DOI:10.13878/j.cnki.jnuist.2017.04.003

陈功谱[1,2]　曹向辉[1,2]　孙长银[1,2]

信息物理系统安全问题研究进展

摘要

信息物理系统(CPS)融合控制、通信和计算等技术,使人与物理世界的交互更加便利.在智慧城市、智能电网、智能制造等领域,CPS 被广泛认为是一项革命性技术.在这些应用中,由于信息安全引起的 CPS 系统安全问题,成为系统设计必须考虑的关键因素之一,并受到越来越多研究者的关注.本文旨在提供针对 CPS 安全问题研究的一种视角.首先介绍了几类具有强大破坏力的信息安全攻击,进而对现有针对这些攻击的分析、检测与防御方法进行了综述.最后讨论了 CPS 安全研究仍然存在的挑战.

关键词

信息物理系统;系统安全;隐私;信息攻击

中图分类号 TP13

文献标志码 A

收稿日期 2017-05-11

资助项目 国家自然科学基金(61573103);东北大学流程工业综合自动化国家重点实验室开放课题(PAL-N201601);中央高校基本科研业务费专项资金(2242016K41068)

作者简介

陈功谱,男,硕士生,主要研究方向为信息物理系统.gp_chen@seu.edu.cn

孙长银(通信作者),男,教授,国家杰出青年基金获得者,主要研究方向为非线性系统控制. cysun@seu.edu.cn

1 东南大学 自动化学院,南京,210096

2 东南大学 复杂工程系统测量与控制教育部重点实验室,南京,210096

0 引言

近年来,随着嵌入式系统、网络通信、泛在感知与计算、自动控制等技术的不断发展与交叉融合,信息世界与物理世界的交互不断深入,促使了信息物理系统(Cyber-Physical System,CPS)的提出和发展.CPS 的概念尽管早在 2006 年就由 Helen Gill 在美国国家科学基金会会议上提出[1],并很快引起了广泛的关注与研究,但由于其自身的高复杂度和较广泛的学科交叉,人们从各自领域出发给出了不同的定义方式.例如,加州大学伯克利分校的 Shankar Sastry 认为信息物理系统就是集成了通信、计算和存储,能实时、可靠、安全、稳定地运行,并且能监控物理世界各实体的网络化计算机系统[2].而另一学者 Edward A.Lee 则认为信息物理系统是一系列计算进程和物理进程的紧密集成,通过计算核心来监控物理实体的运行,而物理实体又借助于网络和计算部件实现对环境的感知和控制[3].美国国家科学基金会将信息物理系统定义为依赖于计算算法和物理现实部件无缝融合基础上的人工系统[4].

CPS 融合了控制、通信与计算等技术(即所谓的 Control,Communication,Computation 组成的 3C 技术),通过对物理对象的认知、通信和控制实现人与物理世界进行交互的信息化、自动化和智能化[5-7],其基本结构如图 1 所示.CPS 在航空航天、工业生产、智能电网、交通系统以及远程医疗等领域具有广泛的应用前景[8-10].例如,德国政府提出“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,进一步提升了全球竞争力[11].我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”[12].

系统安全是 CPS 面向实际应用的关键性新问题.在 CPS 中,信息空间和物理空间的深度融合带来了重要的技术优势,但同时也使攻击者可能通过攻击信息空间来侵入物理空间,进而对后者恣意破坏,其破坏程度之大、危险系数之高往往是 CPS 设计者和管理者始料未

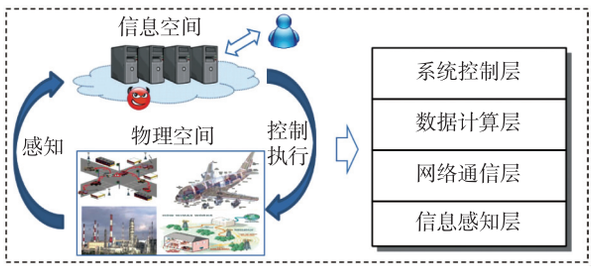

图 1　信息物理系统及其主要构成

Fig. 1　Architecture of cyber-physical-systems

及的.例如,2015 年 12 月 23 日,乌克兰西部地区约 22.5 万居民家中停电数小时,部分地方甚至引起民众恐慌,而该事件被认为是一例网络攻击造成的大停电事件[13].面对信息攻击,工业控制网络也无法幸免,如图 2 所示,据来源于权威机构 ICS-CERT 和 OSVDB 工控网络安全数据库的数据表明,自 2010 年起,安全事故数量逐年大幅上升,特别是重大工业控制网络安全事件呈现爆炸式增长[14].近年来,由于信息空间安全引起的 CPS 系统安全问题受到越来越多的学者和研究人员的关注.

虽然攻击信息空间仍然是针对 CPS 的主要攻击手段,但是 CPS 安全问题和传统的信息安全问题存在很大不同,主要表现在以下几个方面[15-17]:

1) CPS 不再区分安全等级[16].传统的信息系统对系统内的各组件是区分安全等级的,如服务器的安全等级要高于网络边缘的客户端的等级,因此服务器的防御要高于客户端.但是在 CPS 中没有这种区分,中心的控制器和边缘的执行器对系统安全的重要性是同等的.

