋 王秀利 朱建明 宋 彪
(中央财经大学信息学院 北京 100081)

摘 要 信息物理融合系统(Cyber-Physical System,CPS)受到了学术界的广泛关注,其面临的安全性问题及防护措施也日益成为领域研究热点。通过梳理现阶段国内外关于CPS安全问题及其防护措施的研究成果发现,基于整体多层次统筹以及分布式架构的防护措施成为了当前的研究导向,这与区块链技术的整体性分布式架构特征相一致。在区块链分布式拓扑结构及其信息安全特性的基础上,提出了融合区块链技术与CPS的防护思想,论证了结合二者的可能性,并构建了实现二者深入融合的BCCPS框架机制。重点介绍了BCCPS框架在基础层级和集成层级两个层面上的具体构造情况。最后,从信息安全的保密性、完整性、可用性、可追溯性4个维度论证了BCCPS框架的安全性。该研究为建立安全、健壮的CPS提供了新思路。

关键词 信息物理系统,区块链,信息安全,BCCPS框架,安全性分析

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.02.006

Information Security Framework Based on Blockchain for Cyber-physics System

DING Qing-yang WANG Xiu-li ZHU Jian-ming SONG Biao
(School of Information,Central University of Finance and Economics,Beijing 100081,China)

Abstract Cyber-physics system has drawn widespread attention of academia,and the protection problems and protection measures it faces are also increasingly becoming the research focus in the field. By combing the current research results about the security issues of cyber-physics system and corresponding protective measures at home and abroad,it is found that the security protection measures based on the overall multi-level coordination and distributed architecture have become the current research direction,which is in line with the features of distributed architecture of blockchain technology. Based on the introduction of the distributed topology of blockchain and its information security features,this paper proposed the idea of security protection in which the blockchain technology is integrated with the cyber-physics system,proved the possibility of combining the two parts,and constructed BCCPS framework mechanism of integrating the two parts deeply. The specific construction of BCCPS framework at both the basic level and the integrated level was highlighted. Finally,the security of BCCPS framework was demonstrated from four aspects:confidentiality,integrity,availability and traceability of information security. This research provides a new idea for establishing a secure and robust cyber-physics system.

Keywords Cyber-physics system,Blockchain,Information security,BCCPS framework,Security analysis

1 引言

信息物理融合系统(Cyber-Physical System,CPS)是包含了计算机算法、网络和物理实体的复杂系统[1]。CPS采用模型计算、联结和控制系统将真实的物理世界数字化,并实现数字世界和物理世界的统一[2]。CPS通过对物理世界的实体进行监控感知,并通过挖掘和分析实体世界中蕴含的丰富数据,对物理实体的行为进行控制,以实现物理世界的高效运转。美国国家科学基金最先提出该概念并做了详细阐述,此后其受到了美国政府、学术界和产业界的高度重视。2013年,德国《工业4.0实施建议》将CPS定位为工业4.0的核心技术,并在标准制定、技术研发、验证测试平台等方面做出了一系列重要部署。《中国制造2025》指出"基于CPS的智能装备、智能工厂等智能制造正在引领制造方式变革"[3]。《国务院关于深化制造业与互联网融合发展的指导意见》对CPS建设做出了明确的要求和规划,指出"构建信息物理系统参考模型和综合技术标准体系,建设测试验证平台和综合验证实验床,支持开展兼容适配、互联互通和互操作测试验证"[4]。

到稿日期:2017-11-28 返修日期:2018-01-10 本文受国家自然科学基金重点项目:工业信息物理融合系统安全理论与关键技术(U1509214)资助。

丁庆洋(1991-),男,博士生,主要研究方向为区块链应用、信息安全,E-mail:dingqingyang66@163.com;王秀利(1977-),男,副教授,硕士生导师,主要研究方向为网络安全、电子商务安全;朱建明(1965-),男,教授,博士生导师,主要研究方向为信息安全、区块链技术;宋 彪(1983-),男,博士后,主要研究方向为大数据分析、信息安全,E-mail:songbiao_511@163.com(通信作者)。

现阶段，我国 CPS 建设已经取得初步进展，一些先进企业已开展了 CPS 建设试点，正处于 CPS 建设规律总结和逐步推广期。环境的不确定性、安全攻击以及相关设备的运行错误等为确保 CPS 整体的安全性带来了巨大挑战[5]。CPS 将对现实世界进行数字化呈现和智能化管理，大量的物理世界真实信息将会被存储于系统，而一旦系统受到攻击，不仅会造成数据的泄露，而且会导致大量的物理实体被攻击者利用，对企业和社会造成重大损失。传统的信息系统存储模型采用集中化的存储模式，一旦中心系统受到攻击，整个系统将面临灭顶之灾。据此，国内外研究者开展了采用分布式架构方式对 CPS 进行优化的相关研究，例如文献[6-7]虽然只限于采用分布式控制中心对 CPS 的控制层进行优化，并不涉及物理层以及传输层，其安全性依然无法保障，但从整体多层次统筹以及建立分布式架构的研究思想与区块链技术特征相吻合。同时，现有的传统的 CPS 层次划分方式难以实现整体布局的分布式架构。因此，本文结合相关研究，提出将 CPS 从空间维度划分为基础层级、集成系统层级以及系统整合层级，基于此提出基于区块链分布式架构原理的 BCCPS 框架，以实现对 CPS 的布局优化并提高系统的整体健壮性。区块链是一种典型的分布式架构，利用密码学、共识算法、智能合约等技术实现信息收集、流转、存储、共享等过程的不易篡改和可追溯等，能够大大降低中心式数据存储所带来的信息安全风险；将区块链技术与 CPS 在各个层面上相融合，建立健壮、可靠的信息系统，将大大增加 CPS 的信息安全性，并实现信息系统布局的优化。

本文第 2 节描述 CPS 及其面临的安全问题；第 3 节进行基于分布式架构思想的 CPS 结构划分；第 4 节阐述区块链信息安全机制；第 5 节描述区块链融合于 CPS 的信息安全框架(BCCPS 框架)；第 6 节对 BCCPS 框架的安全性进行分析。

