基于信息物理系统(CPS)安全及解决方案的分析

张文婷
(山西大学 自动化系,山西 太原 030000)

摘 要:信息物理系统(CPS)是一个综合计算、网络和物理环境的多维复杂系统,是实现计算、通信和控制的一体化设计,可使系统实时可靠稳定的运行,使人与物理世界的交互信息化和智能化,在航空航天、工业生产、智能电网和交通运输等领域有着广泛的应用前景。在这些应用中,由于信息安全引起的系统安全问题,成为系统设计者必须要考虑的关键因素之一,因此,设计稳健安全和有效的信息物理系统是目前非常活跃的研究领域,受到越来越多研究者的关注。文中介绍了CPS 的核心概念及技术背景,系统阐述了 CPS 整体架构以及重要的安全因素,分别从系统的各个层面介绍 CPS 所面临的信息安全攻击以及安全需求,且针对所面临的安全攻击和需求从单层和多层结合的角度提出相应的安全解决方案,最后阐述 CPS 的未来研究领域。

关键词:信息物理系统;系统架构;系统安全分析;系统安全威胁;解决方案
中图分类号:TP302 **文献标识码**:A **文章编号**:1673-629X(2019)10-0127-07
doi:10.3969/j.issn.1673-629X.2019.10.026

Analysis of Security and Solution Based on Cyber Physical System (CPS)

ZHANG Wen-ting
(Department of Automation, Shanxi University, Taiyuan 030000, China)

Abstract: Cyber physical system (CPS) is a multi-dimensional complex system integrating computing, network and physical environment. It is an integrated design that realizes computing, communication and control, which can make the system work reliably and stably in real time, and the interaction between people and the physical world information and intelligent. It has broad application in the fields of aerospace, industrial production, smart grid and transportation. In these applications, CPS security issues caused by information security have become one of the key factors that system designers need to consider. Therefore, the design of robust, safe and effective CPS is currently a very active research field, and has attracted more and more researchers' attention. We introduce the core concept and technical background of CPS, expound the architecture of CPS and important security factors systematically, and introduce CPS information security attacks and security requirements from all layers of the system. According to security attacks and requirements, the corresponding security solutions are proposed from the perspective of single layer and multi-layer. Finally, the future research fields of CPS are introduced.

Key words: cyber physical system; system architecture; system security analysis; system security threat; solutions

0 引 言

在传统的关于计算系统和物理系统的概念中,信息系统和物理世界是分开的,所以在各领域中信息基础设施的建设与物理世界的基础设施建设是分隔开的。近年来,随着自动化控制、网络通信与嵌入式系统等技术的不断发展与融合,人们对信息技术提出了更为严格的要求,人类赖以生存的世界正朝着网络化、信息化和智能化的方向发展,在这样的背景环境下,促使了信息物理系统的提出和发展。

信息物理系统是一个利用现代传感器、计算和网络技术有效集成网络和物理组件的系统。就是将信息技术融入到物理系统中从而提高物理系统的原有功能,并且增加原有系统不能通过其他途径获得的特点。CPS 在航空航天、交通系统、智能电网、工业生产以及远程医疗等领域具有广泛的应用前景[1-3]。CPS 的广泛采用与德国“工业 4.0”的概念有关,它构成了技术

收稿日期:2018-11-23 **修回日期**:2019-03-19 **网络出版时间**:2019-04-24
基金项目:国家自然科学基金(61603232)
作者简介:张文婷(1994-),女,硕士研究生,研究方向为网络化信息物理系统的分析与设计。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.tp.20190424.1100.088.html