2) 软件补丁和频繁的更新不再适用于 CPS[17].在传统的信息系统中经常使用补丁和更新的方式来改进防御系统,但是 CPS 往往涉及到大规模工业生产或者重要基础设施,而更新和升级补丁需要暂时

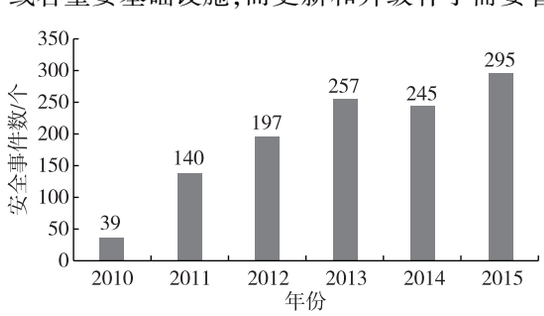

图 2　ICS-CERT 统计的工业控制系统安全事件[18]

Fig. 2　Statistics of security incidents in industrial control systems by ICS-CERT[18]

停止系统运行,这不仅需要事先制定复杂的脱机计划,还往往意味着相当的经济损失.

3) CPS 对实时性和可靠性的要求不同于信息系统[16].信息系统是所谓软实时系统,它对实时性的要求是在一定的时间长度内完成操作.而 CPS 是硬实时系统,它要求的是在一个固定的时间节点之前完成操作.对于信息系统来说,达不到实时性要求可能只会降低服务质量,但对于 CPS 来说,错过系统要求的时间节点往往就意味着整个系统运行的失败.

如前所述,与传统的信息安全相比,CPS 安全面临的是更加严峻、更加复杂的情况,而且由于 CPS 与国民生产和人类生活的紧密联系,其重要性比传统信息安全有过之而无不及,所以急需更多研究者的关注和努力.

1　CPS 安全威胁

由于信息物理系统中信息空间与物理空间的高度融合,通过入侵信息空间进而破坏整个系统的信息攻击成为 CPS 的主要安全威胁.在网络通信的发展中,信息攻击始终是挥之不去的安全隐患,并且随着通信技术的发展也一直在发展,甚至早在 CPS 提出之前就已经形成了种类繁多的攻击方式,而现在这些攻击大多也可以直接对信息物理系统造成破坏.根据攻击者是否具有被攻击系统的相关知识,信息攻击大体可以分为以下几种方式:

1)干扰通信.攻击者通过干扰甚至阻断系统中节点之间的通信链接和数据包路由,使系统丧失实时管控能力,从而对系统的运行和性能造成破坏.由于攻击者的目的是破坏系统通信,干扰甚至截断系统的信息流,因此这种攻击方式对攻击者相关知识要求较低,攻击者只需要从一般化的通信信道着手就可实施攻击,甚至几乎不需要了解系统中物理对象的相关信息.此外,由于攻击者并不关心通信中传递的数据内容,所以对数据进行加密传输很难对这种攻击构成挑战.干扰通信最主要的方式就是 DOS 攻击[19].DOS 攻击一般通过向网络发送大量的数据,使网络忙于处理这些无意义的数据从而无法响应正常服务请求.DOS 攻击的攻击者只需要掌握系统组件之间的通信协议,就可以据此开展多种形式的攻击,包括对控制器或网络进行泛洪攻击[20]、对控制器或网络发送无效数据致其非正常终止运行、DDOS 攻击和信道拥塞攻击等.其中信道拥塞攻击(channel jamming attack)是 DOS 攻击的一种主要形

式,它通过干扰无线信号来降低接收端的信噪比,从而破坏现有的无线通信[21].文献[22]指出,拥塞攻击是无线传感器网络(WSNs)领域面临的最严重威胁,因为它可以无视 WSNs 的初始化设计和上层安全机制,轻易地使目标系统陷入混乱.此外,WSNs 在实际应用中的诸多限制,如较低的计算能力、有限的存储资源和能量资源以及使用不安全的通信信道等,更加削弱了其对拥塞攻击的抵抗力.

2)获取隐私.攻击者对系统中节点间的通信数据、数据流向及流量等信息进行监听,经过适当的数据分析技术,窃取系统中的关键参数、运行数据等隐私信息,理解并掌握系统的运行状态,从而有利于其采取进一步的入侵式攻击.窃听者需要对系统具有一定的相关知识,才能从监听到的数据中分析得到想要的、有价值的信息.攻击者可以通过特殊的设备和软件来窃听系统正在使用的信道,捕获其中传输的数据.此外,攻击者可以实施中间人攻击(man-in-the-middle attack)[23],即在通信双方都不知情的情况下介入他们的通信,分别伪装二者各自正确的通信对象,从而不仅可以窃听二者的通信数据,甚至还可以转发经过篡改的数据以达到破坏目的.攻击者窃听到数据后,通过数据分析获取物理系统大量信息,例如通过数据流量分析获得传感器采样周期、控制周期等信息,通过传感器数据滤波获得物理系统状态信息,通过输入输出分析并结合系统辨识获得物理对象模型,通过分析控制信号获取控制器参数等.