2　CPS 及其面临的安全性问题

CPS 是一项复杂、综合的系统工程，涉及传感器、智能机器人、物联网、异构网络集成、计算机算法、数据存储等多个学科和领域。但学术界对 CPS 的定义并不统一，如文献[8-16]。通过梳理相关理论观点不难发现，CPS 利用感知技术、通讯、网络联结技术等手段实现对物理世界的感知和数字化呈现，进而形成在信息世界的数据投射，利用先进的计算机算法实现对物理世界运行过程的优化，并形成物理实体世界和信息世界相互影响、相互作用的闭合回路。结合相关文献(诸如文献[11-21])对 CPS 特征的描述，可以将其概括为 3 个主要特征，即融合性、多样性、智能性。

现有研究中，最早关于 CPS 安全的文献出现于 2008 年，近年来相关文献逐渐增多。其中，文献[11]基于传统的 CPS 框架体系理论介绍了 CPS 感知层、数据传输层、应用控制层所面临的威胁。在物理层，攻击者主要针对传输媒介和物理设备发起攻击；在传输层，攻击者主要针对控制命令和路由信息发起攻击；在应用层，攻击者主要针对软件系统漏洞和用户隐私发起攻击[22]。其中感知层主要面临的安全威胁包括：物理攻击、设备故障、线路故障、电磁泄露、电磁干扰、拒绝服务攻击、信道阻塞、女巫攻击、重放攻击、感知数据破坏、假冒伪装、信息窃听、数据篡改、非法访问、被动攻击、节点捕获等。数据传输层主要面临的安全威胁包括：拒绝服务攻击、路由攻击、控制网络、DoS 攻击、汇聚节点攻击、方向误导攻击、黑洞攻击、泛洪攻击、攻陷门、Sybil attack、Sinkhole attack、Wormhole attack、Routing loop attack、HELLO 泛洪攻击、应答哄骗、错误路径选择、选择性转发、隧道攻击、虚假路由信息。应用控制层面临的安全威胁包括：用户隐私泄露、非授权访问、恶意代码、分布式拒绝服务、数据挖掘中的隐私泄露、控制命令伪造攻击、漏洞攻击、病毒木马、数据库攻击、云计算服务威胁。

同时，文献[23]指出 CPS 的独特性使得传统的安全策略和方法不足以应对不同规格和不同联结方式的 CPS 所面临的安全挑战。文献[24]从单层次和多层次两个角度共同应对 CPS 的安全问题。在单层次的应对策略中可以采用非对称密钥[25]和云端一体化[26]的方式应对数据传输层中的安全挑战，采用认证协议的方式确保 RFID 的信息安全[27]，利用带有物理随机函数的硬件来提高硬件设备的抗入侵性[28]。多层次的应对方式主要包括：采用联合公钥的方式应对跨层次的认证问题[29]，结合密码学和快速加密技术对 CPS 进行整体设计[30]，采用点对点联结的方式实现物理设备之间的信任[31]，基于 RIFD 设备利用混合信任模型应对物理实体在不同所有者之间流转时的信任问题[32]。

另外，文献[6]基于 CPS 中的动态性指出，分布式系统的架构方式相比于中心式的架构方式更能满足使用者对于系统健壮性和可控性的要求。文献[7]以电力网络为具体场景，提出了一种采用分布式控制中心的方法，以评估电厂的运行状态并确定最终威胁因素。其中分布式方法主要依赖控制中心之间的合作方式，即增量式的合作方式以及扩散交互式的合作方式。文献[33]基于群集理论和结构控制理论，提出了一种基于智能网格技术的分层控制理论。该理论主要针对中心式分布控制系统中的数据冗余以及网络荷载过大引起的网络攻击，通过分层次多节点的控制体系来保证 CPS 的安全性。文献[34]提出了一种分布式状态评估方法，以应对利用错误数据对传感器发起的攻击。

当前研究者围绕 CPS 面临的安全威胁以及防护机制开展了大量研究并取得了有指导意义的研究成果。研究导向逐渐从针对 CPS 所面临的某一方面的安全威胁展开研究，过渡到从多层次整体系统布局设计的角度考虑建立安全健壮的 CPS 架构；从针对中心式架构的 CPS 所面临的安全问题展开研究，过渡到建立分布式 CPS 系统。区块链技术作为典型的分布式数据存储技术，涵盖了密码学、共识算法、智能合约等多种技术体系，与现有的 CPS 安全防护研究导向相契合。

3　基于分布式架构思想的 CPS 结构划分

文献[15,19,22-24]对 CPS 结构进行了分析，按照数据在系统中的流转过程及其形成的回路将 CPS 架构划分为物理空间(物理层)、传输层(空间层、网络层)、信息空间(应用层、决策层、网络物理层)。另外，考虑到人与系统的交互过程或人对系统的控制作用，将 CPS 架构扩展为人类、物理层、传输层、信息空间。

在 CPS 的构建过程中，由于实际应用场景不同，所构建的系统规模和类型也有较大区别。在传统的分析思路中，针对 CPS 架构的划分方式以中心化存储和控制为基本思想，本文结合相关理论研究成果(诸如文献[8])，基于分布式存储和控制的思想对 CPS 框架进行了重新梳理，其层级划分如下。

1)基础层级。基础级是 CPS 的最小层级，具有不可分割性。基础层级的 CPS 构件可以实现对物理实体及环境的状态感知、计算分析和控制，可以构建独立的数据流转闭环，实现物理世界在信息世界中的投射。除此之外，基础层级的构件也可以与外界交互。因此，基础层级的 CPS 构件具备感知能力、计算能力和自决策能力，同时又可以进行延展。基础层级又可以划分为两个部分，即物理基础装置层和信息延展层。物理基础装置层包括物理实体、传感器、执行器以及与外界交互的装置等。该部分构成物理过程的实际操作部分。信息延展层的主要功能在于进行物理装置与信息世界的交互以及低层次的自优化控制，实现物理空间与信息空间的最终融合。