与知识相结合的过程,在没有人类参与的情况下提供了自主性、可靠性、系统性和控制性。CPS 的主要技术趋势包括物联网、大数据、智能技术、云计算等。

信息物理系统是新兴的科技领域,其一出现就得到全世界的广泛关注,各个国家都试图从中得到其核心竞争力。例如,德国政府根据其提出的“工业 4.0”战略,通过打造由智能化的机械、存储系统和生产手段构成并应用于智能工厂的“网络物理融合生产系统”,使德国成为新一代工业技术的供应国和主导市场的核心力量,进一步提升全球竞争力[4]。中国政府也高度重视网络化系统的重要性,国务院 2015 年发布的《中国制造 2025》规划中多次提到网络系统的建设,特别要求“针对信息物理系统网络研发及应用需求,组织开发智能控制系统、工业应用软件、故障诊断软件和相关工具、传感和通信系统协议,实现人、设备与产品的实时联通、精确识别、有效交互与智能控制”[5]。

系统的安全问题是 CPS 面向实际应用的关键性新问题。在 CPS 中,信息技术与物理世界的深度融合带来了很重要的技术优势,但是 CPS 系统是以网络作为核心承载,所以系统的网络规模的增长和分布式的信息处理环境使得 CPS 系统非常容易受到网络攻击,从而对系统进行肆意的破坏,造成不可估量的损失。因此,CPS 系统安全面临着非常严峻复杂的挑战,其重要性与传统信息安全相比有过之而无不及,急需越来越多研究者的关注和努力。

1 信息物理系统

1.1 CPS 的核心概念

CPS 是以外界环境感知为基础,融合计算、通信和控制能力的可控、可信、可扩展的网络化物理设备系统,它通过计算进程与物理进程的彼此影响实时反馈循环,使信息世界与物理世界深度融合且实时交互。其中,通信网络子系统包括传感器网络,用以感知收集数据、泛在通信网络,用于完成传输和通信功能;计算子系统完成对各类数据的分析、存储和处理;控制子系统通过通信和计算子系统提供的信息来确定对物理世界的控制策略,从而协调各个执行器,实现对物理世界的操作和控制,使虚拟世界与实际物理世界互联协同发展。因此,CPS 是一类“系统的系统”。具体如图 1 所示。