3)入侵攻击.对于功能强大的攻击者,若其已经掌握了系统大量相关知识,就可以侵入系统内部,干扰或破坏其他节点的正常运行、劫持或瘫痪系统运行、制造系统性破坏等.例如,若攻击者已经获得相关通信密钥和节点地址信息,就可以通过修改地址数据伪装成正常节点甚至系统管理者,发送有害信息对系统进行破坏.ARP 攻击就是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗的,它能够在网络中产生大量的 ARP 通信量使网络拥塞,攻击者只要持续不断地发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP-MAC 条目,造成网络中断或中间人攻击[24].另一种典型的入侵攻击是网络钓鱼攻击,它将恶意邮件或者网站伪装成合法的样子然后欺骗用户输入自己的个人信息,或者欺骗用户下载、安装恶意软件,然后通过该软件来扫描甚至监控用户的设备以获取其隐私信息[25].这些网络入侵攻击方式在信息物理系统中极易造成很大破坏,例如攻击者侵入某个控制器中并迫使后者发送错误的控制命令,从而使系统出现不稳定.震网(Stuxnet)应该是入侵攻击中最具代表性的一种,作为第一个被发现的网络武器,它制造了轰动世界的伊朗核电站事件[26].震网病毒通过 USB 接入感染,侵入系统后会检测该系统是否为目标系统,如果是则开始尝试接入互联网并下载它自己的最新版本,然后利用零日漏洞迅速展开攻击.它会监视目标系统的操作并收集相关的信息,然后利用这些信息来控制目标系统(比如伊朗核电站事故中的离心机)并使之错误运行,同时它还会向外界的控制器提供错误的反馈,使之无法发现运行错误,直至对系统造成不可挽回的破坏[27].

这些攻击方式从系统外部逐渐深入到系统内部,从干扰运行到劫持系统,对信息物理系统的安全运行构成层次渐深、危害渐大的破坏.我们也注意到,单纯通过信息加密已经难以有效应对以上所有攻击方式,同时,由于信息空间和物理空间的融合,促使我们必须同时考虑两种空间,采用通信、计算和控制相融合的安全技术,来提升系统的安全性和可靠性.

事实上,CPS 的安全问题并不局限于信息安全.由于 CPS 是一个信息和物理相融合的系统,攻击者不仅可以从信息空间入侵,有时候甚至可以直接影响物理组件来实现攻击目的[28].比如攻击者可以通过对温度传感器加热的方式来从物理上制造错误的测量数据.类似的这种全新的攻击方式已经不是传统的信息安全策略所能应对的了,这就更加要求研究者从系统和控制的角度出发,重新审视 CPS 安全问题.

2 CPS 安全的研究进展

近年来,CPS 的安全问题研究逐渐受到国内外学者的关注,成为相关领域的热点方向之一.虽然针对 CPS 的攻击方式和传统的网络攻击方式有很多相似之处,但正如前文所提到的,信息物理系统信息空间和物理空间深度融合的这一特性,使得信息物理系统与传统的信息安全问题有很大的不同.这些因素促使 CPS 的安全问题要跳出传统信息安全问题的藩篱,可以也必须要从更多的角度去考虑,而不再仅仅局限于通信的角度.下面根据最新的文献分析,从三个方面来介绍相关研究.

2.1 从计算和通信的角度出发,加强信息空间的安全性

从计算角度出发,现有方法很多集中于数据的

加密及其相关的密钥分配与管理等技术,通过对系统信息和隐私数据的加密,使其免于泄露和免受外界入侵.例如,文献[29-30]提出基于公共密钥的方法对智能电网通信数据包进行加密以保护隐私,这种发送方用公共密钥加密然后接收方用私人密钥解密的方法不仅能实现双向验证,还能确保共享密钥的语义安全.此外,由于在加密信息中带有时间戳,这种方法还可以有效防止重放攻击.IEEE 802.11 和 IEEE 802.15.4 等网络通信标准都提供了数据加密协议[31-32].然而,由于加密本身带来的复杂度,计算和通信的代价为之提高[33],因此,相关研究提出了通过代理和协同验证等方式,在保护隐私的同时降低加密成本[34-35].例如文献[34]考虑的是在车联网这种典型的信息物理系统中,车辆周期性广播自己的位置信息,然后通过特定的协议来选择周边的车辆作为这个信息的验证者,一旦该信息被验证为无效,验证者就会向周边车辆广播一个警告信息.收到警告信息的车辆会再做第二次验证,这样就能防止在有效位置信息丢失的情况下攻击者恶意发送警告信息带来的误判.这样一来,验证过程就通过邻近车辆的相互验证完成,从而可以降低系统的加密成本.

同时,从网络通信角度出发,针对拒绝服务(Denial of Service,DoS)攻击、女巫(Sybil)攻击、洪泛(flooding)攻击、中间人攻击、重放(replay)攻击等,研究者提出了大量安全防御对策,包括节点身份验证、安全路由、安全定位、安全的密钥共建与管理协议等方法,以加强网络通信安全性[9-10,36-43].例如,文献[36]提出一种鲁棒、安全时间同步协议(RTSP)来抵御女巫攻击.该协议采用分布式时间同步算法,除了信息接收、时钟更新和信息广播这三个在时钟同步协议中常见的步骤外,还加入了一个异常检测的安全机制.当接收到足够多的时钟同步信息之后,节点就会实施异常检测算法滤掉错误信息.该算法的核心是通过合法时间戳之间的一致性关系来检测并去掉非法时间戳.文献[37]研究了 CPS 中远程状态估计器面临的拥塞攻击的相关问题,提出了一种基于博弈论的防御策略.考虑到网络中的传感器节点和攻击者节点都受到能量约束,因此对双方来说,何时发送数据或者何时开展攻击是一个相互影响的决策过程.于是文章提出了一个基于博弈论的架构,并证明存在最优策略可以使双方在零和游戏上达到纳什均衡.