2)集成层级。社会生产活动的复杂性和协同性使任何活动都要由多个人、机、物料协同参与。这就决定了多个基础层级的 CPS 必然要通过互联、互通和互操作整合成为一个集成层级的 CPS。集成层级的 CPS 以若干个基础层级 CPS 的状态感知、信息交互、实时分析为基础，可以实现局部范围内的资源自组织、自配置、自决策、自优化，进而提高资源优化配置的广度、深度和精度。

3)系统整合层级。系统整合层级的 CPS 是由多个系统层级的 CPS 互联互通而整合形成的，是涵盖物理空间和信息空间最广的系统，可以实现多源异构数据的集成，使得数据可以在全局范围内实现交换、共享的闭环流动，进而实现信息的全面感知、深度分析、科学决策和精准执行。在此系统中，物理空间和信息空间的融合度最深，涉及的技术种类最多，联网方式最复杂，智能化水平最高，可以提供的价值增值项目最多。因此它是 CPS 系统的最高形态。

4 区块链信息安全机制

4.1 区块链的原理

区块链是由一系列按照时间顺序排列的区块构成的。每一个新的区块加入到区块链中时，都要经过所有节点的验证，只有通过共识性验证的数据才能加入到区块链中。现阶段较为流行的区块链共识算法主要包括以比特币为代表的工作量证明(Poof of Work，POW)和以以太坊为代表的股权证明(Poof of Stake，POS)。对于前者，通过节点解决一个数学难题而最先获得答案的节点便拥有该区块的记账权；后者则是依靠持有和维护网络的时间、拥有以太币的数量来确定记账权的分配。区块的顺序由区块上加盖的时间戳的先后顺序确定。

区块一般由两部分组成，区块头和区块体。区块头中封装着本区块的哈希值、上一区块的哈希值、时间戳、区块难度值、随机数以及 Merkle 根。区块头的主要作用是对区块的唯一性进行标识，同时确保区块可以按照时间顺序连接到区块链中。区块体中主要封装的是交易事项(具体信息)。在区块体中所封装的具体信息以哈希值的形式存在，从而减小了数据存储所占用的物理存储空间。由于区块链中共识的时间点之间存在间隔(例如比特币的共识时间间隔为 10 min)，因此区块链中所封装的交易事项一般为在间隔期内存储到区块中的交易事项(具体信息)。区块体的主要作用是存储全网在共识时间间隔期所发生的交易事项。图 1 给出了区块链示意图。

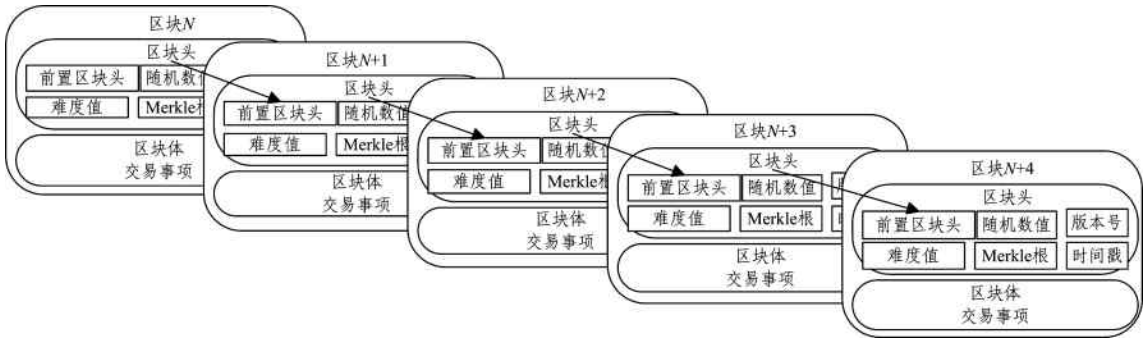

图 1 区块链示意图

Fig. 1 Schematic diagram of blockchain

区块链采用分布式存储。与传统的中心式存储方式不同，区块链的全部数据并非存储于某一中心节点，而是每一个节点均可以保存区块链中的全部数据，即每一个节点都保存区块链的“副本”，都可以对区块链中的数据进行实时监控和获取。为解决节点物理存储空间随着区块链中数据的增加而难以承载的问题，区块链的节点被设计划分为核心节点、轻型节点。核心节点中保存了完整的区块链数据；而轻型节点只存储与自身交易有关的区块数据，但可以随时向全网请求获得全部的区块链信息。

文献[38]对区块链的基础架构进行了总结，将区块链划分为数据层、网络层、共识层、激励层、合约层、应用层 6 个层次。其中数据层由区块组成；网络层主要涉及组网方式、数据传播及数据验证机制；共识层主要包括各类共识算法；激励层主要包括为实现新区块的不断产生以及区块链的实时维护而设计的对节点的激励机制；合约层包括各类脚本、算法和智能合约；应用层是将区块链应用于具体情境的抽象化概括。

4.2 区块链数据安全机制

区块链是一种典型的分布式存储技术，利用密码学、共识算法、智能合约等技术实现信息收集、流转、共享等过程中的完整性、保密性、可用性等。区块链的数据安全性主要由其设

计原理决定。

区块链采用分布式存储，并采用 P2P(Peer to Peer)的组网方式进行网络联结。分布式存储使得每一个节点都可以保存包含区块链全部数据的“副本”，进而避免当采用中心节点存储时，中心节点遭受攻击而致使全部数据受到损失的情况。P2P 的组网方式可以实现网络节点之间的直接互联互通，可以避免对单一节点访问量过大而带来的网络访问拥挤的现象；并且其通过共识认证的方式确定新的区块产生和数据一致性，建立节点之间的信任关系。