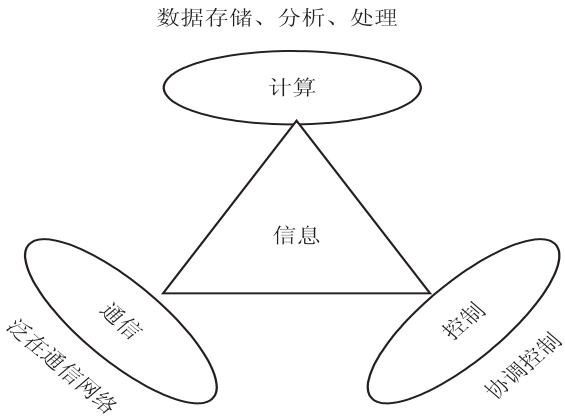

图 1 CPS 概念示意图

1.2 CPS 的技术背景

· 是基于嵌入式处理器的设备,增加了用于数据存储的存储器的记忆功能。

· CPS 控制算法的质量会影响其复杂性和可靠性,这增加了计算工作量的强度。

· 响应时间表征反馈延迟,反馈延迟越多,对象的质量控制越差。

· 大型系统中不同技术趋势的结合:物联网,智能环境等。

· 随着信息量的增长,有必要转移部分 CPS 控制由人来操控[6]。

1.3 CPS 的独特功能

· 嵌入式和移动感应。

· 传感器源和数据流。

· 网络和物理组件的相互作用[7]。

· 培训和适应能力。

· 通过互联网的互操作性(如物联网)。

· 通过集中自动控制确保系统(如 ATM 和 POS)的可靠运行。

· 存在一个共同的网络空间,以密码系统,防火墙,防病毒等形式提供系统内部和环境的交换,以及信息安全[8]。

· 在某些情况下,操作必须可靠且经过认证。

· 通过自动智能控制确保系统的稳健性。

· 人在循环内外。

2　信息物理系统架构

信息物理系统架构如图 2 所示。

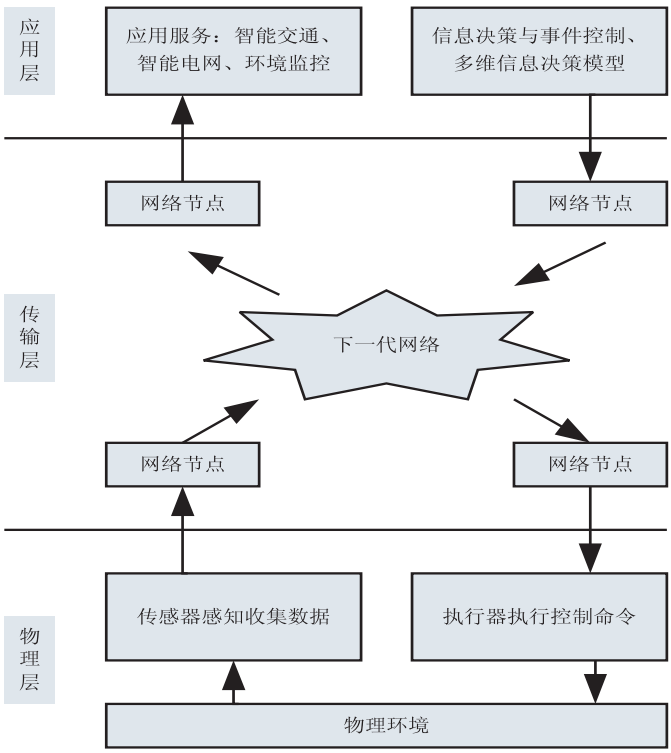

图 2　信息物理系统三层体系结构

2.1　物理层

物理层为 CPS 架构奠定了基础。物理层由传感器、执行器组成,它们通过无线或有线网络相互连接。例如,2G/3G/4G, WiFi, ZigBee, 蓝牙, WiMAX, RFID 阅读器和标签以及有线技术等,主要负责感知获取外界物理环境的数据以及执行系统的控制命令。通过分布在外界物理设备中的嵌入式传感器以及执行器与外部环境进行交互,对物质属性、环境状态等开展大规模的分布式数据获取与状态辨识,且通过数据通信层获得上层数据的处理结果,再反馈至执行器,根据控制命令进行操作,以适应系统与物理环境的变化。收集的数据可以包括声音、光学、力学、化学、热学,电,生物学或位置等,传感器可以在广域网和本地网域中通过节点协作生成实时数据,在控制层进行汇总和分析,传感器根据其类型可以汇总与温度、加速度、湿度、振动、位置或空气化学变化相关的信息[9]。

2.2　传输层

数据传输层由若干的通信基站和网络节点组成,主要负责将从物理层感知的原始数据传送至信息中心,主要通过互联网、局域网、专网、通信网等现有网络对数据进行传输,实现数据之间的交互。同时数据传输层还需具有对海量信息进行智能处理和安全高效管理的能力。

2.3　应用层

应用控制层是信息物理系统交互的核心部分。该层存储、分析和更新从先前层接收的信息,通过在聚合数据上实施复杂的决策算法来生成正确的决策,对信息进行抽象处理,再经过预设规则和高层控制语义规范的判断,确定要调用的所需自动化操作,生成执行控制命令,将生成的执行控制命令通过传输层反馈至物理层中的底层物理单元,由执行器进行相关操作。应用控制层也使信息物理系统与行业专业领域相结合,从而实现广泛化智能化的应用解决方案,如智能交通、智能电网和工业控制等。

3　信息物理系统的安全问题

一般来说,CPS 的安全性分为信息(数据)安全和控制安全两个方面。信息安全是指在网络环境下,尤其是开放的松散耦合网络中,在数据聚集、处理和大规模共享过程中对信息的安全保护。控制安全性包括解决网络环境中的任何控制问题,以及减轻对系统估计和控制算法的任何攻击。信息安全侧重于数据保护,例如使用加密技术,而控制安全则侧重于保护控制系统的动态免受网络攻击[10]。