总体而言,目前的这些方法能够抵御某些具体的网络通信攻击行为,但大多局限于信息空间,只考虑数据安全和网络通信安全,以保护数据隐私和网络正常通信为主要目标,并没有与物理空间深入结合,没有考虑物理系统的动态性.而信息物理系统除了数据和通信的安全,更在于保护物理系统的安全运行,因此上述方法尚不能完全满足信息物理系统安全性需求.

2.2 从控制的角度出发,加强物理空间的安全性

目前,针对信息攻击下的信息物理系统控制安全性,相关研究主要考虑拒绝服务攻击、重放攻击、注入错误数据(false data injection)等,研究攻击方的最优攻击策略和防御方(被攻击系统)的稳定性及安全控制方法[8,44-64].例如,文献[55]假设攻击者可以通过注入数据来篡改状态估计器的测量值,考虑在这种情况下攻击者和防御者之间可以进行的博弈——因为无论攻击者还是防御者都不能完全掌握所有节点,双方都试图增加或者减少错误数据的注入.文章探讨了在这个零和博弈中最终可以达到的纳什均衡以及双方可以达到的最大收益.文献[46]考虑了 DoS 攻击下线性二次高斯(LQG)控制问题,并提出了最优反馈控制器.文献[48]研究了重放攻击下的 LQG 控制问题,并提出用检测器剔除错误数据和含噪音控制器来检测攻击行为.文献[45,47]研究了重放、注入错误数据等攻击形式下线性控制系统的稳定性问题,并提出了通过增强控制器设计[45]或增加攻击检测与鉴别观测器[47]等方法来改善系统安全性.文献[56]则将隐秘的攻击当成影响系统状态和传感器测量的一个输入,然后定义了攻击的可检测性和可识别性,并设计了相应的检测算法.虽然很多方法考虑了信息攻击,但在研究中往往将攻击简化为造成数据丢包(针对 DoS 攻击)或在系统中注入有害数据,并没有深入信息空间内部分析攻击的形成或攻击效果.例如,在无线网络中,针对 DoS 攻击,其往往由于攻击者制造干扰信号所引起,考虑到实际中无线通信信道的动态性以及路径衰减等性质,DoS 攻击将体现在时域、频域和地域等多个维度上.

文献[57]考虑在智能电网中如何利用卡尔曼滤波防御各种类型的攻击,提出了一种结合卡尔曼滤波器 χ^2 探测器[64]和欧几里得探测器的安全智能电网框架.其中 χ^2 探测器能够检测重放攻击、DoS 攻击,但不能检测到错误数据注入的攻击,而欧几里得探测器可以检测错误数据注入的攻击.文献[58]研

究了单个传感器、单个系统的无线状态估计中,当传感器具有一定的能量限制时,如何选择发送数据的时机以使得系统的估计性能达到最优,并且给出了具体的调度方案.文献[59]则考虑无线状态估计中,被测系统可以同时被两个传感器检测,但是由于传输带宽的约束,同一时刻最多允许一个传感器向远程状态估计器发送本地状态估计信息的情况,并给出了这种情况下传感器的最优调度方案.

文献[50-51]提出了针对无线状态估计和网络控制的最优 DoS 攻击调度策略.其中文献[50]指出攻击者受到能量限制时,最优的攻击为连续攻击,且连续攻击可以在[0,T]的任意位置.文献[60]将文献[50]中的单系统情况扩展到多个独立传感器、多个独立系统的情况,并且假设攻击者由于信道带宽限制,同一时刻只能攻击一个信道,此时攻击者的最优攻击策略与系统参数、攻击者的能量限制有关.文献[61]则考虑系统的带宽有限时,两个独立系统之间如何调度可以使得两个系统的平均误差协方差之和达到最优,并给出了具体的调度方案.另外,也有一些学者同时考虑攻防双方,例如,文献[62]研究了在无线传感网中最优的干扰与防御策略,文献[63]则从博弈论的角度研究攻击方与防御方的博弈问题,构建了一个马尔可夫游戏框架,并利用一种改进的纳什 Q-learning 算法求得问题的最优解.

分布式计算与控制系统(如多智能体系统)是 CPS 的典型应用场景,一致性(consensus)算法在这些系统中有着重要的作用,但是在一致性过程中需要和周边节点进行的信息互换同样带来了信息泄露的风险,因此一致性算法的隐私保护问题也引起了很多学者的关注.文献[65]研究了在平均一致性算法中如何保护节点的初始状态不被泄露的问题,提出了一种通过加减随机噪声的方法来实现隐私保护.每个节点在广播自己的状态之前独立产生一个符合标准正态分布的随机噪声,然后将这个噪声加到自己当前状态中再广播出去.这样所有节点收到的其他节点的信息都不是真实的,但由于所有噪声都符合标准正态分布,因此不会对最后要达到的平均值造成影响,也就能在保护了节点隐私的前提下达到系统一致性.而文献[66]则研究了在最大一致性算法中的隐私保护问题,给出了被称之为 PPMC 的隐私保护算法.每个节点在发送初始状态之前随机产生一列不大于自身状态的随机数(其个数也是随机的),并将这列随机数的第一个作为自己的初始状态广播出去,然后在每次迭代中取随机序列中对应的随机数和上一时刻周边节点状态之间的最大值作为自己的新状态,直到自身状态和周边节点的状态都相等为止.