区块链技术利用密码学算法将数据存储于区块中，例如哈希算法。其优势在于不仅可以将文本数据保存为固定字符长度的哈希值，更重要的是一旦文本数据有任何改动，哈希值将会发生巨大变化，因此可以轻易识别数据是否被篡改。区块头中保存的当前区块的哈希值是区块的唯一性标识。该哈希值是利用哈希算法将区块中的全部数据进行加密后得到的唯一字符值。一旦区块中任意数据发生改变，区块头中封装的当前区块哈希值都会发生变化。而当前区块的哈希值又是其后续区块的前一区块哈希值，因此一旦当前区块发生变化，其后续区块都将发生变化，这意味着改动一个区块的数据便要对其后续区块的数据全部进行更改。而通过共识后，区块链中全部的参与节点都保存了该区块的原始数据，如果要强行改变某一区块的数据，则要花费全网 51% 的算力，使得攻击难以成功。这就确保了信息的真实性和可用性。

区块链以时间的先后顺序为扩展法则，由区块组成首尾相连的区块链条。区块按照时间的先后顺序排列，而区块内的交易事项则以在共识间隔期传输到全网中的先后顺序依次排列在区块中，以确保区块链中的数据具有可追溯性。

5　区块链融合于 CPS 的信息安全框架(BCCPS 框架)

5.1　区块链与 CPS 融合的可行性

区块链作为一种典型的分布式存储技术，具有安全健壮性和信息追溯性，将区块链技术与 CPS 相结合有利于增强其安全健壮性。其具体表现在以下几方面。

1)区块链所采用的分布式架构为 CPS 布局优化提供了崭新思路。区块链是一种融合了加密算法、智能合约的典型的分布式架构技术，其中的每一个节点都拥有数据“副本”。将区块链的分布式构架原理融入 CPS 可实现各层级的 CPS 分布式布局。CPS 的基础层级以感知设备等为物理载体，存储该物理载体的功能信息、环境感知信息，而且每一个基础层级的 CPS 都备份了其他基础层级 CPS 的数据；集成层级的 CPS 由各个基础层级的 CPS 互联互通整合而成；在此基础上由集成层级的 CPS 搭建系统整合层级的 CPS。此种分布式构筑方式可以有效防止局部的 CPS 出现功能障碍而导致全局范围的 CPS 难以正常运转的问题。

2)区块链可以满足 CPS 对信息安全性的要求。区块链技术融合了多种数据加密技术以及数字签名技术，并通过共识算法进行数据一致性认证。同时，在 CPS 中，信息的传输和存储对机密性、完整性、可用性、可追溯性的要求也极高，无论将 CPS 应用于何种场景，例如智能家居、电力能源、军事工程、生物医药和机器制造业领域，信息安全都是首要考虑的因素[2]。将区块链技术与 CPS 相融合可以借助区块链技术中固有的信息安全技术应对 CPS 面临的安全挑战。

3)区块链技术的链式构筑方式和分布式存储为 CPS 实现数据追溯提供了新路径。区块链中的每一个区块头部分中都封装了前置区块的哈希值，因此将数据区块构造成为首尾相连的数据链条，确保了在整个区块链中数据的可追溯性，而分布式存储方式又保证了数据的可共享性。在 CPS 中，尤其是工业 CPS，实现数据的可追溯和数据共享至关重要。例如，通过对制造过程中历史数据的分析，企业质检人员可以便捷、快速地实现产品问题溯源，发现整个制造过程中的薄弱环节，进而实现生产流程的优化，提高产品质量。同时，通过数据分享以及加强生产流程中各环节之间的沟通，可以有效减少不必要的生产活动，实现精细化、节约化生产，进而降低生产成本。

5.2　BCCPS 框架

现有研究中基于区块链的 CPS 框架设计机制已经取得了诸多成果，但依然存在诸多问题，部分研究者注重于基于区块链的 CPS 框架的信息传输和信息查询，其框架的设计过多地借鉴比特币等数字货币的底层区块链交易构建原理，而忽视了区块链分布式存储这一本质特征。为此，本文在 BCCPS 的设计中更加注重基于区块链分布式存储的 CPS 保护框架。

5.2.1　整体架构

基于区块链的 CPS 框架除具有前文中所提及的融合性、智能性和多样性外，还具有显著的特征——分布式存储。而分布式存储面临的主要问题有两个方面：1)数据的一致性认证，即保证存储于 BCCPS 中的数据是真实、可靠、合法的且具有一致性；2)数据传输，同一级别中同一类型的 CPS 数据可以实现自由传输，同时高级别的 BCCPS 可以获取低级别的 BCCPS 的数据，而且在同一级别不同类型的 CPS 之间的异构数据也可以通过统一的转化规则来实现转化。除此之外，限于 CPS 的物理构件多为低功率、低存储的感知设备，确保数据的低冗余和高效存储也是值得关注的问题。以上述 3 个问题为切入点，建立安全可靠且可以实现对数据进行追溯与共享的 BCCPS 框架，这要求其与 CPS 本身的层次结构相结合，在 3 个层级上实现区块链技术与 CPS 的融合，如图 2 所示。

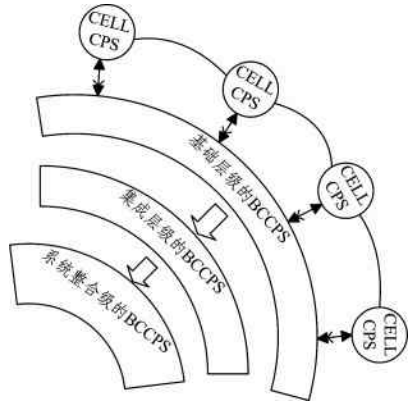

图 2　BCCPS 的总体框架

Fig. 2　Overall framework of BCCPS

1)基础层级的融合。基础层级的 CPS 作为整个 BCCPS 的底层支撑，除具备传统 CPS 物理构件的基本感知与数据存

储、传输功能外，还需要具备数据标准化的功能，尤其是同级以及物理功能类似的 CPS 之间的数据标准化以及数据备份功能。另外，基础层级的 CPS 也需要保存各个基础层级的 CPS 彼此之间进行数据传输的信息以及传输记录。