3.1　CPS 中的重要安全因素

(1)保护对设备的访问。

保护对设备的访问是安全问题的第一个挑战。如果身份验证不受支持或支持不当,未经授权的对象将获得访问和操作系统的权利。

(2)保护数据传输。

为了检测 CPS 通信网络中的冒充者和恶意活动,并阻止未经授权访问的进行,需要保证数据传输的安全性。例如,攻击者试图拦截系统功耗的物理特性和定时行为,以分析正在发送和接收的数据,一些攻击者通过发起拒绝服务攻击或中断路由拓扑来破坏网络。

有些终端设备不是一个完整的计算机系统,没有很强的数据处理和通信能力,也没有足够的存储能力,使得这些设备更容易被渗透。在工业控制系统终端,依赖于开放网络标准的连通性有助于提高系统性能和降低运营成本。虽然这样的终端会带来更高效的操作,但它们会使系统面临更高的入侵和恶意攻击的可能性,例如恶意代码、分布式拒绝服务、窃听和未经授权的访问。另一个直接导致漏洞的因素是,设计过程总是受到处理时间即速度、硬件资源和功耗的限制。此外,嵌入式系统是由在安全问题上经验有限的专家设计的,他们更注重功能、错误更正和性能,而不是安全性[11]。这反过来又会导致系统中的漏洞,这些漏洞可能会将安全信息泄漏给未经授权或不想要的用户。

(3)保护应用程序。

应用层结合了不同的应用程序和安全挑战。在此,攻击者可以对用户的私有信息进行分析,从而导致隐私数据的泄露和隐私的丢失。由于这些数据可能包含用户访问过的过去和现在的位置,因此在这一层中有关于数据保护的一些技术,包括位置伪装、匿名空间或空间加密。

(4)保护数据存储。

保护 CPS 设备中存储的秘密数据是非常重要的。大多数 CPS 设备,如传感器,都是微小的无线连接的和资源受限的节点。虽然各种基于软件的解决方案,通过使用加密技术对这些设备中的数据进行加密,但由于这些设备的内存限制和处理能力薄弱,它们是不够的。

(5)保护执行器。

执行安全性是指任何驱动动作必须从授权来源发出。这将确保所提供的反馈和控制命令是正确的。

3.2 对 CPS 的攻击

对 CPS 的攻击可能会对物理环境造成严重破坏,CPS 的每一层都容易受到被动或主动攻击。本节根据攻击目标所处的层次,分别对物理层、传输层和应用层所面临的攻击展开讨论。

3.2.1 物理层面临的攻击

物理层由终端设备组成,如 RFID 中的标签和传感器,这些设备大多位于室外环境中,容易造成物理攻击,例如篡改设备的组件或替换设备。物理层的常见攻击包括设备故障、线路故障、电磁干扰、感知数据损坏、差分功率分析,信息披露,信息跟踪,篡改,感知信息泄漏,物理破坏和能量耗尽攻击。攻击方法包括:直接在物理设备上进行损坏;迫使物理系统在指定的频率附近产生谐振;散布虚假时钟消息,破坏系统内部各个单元间的协同工作;用注入恶意代码等节点控制的方式掌握物理设备内存储的隐私数据和对话密钥,从而对该节点的传输消息进行窃听、监测、流量分析等被动攻击或篡改、伪造等主动攻击,并以捕获的节点为跳板进一步攻击其他节点[12]。这些攻击的常见形式有:

节点捕获:接管节点,获取和泄漏可能涉及加密密钥的信息,然后使用加密密钥威胁整个系统的安全,这种攻击的目标是机密性、可用性、完整性和真实性。

虚假节点:向网络中添加另一个节点,通过发送恶意数据攻击数据完整性,这反过来又会消耗系统中节点的能量,从而导致拒绝服务攻击。

节点中断:停止节点服务,从而很难从这些节点读取和收集信息,并发起各种其他影响可用性和完整性的攻击。

基于路径的拒绝服务:沿路由路径向基站发送大量数据包,淹没数据包,导致节点电池耗尽,网络中断,从而降低节点的可用性。

共振:强迫受损的传感器或控制器以不同的谐振频率工作。

3.2.2 传输层面临的攻击

对这一层的攻击是在信息传输期间以数据泄漏的形式进行的,这是由于传输媒体的开放性,特别是在无线通信中。这类攻击通过无线电接口捕获传输的消息,冒充合法用户,对其进行修改和重传,或在异构网络之间交换信息。此外,一些其他因素,如大量网络节点之间的远程访问机制,可能导致交通阻塞,也会增加受到攻击的可能性[13]。这一层常见的攻击包括流量分析、篡改、耗尽、碰撞、黑洞、洪水、陷阱门、下沉节点、误导性天坑、虫洞、错误路径选择、隧道、非法进入等,通过手段影响网络内部节点之间的正常通信。以下是传输层常见的攻击形式:

路由:创建可能导致抵抗网络传输、增加传输延迟或扩展源路径的路由循环。

虫洞:通过宣布所有数据包路由的错误路径在网络中建立信息漏洞。

干扰:干扰传感器节点和远程基站之间的无线信道,以引入噪音或同频率的信号。这种攻击会造成有意的网络干扰,从而导致拒绝服务。

选择性转发:使一个受损的节点丢弃且丢弃数据

包,并转发选定的数据包。在某些情况下,受损节点停止将数据包转发到预定的目的地,或者只转发选定的消息并丢弃所有其他数据包,而此节点被认为是合法的。

3.2.3　应用层面临的攻击

由于这一层收集了大量的用户信息,这里的攻击会导致数据损坏、隐私丢失以及对设备未经授权的访问,应用层的常见攻击包括用户隐私泄漏、未经授权访问、恶意代码、数据库和控制命令伪造攻击[14]。应用层在对大量用户数据进行挖掘以改善服务时,就会导致用户的个人隐私面临着巨大威胁,用户的个人隐私很有可能由于不安全的数据传输和存储而被泄露。此外,应用层也可能遭受非授权访问攻击,包括未认证用户假冒已认证用户进入网络和已认证用户擅自扩大自己的权限等访问攻击。这一层的常见攻击例子包括:

缓冲区溢出:利用软件中任何导致缓冲区溢出情况发生的漏洞,并利用此漏洞发起攻击。

恶意代码:通过启动各种恶意代码(如病毒和蠕虫)攻击用户应用程序,并导致网络减速或造成损坏。

3.3　CPS 安全分析

CPS 中的安全挑战可分为两大类:(1)与实现所需功能相关的异构技术带来的挑战;(2)应用安全功能所带来的挑战。由于 CPS 与 Internet 的广泛连接,CPS 的安全体系结构将包括因特网、无线传感器网络和移动通信网络中的所有安全问题。CPS 没有像传统 IT 那样具有统一的执行或计算处理能力以达到高安全性的要求,因此,基于动态变化的环境采用任何统一的安全机制都是很有挑战性的。

目前提出的大多数安全解决方案都试图在每个层解决不同的安全问题,虽然这种办法可能有助于确保系统所需部分的安全,但风险可能来自该系统的其他部分。为了克服这一问题,CPS 的安全体系结构用于通过从底层到顶层的所有层(如信息收集、传输和处理)来保护安全性。在接下来的内容中,对 CPS 的每一层的安全需求进行了自下而上的分析,因为在每一层都有许多安全问题需要考虑,且从多层结合的角度分析系统的安全性能,以保护这些系统免受攻击。

3.3.1　物理层的安全性分析

这一层的主要目标是对象感知、识别和数据收集,但是,连接设备的数量会导致额外的安全漏洞,保护这些装置和防止任何的信息泄露是非常重要的。添加室外环境中的设备也可以被攻击者利用,以泄露信息或分析系统情况,从而导致物理攻击,例如篡改设备组件或用另一设备替换原有设备,因此,添加任何新设备都是一个需要考虑的重要问题。

许多物理层设备缺乏身份验证支持,这反过来又允许未经授权的访问,并公开私有信息或安装可能危害系统的恶意程序,然而由于许多原因,将身份验证应用于此类设备是非常困难的,在这一层实现身份验证的合适机制是加密。然而,在某些情况下,由于受约束设备的资源有限,无法实现足够的加密功能。