2.3 环境感知的综合安全技术

因为信息物理系统本身都和其所处的物理环境紧密相连,切实地考虑系统与环境的相互作用也有利于提高系统安全性.文献[67]提出了一种被称之为 CYPSec 的解决方案,它考虑了传统的安全因素与环境信息的交互,利用 CPS 所自带的监控能力来保证系统安全.该方案研究的是在体域网(Body Area Networks)的场景下,提出了一种基于生理信号的密钥协商(PSKA)方法,利用生理信号(比如心电图)来达成体域网中两个传感器的对称密钥协商.为了证明 CYPSec 解决方案的可行性,该文章还提出了一种环境耦合型的接入控制模型.

文献[68]研究了基于上下文感知的安全架构,如图 3 所示,该方法设想将系统所处环境的各种状态和信息融入到传统的安全手段如认证、加密、接入控制等过程中,使 CPS 的安全机制能够动态地适应所处的环境.CPS 因其系统需要,本身就需要收集大量的环境数据,包括系统环境(如 CPU、网络状态等)、物理环境(如温度、光照等)以及时间等在内的信息,将这些物理数据再利用并有机地融入到安全机制中也是 CPS 安全的一个新思路.

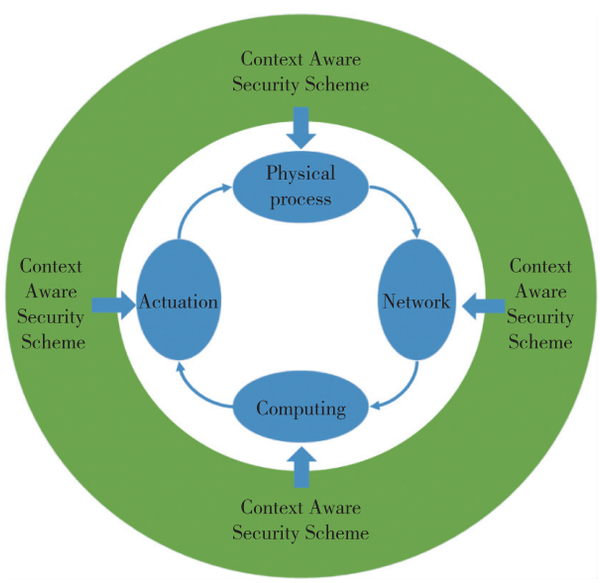

图 3 基于上下文感知的安全架构[68]

Fig. 3 The context-aware security framework [68]

3 CPS 安全的研究挑战

由于 CPS 已经渐渐成为国民生产和人类生活的重要组成部分,而其潜在的安全隐患又意味着巨大的破坏效应,所以世界各国都在积极推进 CPS 安全问题的理论研究和科学实践,CPS 安全问题也已成为国内外学者的研究热点.尽管大量的相关研究已经从各个角度对这个问题进行了探索,但是安全问题向来是攻防双方相互刺激、此消彼长的不断演进的过程.不断复杂化的安全形势也给 CPS 安全问题带来了许多挑战[69-71],具体可以总结为以下几个方面:

1)信息空间和物理空间融合所带来的新的安全问题.目前安全领域大多数成熟的研究成果都是针对传统的信息安全,也就是说只考虑了信息空间的安全问题.但是 CPS 是一个融合了计算、通信和控制的综合系统,CPS 安全的目标也不再局限于传统信息安全的机密性、完整性和可用性.例如前文所提到的,由于 CPS 和物理进程的紧密结合使得其对实时性有着严格的要求[16],达不到实时性要求往往将导致系统的失败,这一特性势必会成为 CPS 的一个安全弱点而被攻击者利用.充分分析和认识这种二元空间的融合下存在怎样的新的安全隐患是当下急需解决的一个问题,然后需要在此基础上考虑新的防御策略.

2)嵌入式系统的资源局限性所带来的安全漏洞.CPS 当中往往存在大量的嵌入式组件,而嵌入式系统的特点是要求专用性强、系统精简.为了节约成本、降低能耗,嵌入式系统的计算、存储等各方面的资源通常是很有限的,因此很多嵌入式操作系统和网络协议栈都是被精简的,这就可能会带来很多安全漏洞.如何在这样资源受限的情况下实现上层软件的安全功能也成了一个难题.

3)通信干扰下 CPS 的安全控制与方法.如前所述,通过干扰通信的攻击形式不依赖于系统知识,并且不易受数据是否加密传输的影响,因此易被恶意节点所使用.为了分析这种攻击的破坏力,从攻击者角度出发,研究最优的攻击策略及其对系统所造成的最大影响,对实际系统的设计具有指导意义.进一步,通过研究攻防两方的对策,可以对防御措施进行综合评估和分析设计,保障系统的稳定、安全运行.

4)隐私保护的系统分析与控制.对于攻击者而言,了解并掌握系统的参数、状态和运行规则,是实施进一步破坏行动的基础.特别是在无线网络化系统中,无线通信数据很可能会被其他临近恶意节点侦听到,即使在有向天线的帮助下,通信仍可能被处于链路之间的节点所捕获.如果没有良好的隐私保护机制,其后果可能包括:通信数据流信息以及数据本身被窃听,造成系统重要隐私数据(例如系统参数、用户信息等)泄露给他人;恶意节点通过对窃听的数据进行分析,掌握系统的真实运行状态,从而伪装成正常节点对系统进行破坏;恶意节点还可以对捕获的数据进行篡改后发送出去,以迷惑接收者,甚至以此方式劫持某个节点或者整个系统.因此,研究系统隐私保护机制,对于保障系统安全运行、免受劫持和篡改具有重要意义.