2)集成层级的融合。集成层级 BCCPS 以通过实现基础层级构筑对物理世界进行感知的物联网为基础，搭建起组织、生产流程等局域范围内的沟通平台。集成层级 BCCPS 并不是基础层级 BCCPS 的简单叠加和汇总，它要实现各基础层级 CPS 的深度整合和互联互通，实现异构数据的转化以及数据查询请求的响应速度和频次的分配，同时对新接入的基础层级 CPS 进行审核认证，统一数据格式或者确立异构数据转化规则，统一局部范围内的联结规则，维护该层级的区块数据并记录设备联结痕迹。

3)系统整合层级的融合。将不同组织内部系统层级的区块数据进行打包处理，形成更高层级的区块，并以此为基础构建系统整合层级的区块链。此区块链用于实现更高层级的数据查询和记录，该层级 BCCPS 需要跨组织的协同，涉及到的业务范围更为广泛，一般以企业之间的深度信息沟通为基础，由于其所涉及的应用场景受限，因此本文不做重点考虑。

5.2.2 基础层级 BCCPS

基础层级 BCCPS 主要用于实现区块之间的联结、基础层级数据的存储以及相关信息的查询。由于区块链中的信息备份在各个基础层级的 CPS 中，因此可以实现数据共享，基础层级的区块链可以有效防止数据被篡改。

在基础层级的 BCCPS 中，各基础层级的 CPS 要将自身物理感知的数据进行标准化处理(如哈希加密)，并收集得到同级 CPS 的数据，将其打包处理后放入区块中。它以数字签名的方式实现一致性的认证，从而规避在诸如比特币、以太坊中的复杂共识算法对资源和数据的浪费。

在基础层级 CPS 区块链中，区块主要由两部分组成：区块头和区块体。区块头中包含的信息包括：1)前置区块的哈希值；2)当前区块的哈希值；3)Merkle 根；4)Nonce 值；5)时间戳以及其他信息。区块体中主要包含的信息包括：1)信息发送者的身份识别号；2)信息接收者的身份识别号；3)信息认证；4)信息类型以及遵守的转化规则；5)加密算法；6)数据。前 3 项用于解决数据一致性认证和数据传输问题，加密算法用于最低程度地减小数据存储容量。基础层级 CPS 的区块结构如图 3 所示。

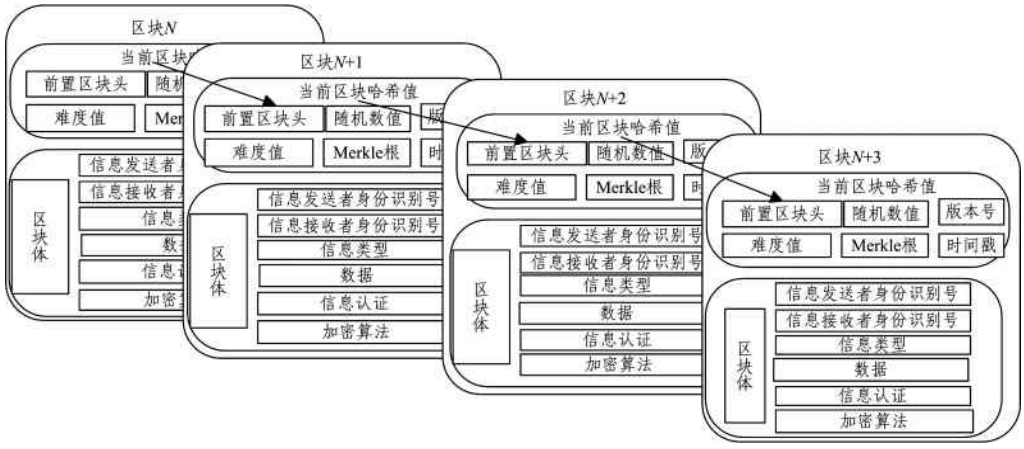

图 3 基础层级 CPS 的区块结构

Fig. 3 Block structure of basic level CPS

5.2.3 集成层级 BCCPS

在基础层级 CPS 功能的基础上，集成层级 CPS 功能还包括互联互通、即插即用、边缘网关、数据互操作、协同控制、监视与诊断等[8]。相比于其他功能可以在已经搭建好的区块链系统中实现，即插即用在系统级 CPS 中实现组件管理，包括基础层级 CPS 的识别、配置、更新和删除等功能，还涉及到在区块链中加入新的节点，这是集成层级 CPS 区块链在构建和维护中需要解决的首要问题，也是安全风险最为突出的问题。因此，本文将重点阐述集成层级 CPS 在组件管理方面的建构原理。

在 BCCPS 中，数字签名是数据一致性认证的关键环节，设备一旦添加则意味着其传输的数据被信任，因而新的物理设备联结到现有集成层级 CPS 中时需要经过严格的审核。因此，新的物理设备联结到现有集成层级 CPS 中时需要经过注册，向其他设备发送信息证明自身存在的合法性以及加入系统过程中的合法性。密码学中的非对称性加密为解决此问题提供了良好的思路。当新设备接入到系统层级的 CPS 中时，可以采用 SHA256 算法产生私钥，采用 Secp256k1 算法产生公钥[2]。当新的基础层级 CPS 设备进入到区块链中时，需要发送利用私钥加密的带有自身标识信息的数字证书以及公钥到集成层级 BCCPS。与此同时，该设备也将作为新的基础层级 CPS 区块链加入到集成层级的 BCCPS。在集成层级 CPS 接纳该设备之后，集成层级的 BCCPS 区块链将会利用该设备发送的公钥对其数字证书进行解密，确认该设备的身份信息，并最终确认该设备接入到系统级的 CPS 区块链中。一旦经过认证，该设备便可以参与到集成层级 BCCPS 中，其数据也将被认为是可信的，该过程实现了数据一致性的认证。