总之,身份验证和访问控制进程将阻止来自无效节点的访问,且防止物理攻击,在数据传输过程中,数据加密将保护数据的机密性以及保证私有数据不被泄露。

3.3.2　传输层的安全性分析

虽然网络在连接设备和为用户提供便捷方面得到了广泛的应用,但它们暴露了各种各样的安全问题,很容易受到攻击者的攻击或窃听。例如,无线可访问性为用户提供了极大的便利,但攻击者却也可以与网络进行交互,造成一些损害或窃取有价值的信息[15]。CPS 通信不同于 Internet 中仅限于机器到人的通信,它引入了机器与机器之间的通信。由于设备连接之间缺乏兼容性,机器对机器的数据传输带来了安全问题。这些安全问题无法使用当前的网络协议来解决,这些协议主要是为 Internet 设计的,虽然这些协议仍然提供了一些保护机制,但它们并不是最佳的解决方案。

为了保护网络中的设备以及网络本身,设备应该能够检测出任何可能影响系统安全性的异常行为或情况,这需要在设备端安装具有稳定的传输协议以及入侵检测功能的软件。传输层的安全性可分为两类,第一类来自连接设备,第二类来自相关技术,以及在实现过程中所设计的相关协议的缺陷。

3.3.3　应用层的安全性分析

该层包含许多应用程序,每个应用程序自身的漏洞可能会影响 CPS 安全性,此层可能包含不同的应用,如智能家居和智能城市中的服务和工业监控。主要的安全问题是此设计导致的漏洞可被攻击者用来攻击系统,可以启动恶意代码或软件以影响系统安全性。另外一个安全问题可能是各种技术集成的结果,这些技术可能会阻碍数据处理,从而在系统中造成瓶颈。这些安全问题会影响系统的可用性和可靠性。

应用层的安全性包括信息访问、用户身份验证、信息隐私和平台稳定性。每个应用程序都有自己的安全需求,而且由于被实时监视和控制的系统应用越来越广泛,对提供这类需求的要求也在增加。事实上,需要考虑的复杂安全问题的数量取决于应用程序的类型,所以,如果不考虑系统的底层执行操作,就很难设计出彼此完全信任的应用程序。另一个问题是,不同的行业标准有不同的 CPS 应用程序,目前,还没有全球标准规范的 CPS 应用程序的交互和开发,这就加剧了安全性的不足,意味着不同的应用程序环境需要不同的

安全需求。

在设计 CPS 应用程序时,需要考虑许多安全问题,包括:针对各种应用程序的不同身份验证机制,使得在保证身份验证时的集成非常复杂;大量连接的设备和共享的数据导致大量的应用程序开销。

4 信息物理系统的安全解决方案

4.1 物理层安全措施

CPS 物理层主要涉及各节点基础设施的物理安全、感知数据的采集以及控制命令的执行。需要保障传感器、执行器、RFID 装置、图像捕捉装置等设备的安全,是信息物理系统安全的基础。以下是针对物理层安全威胁的一些安全措施:

(1)对节点的身份进行适当的管理和保护。这可以在一定程度上延长节点的认证时间,在实际应用中可以权衡系统的安全性和效率,制定较为平衡的节点认证策略。

(2)通过生物识别和近场通信等技术,更好地保护节点感知数据的安全性。

(3)加强立法,对利用 CPS 威胁用户或者系统安全的行为建立法规,明确违法行为及其需承担的后果。

(4)对密码与密钥技术、隐私保护技术、安全路由技术、安全数据融合技术和安全定位技术等进行深入研究。

4.2 传输层安全措施

数据传输层的安全措施主要是为了确保系统的通信数据安全,包括数据的完整性、机密性和一致性等。数据传输层的安全机制可综合利用点到点的加密机制和端到端的加密机制。

(1)点对点加密机制保证数据在传输过程中的安全性,但由于每个节点都可以得到明文数据,因此对节点的可信度要求较高,安全机制包括节点认证、逐跳加密和跨网认证等。

(2)端对端加密机制主要实现端到端数据的机密性,并可以提供不同安全等级的灵活安全策略,安全机制包括端到端的身份认证、密钥协商以及密钥管理等。

4.3 应用层安全措施

应用层是 CPS 做出决策的核心部分,系统中的海量数据要求应用控制层要有较强的数据处理能力,同时必须对数据的安全性和用户隐私数据进行保护,对应用层的安全措施包括:

(1)加强系统的访问控制策略以及不同应用场景的身份认证机制和加密机制。

(2)在不影响各应用的同时为信息物理系统建立起一个统一高效的安全管理平台。

4.4 多层结合的安全措施

在一个层中实现安全性并不能满足所需的安全目标,因此,系统的三层之间以及跨域安全解决方案之间应该进行协作,目前一些研究人员正专注于研究作为所有 CPS 框架的安全解决方案。然而,每一层都有不同的要求,这反过来又导致任何的解决方案都非常复杂,因此,重点必须是开发一种替代机制以适应所用设备的限制。

目前提出一种依赖于组合公钥的离线认证机制[16]。该机制的主要目的是解决与大规模数据集认证相关的安全问题,该安全体系结构为传感器数据、标签隐私和数据传输提供了安全保护,所应用的方法包括集成节点的认证有效性以及身份识别。为了提高网络的安全性,该方法将应用层、传输层和物理层结合起来构建可信系统。在应用层,使用可信访问控制来增强合法访问,唯一地验证连接的设备,然后执行代码验证,以便在开放和不安全的网络环境中保持运行,再使用可信数据库提供数据访问相互认证。在传输层,组合公钥专用通信芯片嵌入无线或有线通信设备,在物理层,标签嵌入椭圆曲线密码算法以提供授权访问,并与基于身份的认证组合公钥一起使用,以提供快速身份验证。

还有一些研究者提出了用于一般 CPS 的感知安全框架,安全框架包括三个重要的安全部分:感知、网络和控制。该框架使用参数来确定系统的行为、态势信息和环境情况,以计算系统的安全性水平,并改进信息安全决策。它将相关的信息集成到多个安全措施中,例如加密、密钥协议和访问控制,以使 CPS 安全适应于物理环境。安全框架的主要目标是保密性、可用性、完整性和真实性。该方法将 CPS 的功能划分为四个阶段:监测物理过程和环境;联网,包括数据汇总和传播;对在监测阶段收集到的数据进行分析和计算;执行确定动作。该方法的目的是为 CPS 提供一种动态适应物理环境的安全机制。

5 CPS 的未来研究方向

CPS 在创造新的市场和解决社会风险方面具有很高的潜力,但对质量、安全和隐私等方面提出了很高的要求,要实现可预测的核查和测量质量水平,有效应对外部和内部变化,就必须进行基础科学研究。基于以上对 CPS 最新安全研究的分析,未来的研究方向包括以下几个方面:

(1)CPS 组件认证方法的开发,组件认证机制的存在,以及传感器和控制器之间的安全通道的存在,使 CPS 不受任何篡改,安全性得以提高[17]。

(2)发展保障个人资料安全的方法,随着数据挖

掘技术的日益普及和发展,个人机密信息的安全问题面临着严重威胁。未经授权访问个人数据可能会侵犯数据隐私,而机器学习算法的广泛应用允许恶意用户使用智能数据分析来访问私有信息,这个问题可以从伦理和技术两个方面来解决[18]。

(3)CPS 安全体系结构的发展,随着网络的快速发展以及物理威胁的产生,CPS 面临越来越多的问题,有必要创建一个可靠和容错的体系结构,以确保高水平的安全性和成本效益。

(4)制定提高 CPS 生存能力的对策,为了最大限度地减少 CPS 中的漏洞,制定对策是一项紧迫的任务,有必要开发防御机制并评估它们对 CPS 生存能力的影响。

(5)安全协议开发,CPS 中越来越多的设备对确保数据机密性和完整性的安全标准和协议提出了质疑,智能安全协议的使用允许 CPS 体系结构的自我采纳和自我控制,并将它们集成到创新的、先进的设备中,这是最优先的任务之一。