5)分布式环境下入侵攻击的检测与防御.当攻击者掌握更多系统知识甚至包括通信密钥时,就可能侵入系统内部,通过伪造地址和身份、篡改或发送有害数据或控制信号、阻碍其他节点的信息传输、诬陷正常节点、包庇合谋攻击者等手段对系统实施最直接的破坏.而且,当入侵节点掌握通信密钥时,可以使其所发信息符合正常的加密规则,导致其恶意行径将很难通过数据认证(authentication)等方式检测出来.特别地,在大规模网络系统中,入侵者可能通过攻击有限范围内的网络节点,达到最终破坏整个系统的效果.因此,如何分布式检测并防御这种入侵行为,对保证系统安全运行、避免事故发生具有重要意义.

4 结束语

CPS 正在引导一场改变人类与物理环境交互方式的大变革,它在工业、农业、交通、航空航天等各个领域都有广阔的应用前景.但所有这些应用都要建立在能够保证系统安全的基础上,否则可能造成的损失将是无法估量的.本文对 CPS 的概念和应用做了概述,并分析了 CPS 安全问题的重要性以及 CPS 存在的安全威胁,随后重点讨论了 CPS 安全问题的研究进展和存在的研究挑战.通过分析发现,针对 CPS 安全问题的研究已引起国内外学者的高度重视,但现有研究仍处于起步阶段,存在很多研究挑战尚待解决,相关研究任重而道远.

参考文献

References

[1] UC Regents.Cyber physical system [EB/OL].[2017-05-10].http://cyberphysicalsystems.org,2011

[2] Sastry S.Networked embedded systems:From sensor webs

to cyber-physical systems[C]//International Conference on Hybrid Systems:Computation and Control,2007:1-1
[3] Lee E A.Cyber physical systems:Design challenges[C]//IEEE International Symposium on Object Oriented Real-Time Distributed Computing,2008:363-369
[4] National Science Foundation. Cyber-Physical systems (CPS)[EB/OL].[2017-05-10].https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286
[5] Wu F K,Kao Y F,Tseng Y C.From wireless sensor networks towards cyber physical systems[J].Pervasive and Mobile Computing,2011,7(4):397-413
[6] Kang W,Kapitanova K,Sang S H.RDDS:A real-time data distribution service for cyber-physical systems[J].IEEE Transactions on Industrial Informatics,2012,8(2):393-405
[7] Rajhans A,Bhave A,Ruchkin I,et al.Supporting heterogeneity in cyber-physical systems architectures[J].IEEE Transactions on Automatic Control,2014,59(12):3178-3193
[8] Mo Y L,Kim T H J,Brancik K,et al.Cyber-physical security of a smart grid infrastructure[J].Proceedings of the IEEE,2012,100(1):195-209
[9] Lee I,Sokolsky O,Chen S J,et al.Challenges and research directions in medical cyber-physical systems[J].Proceedings of the IEEE,2012,100(1):75-90
[10] Ali S,Qaisar S,Saeed H,et al.Network challenges for cyber physical systems with tiny wireless devices:A case study on reliable pipeline condition monitoring[J].Sensors,2015,15(4):7172-7205
[11] Schwab K.The fourth industrial revolution[R].World Economic Forum,2016
[12] 中华人民共和国国务院.中国制造2025[R].2015
State Council of the People's Republic of China.Made in China 2025 strategy[R].2015
[13] 王勇,王钰茗,张琳,等.乌克兰电力系统BlackEnergy病毒分析与防御[J].网络与信息安全学报,2017,3(1):46-53
WANG Yong,WANG Yuming,ZHANG Lin,et al,Analysis and defense of the BlackEnergy malware in the Ukrainian electric power system[J].Chinese Journal of Network and Information Security,2017,3(1):46-53
[14] 李鸿培,于旸,忽朝俭,等.工业控制系统的安全性研究[J].中国计算机学会通讯,2013,9(9):37-42
LI Hongpei,YU Yang,HU Zhaojian.Research on security of industrial control system[J].Communications of the China Computer Federation,2013,9(9):37-42
[15] Moholkar A V.Security for cyber-physical systems[J].International Journal of Computing and Technology,2014,1(6):257-262
[16] Zhu B N,Joseph A,Sastry S.A taxonomy of cyber attacks on SCADA systems[C]//International Conference on Internet of Things and The 4th International Conference on Cyber,Physical and Social Computing,2011:380-388
[17] Cardenas A A,Amin S,Sastry S.Research challenges for the security of control systems[C]//Conference on Hot Topics in Security,2008:6
[18] 北京匡恩网络科技有限责任公司.2016工业控制网络安全态势报告[R].2016
Beijing Kuangen Network Technology Co.,Ltd.Security situation of industrial control network in 2016[R].2016
[19] Peng T,Leckie C,Ramamohanarao K.Survey of network-based defense mechanisms countering the DoS and DDoS problems[J].ACM Computing Surveys,2007,39(1),DOI:10.1145/1216370.1216373
[20] Xiao B,Chen W,He Y X,et al.An active detecting method against SYN flooding attack[C]//IEEE International Conference on Parallel and Distributed Systems,2005:709-715
[21] Grover K,Lim A,Yang Q.Jamming and anti-jamming techniques in wireless networks:A survey[J].International Journal of Ad Hoc and Ubiquitous Computing,2014,17(4):197-215
[22] Mpitziopoulos A,Gavalas D,Konstantopoulos C,et al.A survey on jamming attacks and countermeasures in WSNs[J].IEEE Communications Surveys & Tutorials,2009,11(4):42-56
[23] Nayak G N,Samaddar S G.Different flavours of Man-In-The-Middle attack,consequences and feasible solutions[C]//IEEE International Conference on Computer Science and Information Technology,2010:491-495
[24] Wright J.Detecting wireless LAN MAC address spoofing[R].White Paper,2003
[25] Wu M,Miller R C,Garfinkel S L.Do security toolbars actually prevent phishing attacks?[C]//Conference on Human Factors in Computing Systems,2006:601-610
[26] Langner R.Stuxnet:Dissecting a cyberwarfare weapon[J].IEEE Security & Privacy,2011,9(3):49-51
[27] Kushner D.The real story of stuxnet[J].IEEE Spectrum,2013,50(3):48-53
[28] Wu G Y,Sun J,Chen J.A survey on the security of cyber-physical systems[J].Control Theory and Technology,2016,14(1):2-10
[29] Fouda M M,Fadlullah Z M,Kato N,et al.A lightweight message authentication scheme for smart grid communications[J].IEEE Transactions on Smart Grid,2011,2(4):675-685
[30] Li Q H,Cao G H.Multicast authentication in the smart grid with one-time signature[J].IEEE Transactions on Smart Grid,2011,2(4):686-696
[31] Chen J C,Jiang M C,Liu Y W.Wireless LAN security and IEEE 802.11i[J].IEEE Wireless Communications,2005,12(1):27-36
[32] Xiao Y,Chen H H,Sun B,et al.MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks[J].EURASIP Journal on Wireless Communications and Networking,2006(1):093830
[33] Cao X H,Shila D M,Cheng Y,et al.Ghost-in-ZigBee:Energy depletion attack on ZigBee-based wireless networks[J].IEEE Internet of Things Journal,2016,3(5):816-829
[34] Shen W L,Liu L,Cao X H,et al.Cooperative message authentication in vehicular cyber-physical systems[J].IEEE Transactions on Emerging Topics in Computing,2013,1(1):84-97
[35] Lu R X,Lin X D,Zhu H J,et al.BECAN:A bandwidth-efficient cooperative authentication scheme for filtering