同时，集成层级的 BCCPS 要实现异构数据的标准化处理，因此在集成层级 BCCPS 中，区块头包含的数据以及结构形式与基础层级 BCCPS 的相似。而区块体中主要包含的信息有：1)流程的信息密文；2)设备身份识别信息；3)设备类型；4)传输的主体数据；5)设备数字签名。流程密文用于标注集成层级 BCCPS 涉及到的生产流程以及所包括的基础层级

CPS 的范围；设备身份识别号、设备类型和设备数字签名则用于实现数据一致性认证及新设备的审核管理；传输的主体数据则主要用于解决底层数据获取、异构数据标准化等问题。

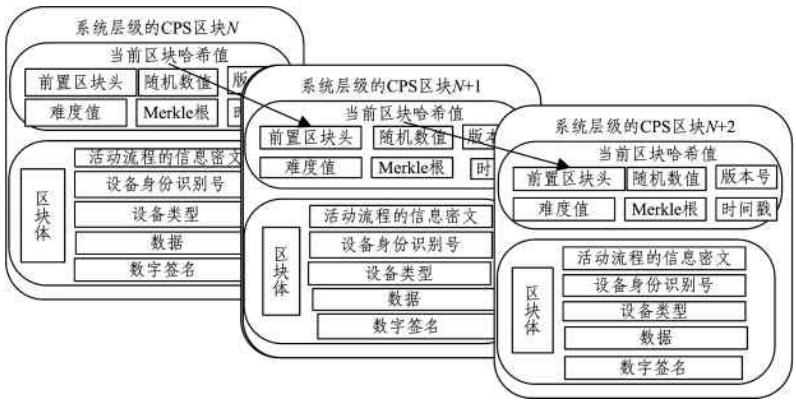

图 4　集成层级 CPS 的区块结构

Fig. 4　Block structure of system level CPS

6　BCCPS 框架的安全性分析

CPS 是安全敏感型系统，其安全目标与其他基于计算机技术的信息系统的安全目标一致，诸如信息保密性、完整性、可用性以及可追溯性[36]。同时，在具体实施信息安全策略时也要与 CPS 的运行机理相结合，诸如文献[37]和文献[38]所提及的对物理环境以及感知设备的安全防范。本文基于学术领域的研究成果将 CPS 安全表述为安全威胁、系统脆弱性、安全攻击以及安全保障措施。同时，将 CPS 的安全关注点分解为安全目标和安全机制。安全措施是指通过融合安全目标和安全机制构建安全健壮 CPS 的措施。本文提出的以区块链安全原理为基点构建的 BCCPS 框架可以视为 CPS 安全措施，因此本文将在此基础上从保密性、完整性、可用性和信息可追溯性 4 个维度分析 BCCPS 框架的安全性。

6.1　BCCPS 框架的信息保密性分析

信息保密性是指隐藏信息或资源[39]，丧失保密性则意味着未经授权的信息被披露[40]。信息保密性意味着即使未经授权的人或组织意识到信息或资源存在，也无法获取。在 CPS 中，系统的运行情况必须向未授权方保密，即系统必须具有足够的安全机制来防止信息被窃取；同时，在一些涉及用户敏感性数据的 CPS 中，需要确保用户的个人隐私数据不被窃取和盗用[36]。

BCCPS 将区块链原理与 CPS 相融合，充分发挥区块链原理的安全机制。在区块链中，节点之间的数据是同步备份的，保证进入到系统中的单元级 CPS 共享信息，同时信息采用加密算法（如 Hash256 算法）加密，并通过非对称密钥对的方式进行数据传输，大大提升了 CPS 数据传输过程中的信息保密性。在 BCCPS 框架下，信息在不同物理设备中传输时，信息发送端利用接收端的公钥将信息加密，而接收端在接收加密信息后利用自身私钥对信息进行解密，进而避免数据通道被劫持后数据被直接获取的危险。

6.2　BCCPS 框架的信息完整性分析

信息完整性是指数据或资源的可信度，通常用来防止对数据不正当的修改或未经授权时对数据的篡改[39]。丧失完整性则意味着信息遭受未经授权的篡改和信息丢失[40]。CPS 中的完整性可以被看作通过检测信息传输过程中的欺骗行为来保证信息的完整性[36]，如果不能保证完整性，则可能发生欺骗性攻击行为，即“授权方收到虚假数据并认为是真实的”[37]。

在 BCCPS 框架下，物理设备接入到系统中时需要经过验证（采用诸如非对称密钥对等密码学的方法），通过验证来确保接入到系统中的物理设备是可信任的，而在 BCCPS 框架下验证机制的最突出之处在于利用分布式节点共同验证而非利用中心节点授权的方式实现验证。该验证机制避免了中心式授权中非法节点伪装被授权节点进行欺骗性攻击。另外，数据区块被加入到区块链中时，各个节点也要对数据进行验证，只有通过验证的数据区块才可以加入到区块链中，以保证数据的真实性。除此之外，在区块链中，由于区块头包含“前置区块哈希值”字段，因此当前区块的哈希值也受到该字段的影响。如果前置区块的身份标识发生变化，那么后续联结区块的身份标识也将发生变化。若前置区块有任何改动，前置区块的哈希值也将发生变化；前置区块的哈希值发生改变，将迫使后续区块的“前置区块哈希值”字段发生改变，从而导致后续区块的哈希值发生改变；而后续区块的哈希值发生改变时，又将导致其后续区块哈希值的“前置区块哈希值”字段发生改变，进而使得该区块的后续区块哈希值发生变化，以此类推，一旦某一区块发生变动，其后续链条上的区块都将发生变化。而随着区块链条中接入的区块越来越多，便会产生“瀑布效应”。这种瀑布效应伴随着区块链中接入的区块数量的增多而大大增加了区块中数据的稳定性，以此防止攻击者对 CPS 系统的数据进行篡改。