6　结束语

文中详细介绍了 CPS 中的重要安全因素以及各个层次面临的安全挑战和攻击方式,并针对所面临的安全问题提出了相应的解决措施,最后阐述了 CPS 的未来研究方向。CPS 的研究是一项长期的计划,其应用涉及各个领域,是一项庞大的综合性、复杂性系统。所以对 CPS 的研究必须着眼于现在,展望于未来数十年或更长时间进行的系统设计、构造、实现、优化和跟踪,使研究者按照需要进行有计划、分阶段的研究。对于 CPS 的研究面临的挑战与机遇并存,只要能够科学的分析、优化决策,持续地开展与研发,按需引导,必定会获得发展与成功。

参考文献:

[1] MO Yilin, KIM T H J, BRANCIL K, et al. Cyber physical security of a smart grid infrastructure[J]. Proceedings of the IEEE, 2012, 100(1): 195-209.

[2] LEE I, SOKOLSKY O, CHEN Sanjian, et al. Challenges and research directions in medical cyber physical systems[J]. Proceedings of the IEEE, 2012, 100(1): 75-90.

[3] ALI S, QAISAR S, SAEE H, et al. Network challenges for cyber physical system with tiny wireless devices: a case study on reliable pipeline condition monitoring[J]. Sensors, 2015, 15(4): 7172-7205.

[4] SCHWAB K. The fourth industrial revolution[R]. [s. l.]: World Economic Forum, 2016.

[5] 中华人民共和国国务院. 中国制造 2025[R]. 北京:中华人民共和国国务院, 2015.

[6] STANKOVIC J A. Research directions for the Internet of Things[J]. IEEE Internet of Things Journal, 2014, 1(1): 3-9.

[7] WANG L, WANG X V. Cloud-based cyber physical systems in manufacturing[R]. London: Springer International Publishing, 2018.

[8] SOBHRAJAN P, NIKAM S Y. Comparative study of abstraction in cyber physical system[J]. International Journal of Computer Science and Information Technologies, 2014, 5(1): 466-469.

[9] KHAN R, KHAN S U, ZZHEER R, et al. Future internet: the internet of things architecture, possible applications and key challenges[C]//International conference on frontiers of information technology. Islamabad, India: IEEE, 2012: 257-260.

[10] LU Tianbo, LIN Jiaxi, ZHAO Lingling, et al. A security architecture in cyber physical sysrems: security theories, analysis, simulation and application fields[J]. International Journal of Security and Its Applications, 2015, 9(7): 1-16.

[11] HU Wei, OBERG J, BARRIENTOS J, et al. Expanding gate level information flow tracking for multilevel security[J]. IEEE Embedded Systems Letters, 2013, 5(2): 25-28.

[12] MAHMOUD R, YOUSUF T, ALOUL F, et al. Internet of Things(IoT) security: current status, challenges and prospective measures[C]//10th international conference for internet technology and secured transactions. London, UK: IEEE, 2015: 336-341.

[13] BHABAD M A, SCHOLAR P G. Internet of things: architecture, security issues and countermeasures[J]. International Journal of Computer Applications, 2015, 125(14): 1-4.

[14] PENG Yong, LU Tianbo, LIU Jingli, et al. Cyber physical system risk assessment[C]//Ninth international conference on intelligent information hiding and multimedia signal processing. Beijing, China: IEEE, 2013: 442-447.

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

[16] ZHANG Bing, MA Xinxin, QIN Zhiguang. Security architecture on the trusting internet of things[J]. Journal of Electronic Science and Technology of China, 2011, 9(4): 364-367.

[17] NOURIAN A, MADNICK S. A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(1): 2-13.

[18] OUADDAH A, MOUSANNIF H, ELKALAM A A, et al. Access control in the internet of things: big challenges and new opportunities[J]. Computer Networks, 2017, 112: 237-262.