injected false data in wireless sensor networks[J].IEEE Transactions on Parallel & Distributed Systems,2012,23(1):32-43
[36] Dong W,Liu X J.Robust and secure time-synchronization against sybil attacks for sensor networks[J].IEEE Transactions on Industrial Informatics, 2015, 11 (6): 1482-1491
[37] Li Y Z,Shi L,Cheng P,et al.Jamming attacks on remote state estimation in cyber-physical systems:A game-theoretic approach[J].IEEE Transactions on Automatic Control,2015,60(10):2831-2836
[38] Han S,Xie M,Chen H H,et al.Intrusion detection in cyber-physical systems: Techniques and challenges [J]. IEEE Systems Journal,2014,8(4):1052-1062
[39] Li X, Liang X H, Lu R X, et al. Securing smart grid: Cyber attacks, countermeasures, and challenges[J].IEEE Communications Magazine,2012,50(8):38-45
[40] Cao X H,Liu L,Shen W L,et al.Real-time misbehavior detection and mitigation in cyber-physical systems over WLANs[J].IEEE Transactions on Industrial Informatics, 2017,13(1):186-197
[41] Vijayakumar P,Azees M,Kannan A,et al.Dual authentication and key management techniques for secure data transmission in vehicular Ad Hoc networks [J]. IEEE Transactions on Intelligent Transportation Systems,2016, 17(4):1015-1028
[42] He J P,Chen J M,Cheng P,et al.Secure time synchronization in wireless sensor networks: A maximum consensus-based approach [J]. IEEE Transactions on Parallel & Distributed Systems,2014,25(4):1055-1065
[43] Zeng Y P,Cao J D,Hong J,et al.Secure localization and location verification in wireless sensor networks:A survey [J]. The Journal of Supercomputing, 2013, 64 (3): 685-701
[44] Cardenas A A,Amin S,Sastry S.Secure control:Towards survivable cyber-physical systems [C] // IEEE International Conference on Distributed Computing Systems Workshops,2008:495-500
[45] Fawzi H, Tabuada P, Diggavi S. Secure estimation and control for cyber-physical systems under adversarial attacks [J]. IEEE Transactions on Automatic Control, 2012,59(6):1454-1467
[46] Amin S,Cárdenas A A,Sastry S S.Safe and secure networked control systems under denial-of-service attacks [C]//International Conference on Hybrid Systems:Computation and Control,2009:31-45
[47] Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems[J].IEEE Transactions on Automatic Control,2013,58(11):2715-2729
[48] Chabukswar R,Mo Y L,Sinopoli B.Detecting integrity attacks on SCADA systems [J]. IFAC Proceedings Volumes,2014,22(4):1396-1407
[49] Zhu M H,Martínez S.On the performance analysis of resilient networked control systems under replay attacks [J].IEEE Transactions on Automatic Control,2013,59(3):804-808
[50] Zhang H,Cheng P,Shi L,et al.Optimal denial-of-service attack scheduling with energy constraint[J].IEEE Transactions on Automatic Control,2015,60(11):3023-3028
[51] Zhang H, Cheng P, Shi L, et al. Optimal DoS attack scheduling in wireless networked control system [J]. IEEE Transactions on Control Systems Technology,2016, 24(3):843-852
[52] Li Y Z,Shi L,Cheng P,et al.Jamming attacks on remote state estimation in cyber-physical systems:A game-theoretic approach[J].IEEE Transactions on Automatic Control,2015,60(10):2831-2836
[53] Bonaci T,Yan J J,Herron J,et al.Experimental analysis of denial-of-service attacks on teleoperated robotic systems[C] // ACM/IEEE International Conference on Cyber-Physical Systems,2015:11-20
[54] Sridhar S,Hahn A,Govindarasu M.Cyber-physical system security for the electric power grid[J].Proceedings of the IEEE,2012,100(1):210-224
[55] Esmalifalak M,Shi G,Zhu H,et al.Bad data injection attack and defense in electricity market using game theory study[J].IEEE Transactions on Smart Grid,2012,4(1): 160-169
[56] Pasqualetti F, Dörfler F, Bullo F. Attack detection and identification in cyber-physical systems[J].IEEE Transactions on Automatic Control,2013,58(11):2715-2729
[57] Manandhar K,Cao X J,Hu F,et al.Combating false data injection attacks in smart grid using Kalman filter[C]// IEEE International Conference on Computing,Networking and Communications,2014:16-20
[58] Shi L,Cheng P,Chen J M.Sensor data scheduling for optimal state estimation with communication energy constraint[J].Automatica,2011,47(8):1693-1698
[59] Shi L,Cheng P,Chen J M.Optimal periodic sensor scheduling with limited resources [J]. IEEE Transactions on Automatic Control,2011,56(9):2190-2195
[60] Peng L H,Cao X H,Sun C Y,et al.Optimal jamming attack schedule against wireless state estimation in cyber-physical systems[C]//International Conference on Wireless Algorithms, Systems, and Applications, 2016: 318-330
[61] Shi L,Zhang H S.Scheduling two Gauss-Markov systems: An optimal solution for remote state estimation under bandwidth constraint [J]. IEEE Transactions on Signal Processing,2012,60(4):2038-2042
[62] Li M Y,Koutsopoulos I,Poovendran R.Optimal jamming attacks and network defense policies in wireless sensor networks[J].IEEE International Conference on Computer Communications,2007,9(8):1307-1315
[63] Li Y Z, Quevedo D E, Dey S, et al. SINR-based DoS attack on remote state estimation: A game-theoretic approach[J].IEEE Transactions on Control of Network Systems,2016,99:1-10
[64] Brumback B,Srinath M.A Chi-square test for fault-detection in Kalman filters [J]. IEEE Transactions on Automatic Control,2003,32(6):552-554
[65] Mo Y L, Murray R M. Privacy preserving average consensus[J].IEEE Transactions on Automatic Control, 2017,62(2):753-765
[66] Duan X M, He J P, Cheng P, et al. Privacy preserving maximum consensus[C]//IEEE Conference on Decision