6.3　BCCPS 框架的信息可用性分析

信息可用性是指使用所需信息或资源的能力[39]。丧失可用性意味着访问或使用信息或信息系统受到阻隔[40]。拒绝服务（Denial of Service，DoS）的特点便是明确地尝试“防止合法使用服务”[41]，是针对信息可用性的安全攻击。因此，CPS 中的可用性目标是防止 DoS 攻击以保证信息的可用性。同时，CPS 的一个典型特征是时空融合性，因此确保系统的实时运转也是保障信息可用性的重要方面。

在 BCCPS 框架下,单元级 CPS 便可以实现物理世界与信息世界交互的回路,同时具有感知和计算以及与外部信息沟通协调的功能;设备可以实现自优化决策,区别于传统 CPS 中物理设备处于物理感知层、传输层、控制层的单一层级中对中心控制系统的高强度依赖,避免了攻击者对系统采取的 DoS 攻击,保证了信息的可用性。同时,在 BCCPS 框架下,单元级 CPS 可以实时感知并进行自我优化,避免了传统 CPS 通过感知、传输、控制以及优化反馈各个环节所产生的时滞性,确保了实时实地的跟踪。

6.4 BCCPS 框架的信息可追溯性分析

信息可追溯性是除保密性、完整性、可用性以外的重要信息安全目标。信息可追溯性意味着可以对信息进行跟踪。在 CPS 中可追溯性意味着对物理实体的运行情况进行实时跟踪,当物理世界的运行状态出现偏差时,可以准确地查找发生偏差的时间和原因。

在 BCCPS 框架下,区块链中的每一个区块都包含区块头和区块体两部分。在区块头中封装着当前区块头值、前置区块头哈希值、时间戳、区块难度以及随机数等信息。通过在每一区块中封装前置区块哈希值的方式将当前区块与其前置区块相连接,进而形成链式结构,而区块链中区块的前后顺序则通过加盖时间戳的时间顺序进行确认,区块的前后排列与时间戳标记的历史顺序一致,从而便形成了具有时间先后顺序的链条式的区块链结构。数据按照时间先后顺序排列保证了信息的历史可溯源性,当物理实体的运行状态出现偏差时,其反馈到 CPS 中的错误信息可以依据时间顺序进行查找,同时集成层级 CPS 中可以存储基础层级 CPS 中的信息,因此可以从集成层级追溯物理实体运行的偏差,甚至从系统整合层级 CPS 也可以进行追溯。

结束语 本文首先回顾了现有研究中关于 CPS 及其安全问题的学术成果,进一步分析了其研究导向,提出了基于分布式架构的思想将区块链技术与 CPS 相结合的防护机制,并对 CPS 的结构进行了重新划分。在阐释区块链原理及其安全机制的基础上提出了将区块链技术与 CPS 相结合的 BCCPS 安全框架,并论述了二者结合的可能性以及 BCCPS 的具体框架结构。最后,以信息安全的保密性、完整性、可用性以及可追溯性 4 个维度为基准,对 BCCPS 框架的安全性进行了分析。本研究为防范 CPS 可能面临的安全攻击及建立健壮可靠的 CPS 提供了新的思路。在以后的研究中,需要解决基础层级 CPS 在能源限制以及物理形态体量受限的实际环境中如何提高存储容量以及计算性能的问题,以夯实 BCCPS 架构的结构基础。

参 考 文 献

[1] PARK K J,ZHENG R,LIU X. Cyber-physical systems:Milestones and research challenges[J]. Computer Communications,2012,36(1):1-7.

[2] YIN S Y,BAO J S,ZHANG Y M,et al. M2M Security Technology of CPS Based on Blockchains[J]. Symmetry,2017,9(9):193-210.

[3] 中华人民共和国国务院. 中国制造 2025[EB/OL]. (2015-05-08)[2017-11-24]. http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

[4] RAJKUMAR R,LEE I,SHA L,et al. Cyber-physical systems:The next computing revolution[C]// Proceedings of the 47th Design Automation Conference. New York:ACM,2010:731-736.

[5] ALI S,ANWAR R W,HUSSAIN O K. Cyber security for cyber physical systems:a trust-based approach[J]. Theory Apply Inf-Technoly,2015,71(2):144-152.

[6] PASQUALETTI F,CARLI R,BULLO F. A distributed method for state estimation and false data detection in power networks[C]// Smart Grid Communications. New York:IEEE Press,2011:469-474.

[7] PALAVICINI G,BRYAN J,SHEETS J,et al. Towards firmware analysis of industrial internet of things (IIoT)—Applying symbolic analysis to IIOT firmware vetting[C]// Proceedings of the 2nd International Conference on Internet of Things,Big Data and Security. Porto,2017:470-477.

[8] China Information Physics System Development Forum,White Paper on Information Physics Systems [M]. Beijing:China Information Physics System Development Forum,2017. (in Chinese)
中国信息物理系统发展论坛. 信息物理系统白皮书[M]. 北京:中国信息物理系统发展论坛,2017.

[9] LEE E A. Computing Foundations and Practice for CyberPhysical Systems:a Preliminary Report[R]. University of California,2006.

[10] HE J F. Cyber-Physical System[J]. China Computer Society Newsletter,2010,6(1):25-29. (in Chinese)
何积丰. Cyber-Physical System[J]. 中国计算机学会通讯,2010,6(1):25-29.

[11] BAHETI R,GILL H. Cyber-physical systems[J]. Computer,2017,50(4):14-16.

[12] LI Z,PENG Y,XIE F,et al. Security threats and measures of information physics system [J]. Journal of Tsinghua University (Science and Technology),2012,52(10):1482-1487. (in Chinese)
李钊,彭勇,谢丰,等. 信息物理系统安全威胁与措施[J]. 清华大学学报(自然科学版),2012,52(10):1482-1487.

[13] The European Union's Seventh Framework Programme. CyPhERS Cyber-Physical European Roadmap & Strategy[EB/OL]. (2013-10-11) [2017-11-25]. http://www.cyphers.eu/sites/default/files/D2.1.pdf.