and Control,2015:4517-4522
[67] Venkatasubramanian K K,Nabar S,Gupta S K S,et al. Cyber physical security solutions for pervasive health monitoring systems [M] // User-Driven Healthcare: Concepts, Methodologies, Tools, and Applications. Hershey, PA: Medical Information Science Reference,2012
[68] Wang E K,Ye Y M,Xu X F,et al.Security issues and challenges for cyber physical system[C] // IEEE/ACM International Conference on Green Computing and Communications,2011:733-738
[69] 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].信息网络安全,2016(7):20-28
PENG Kunlun, PENG Wei, WANG Dongxia, et al. Research survey on security issues in cyber-physical systems[J].Netinfo Security,2016(7):20-28
[70] 张恒.信息物理系统安全理论研究[D].杭州:浙江大学控制科学与工程学院,2015
ZHANG Heng. Research on security theory for cyber-physical systems [D]. Hangzhou: College of Control Science and Engineering,Zhejiang University,2015
[71] Cardenas A,Amin S,Sinopoli B,et al.Challenges for securing cyber physical systems[C] // Workshop on Future Directions in Cyber-physical Systems Security, 2009: 363-369

A survey on the security of cyber physical systems

CHEN Gongpu[1,2] CAO Xianghui[1,2] SUN Changyin[1,2]
1 School of Automation,Southeast University,Nanjing 210096
2 Key Lab of Measurement and Control of Complex Systems of Engineering, Ministry of Education,Southeast University,Nanjing 210096

Abstract Cyber Physical Systems (CPSs) integrate control,communication and computation technologies to facilitate close interactions between human being and physical world.CPS is widely recognized as one of the revolutional technologies for smart cities,smart grid,intelligent manufacturing and so on.In all of these applications,due to potential vulnerability to cyber attacks,CPS security is one of the key design concerns and has drawn increasing research attention recently.In this paper,we provide a review of recent studies on CPS security.We first introduce several types of security threats that are able to cause severe damage to any target CPS if not well protected.We then present a survey of recent literature on attack analysis,detection and defeating strategies,and discuss a list of research challenges in this area.

Key words cyber physical system;system security;privacy;cyber attacks