[14] JING B,ZHOU W,HUANG Y F,et al. Information Physics Fusion System and Its Application [J]. Journal of Air Force Engineering University (Natural Science Edition),2014,15(2):1-6. (in Chinese)
景博,周伟,黄以锋,等. 信息物理融合系统及其应用[J]. 空军工程大学学报(自然科学版),2014,15(2):1-6.

[15] NSF. Cyber-physical systems (cps) program solicitation,2016. [EB/OL]. (2016-03-08)[2017-11-24]. http://www.nsf.gov/

pubs/2016/nsf16549/nsf16549. html.

[16] LEE J，BAGHERI B，KAO H A. A Cyber-Physical Systems architecture forIndustry 4. 0-based manufacturing systems[J]. Manufacturing Letters，2015，3(1)：18-23.

[17] GUAN X P，YANG B，CHEN C L. A Comprehensive Overview of Cyber-Physical Systems：From Perspective of Feedback System[J]. IEEE/CAA Jouranal of Automatica Sinica，2016，3(1)：1-14.

[18] RAJKUMAR R，INSUP L，LUI S，et al. Cyber-physical systems：the next computing revolution[C]// Proceedings of the 47th ACM/IEEE Design Automation Conference. California，USA：IEEE，2010：731-736.

[19] WEN J R，WU M Q，SU J F. Information physics fusion system [J]. Automation，2012，38(4)：517-528. (in Chinese)
温景容，武穆清，宿景芳. 信息物理融合系统[J]. 自动化学报，2012，38(4)：517-528.

[20] MÖLLER D P E. Guide to Computing Fundamentals in Cyber-Physical Systems[M]. Switzerland：Springer Nature，2016.

[21] ZHOU X S，YANG Y L，YANG G. Methodology for constructing dynamic behavior model of information-physical fusion system [J]. Chinese Journal of Computers，2014，37(6)：1411-1421. (in Chinese)
周兴社，杨亚磊，杨刚. 信息-物理融合系统动态行为模型构建方法[J]. 计算机学报，2014，37(6)：1411-1421.

[22] TAN Y，GODDARD S，PEREZ L. A prototype architecture for cyber-physical systems [J]. Acm Sigbed Review，2008，5(1)：1-2.

[23] PENG K L，PENG W，WANG D X，et al. Review on the Security of Information Fusion Systems [J]. Journal of Network Safety，2016，7(7)：20-28. (in Chinese)
彭昆仑，彭伟，王东霞，等. 信息物理融合系统安全问题研究综述[J]. 网络安全学报，2016，7(7)：20-28.

[24] ASHIBANI Y，MAHMOUD Q H. Cyber physical systems security：Analysis，challenges and solutions[J]. Computers Security，2017，68(68)：81-97.

[25] NOURIAN A，MADNICK S. A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet [J]. IEEE Transactions on Dependable & Secure Computing，2015，12(12)：1.

[26] PREMNATH S N，HAAS Z J. Security and privacy in the internet-ofthings under time-and-budget-limited adversary model[J]. IEEE Wireless Communications Letters，2015，4(3)：277-280.

[27] WANG J，ABID H，LEE S，et al. A secured health care application architecture for cyber-physical systems[J]. Control Engineering Applied Informatics，2011，13(3)：101-108.

[28] TRAPPE W，HOWARD R，MOORE R S. Low-energy security：limits and opportunities in the internet of things[J]. IEEE Security & Privacy，2015，13(1)：14-21.

[29] KIRKPATRICK M，BERTINO E，SHELDON F T. Restricted Authentication and Encryption for Cyber-physical Systems[C]// DHS CPS Workshop Restricted Authentication and Encryption for Cyber physical System. Newark：Newark Press，2009：1-4.

[30] ZHAO K，GE L. A survey on the Internet of Things security[C]// Ninth International Conferece on Computational Intelligence & Security. Leshan：IEEE Press，2013：663-667.

[31] VEGH L，MICLEA L. Enhancing security in cyber-physical systems through cryptographic and stegano graphic techniques[C]// IEEE International Conference on Automation. New York：IEEE Press，2014：1-6.

[32] WEI J，KUNDUR D. Biologically inspired hierarchical cyber-physical multi-agent distributed control framework for sustainable smart grids[M]// Cyber Physical Systems Approach to Smart Electric Power Grid. Springer Berlin Heidelberg，2015，12(3)：219-259

[33] DJOUADI S，MELIN A，FERRAGUT E，et al. Finite energy and bounded attacks on control system sensor signals[C]// American Control Conference. Portland，IEEE Press，2014：1716-1722.

[34] YUAN Y，WANG F Y. Study on the Technology and Development of Blockchain[J]. Journal of Automation，2016，42(4)：482-491. (in Chinese)
袁勇，王飞跃. 区块链技术与发展现状与展望[J]. 自动化学报，2016，42(4)：482-491.

[35] NGUYEN P H，ALI S，YUE T. Model-based security engineering for cyber-physical systems：A systematic mapping study[J]. Information and Software Technology，2017，83(2)：116-135.

[36] CARDENAS A A，AMIN S，SASTRY S. Secure control：towards survivable cyberphysical systems[C]// The 28th International Conference on Distributed Computing Systems Workshops. Washington，IEEE Press，2015：495-500.

[37] OATES R，THOM F，HERRIES G. Security-aware，model-based systems engineering with sysML[C]// Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research. Berlin：BCS Press，2013：78-87.

[38] BISHOP M. Computer Security：Art andScience[M]. Boston：MA Press，2002：62-68.

[39] Smart Grid Interoperability Panel Cyber Security Working Group，Guidelines for smart grid cyber security[S]. Washington：National Institution of Standards and Technology，2010.

[40] MCDOWELL M. Understanding denial-of-service attacks[EB/OL]. (2004-07-06)[2017-11-21]. http：//www. us-cert. gov/ncas/tips/st04-015.

[41] MIRKOVIC J，REIHER P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms[J]. Acm Sigcomm Computer Communication Review，2004，34(2)：39-53.