DOI:10.3969/j.issn.1672-6685.2015.02.010

工业物联网安全防护体系研究*

杨悦梅[1,2],宋执环[2]

(1.杭州科技职业技术学院 信息工程学院,浙江 杭州 311402;
2.浙江大学 控制科学与工程学系,浙江 杭州 310027)

摘 要:随着物联网技术的发展,其在工业领域的应用也日益广泛,但物联网的安全隐患对其在工业领域的应用提出了新的挑战.分析了工业物联网特有的潜在攻击形式,通过建立工业物联网层次化安全防护体系模型,详细分析了感知层、传输层、处理层、综合应用层以及控制系统的安全架构,同时对工业物联网安全防护产品的开发提出了建议.

关键词:工业物联网;潜在攻击;安全防护体系模型;安全架构
中图分类号:TP29 **文献标识码**:A **文章编号**:1672-6685(2015)02-0036-04

Study on the Security System of Industrial IOT

YANG Yue-mei[1,2], SONG Zhi-huan[2]

(1. College of Information Engineering, Hangzhou Polytechnic, Hangzhou 311402, China;
2. Dept. of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China)

Abstract: With the development of the technology of the Internet of Things (IOT), the industrial application of IOT is increasingly widespread, but the potential security risks of IOT put forward new challenge for its industrial applications. This paper analyzes the latent attack forms of industrial IOT, establishes hierarchical security system model, makes a detailed analysis on the security framework of the perception layer, transmission layer, processing layer, application layer as well as the control system, and thus puts forward suggestions for the development of industrial network security products.

Key words: industrial IOT; latent attack; security system model; security framework

随着物联网在工业实体领域崭露头角,信息安全也告别传统的病毒感染、网络黑客攻击及资源滥用等阶段,迈进一个复杂多元、综合交互的新时期.物联网应用规模越大就越能放大安全问题造成的影响.因工业物联网的应用往往是行业性的,故出现问题也将是全局性的.2010 年 6 月第一个专门攻击真实世界中基础设施的 Stuxnet 病毒的出现,打破了工业领域不会被攻击的神话,工业控制系统的安全性问题就变成一个现实问题,工业设施也成为网络上一些恶意势力所关注的重点,而物联网与工业结合也为这些恶意势力提供了新的入侵口.故设计工业物联网系统,首先要考虑安全性问题.

1 工业物联网的潜在攻击形式

从物联网的发展来看,物联网与因特网的区别在于全面感知层和可靠传输层.而对于工业物联网来说,感知层主要是基于传感器的现场设备;可靠传输层可

* 收稿日期:2015-03-10;修订日期:2015-05-19
基金项目:浙江大学工业控制技术国家重点实验室开放课题(ICT1241);浙江省高等学校访问学者教师专业发展项目(FX2012139)
作者简介:杨悦梅(1972—),女,江苏泰州人,杭州科技职业技术学院信息工程学院副教授,硕士,主要从事嵌入式技术及工业物联网方面的研究,(E-mail)353306316@qq.com.

以是基于传统的网络技术的工业以太网,因此传统互联网的攻击技术和形式也同样适用于可靠传输层.工业物联网特有的潜在攻击形式最主要有以下两种.

(1) 针对节点的攻击.主要有节点控制和节点捕获.节点控制是由于网络攻击者获取了网内节点的共享密钥或是网关节点和远程信息处理平台间的共享密钥被泄露,网络攻击者就可以通过控制传感器节点得到传感网与该节点所有的交互信息.节点捕获不涉及网络节点的密钥,是网络攻击者以阻断节点的方式破坏网络的连通性,或通过鉴别传感器类型和推测网络的运行模式获得网络隐私.

(2) 针对 RFID 系统的攻击.RFID(射频识别)无需接触即可通过射频信号完成对目标对象的识别和相关数据的获取.该技术可以实现全程自动化,可识别高速运动物体并可同时识别多个标签,操作也非常方便.而针对 RFID 系统的攻击主要集中于标签信息的截获和对这些信息的破解.在获得了标签中的信息之后,攻击者可以通过伪造等方式对 RFID 系统进行非授权使用.

此外,工业物联网由于工业控制系统的引入而催生了一系列全新的攻击形式:① 谐振攻击.网络攻击者在实施该攻击时,会通过对传感器或控制器的非法控制,迫使现有物理系统在特定频率附近产生谐振继而破坏系统正常运行.② 时钟同步攻击.对于工业控制系统这样的严格的时序系统,网络攻击者往往通过散播虚假时钟消息破坏统一的系统时钟,从而达到攻击目的.③ 控制系统攻击.该攻击中网络攻击者会通过干扰控制系统,影响其对当前网络状态的正确评估,以伪造或重放控制命令的方式实施伪造攻击、感知数据篡改攻击和控制网络 DoS 攻击[1].

2　工业物联网层次化安全防护体系

工业物联网安全的总体需求就是物理安全、信息采集安全、信息传输安全和信息处理安全的综合,安全的最终目标是确保信息的机密性、完整性、真实性和网络的容错性.考虑到现有通信网络的安全架构都是从人的通信角度设计的,并不适用于机器的通信,使用现有安全机制会割裂物联网机器间的逻辑关系.因此在设计工业物联网安全防护系统时采用分层的网络结构,从每个逻辑层次入手,为同一安全问题设置多重安全机制,形成感知层、传输层、处理层和应用层协同、联动的深度安全防护机制,构建一体化的工业物联网安全防护体系(见图 1).

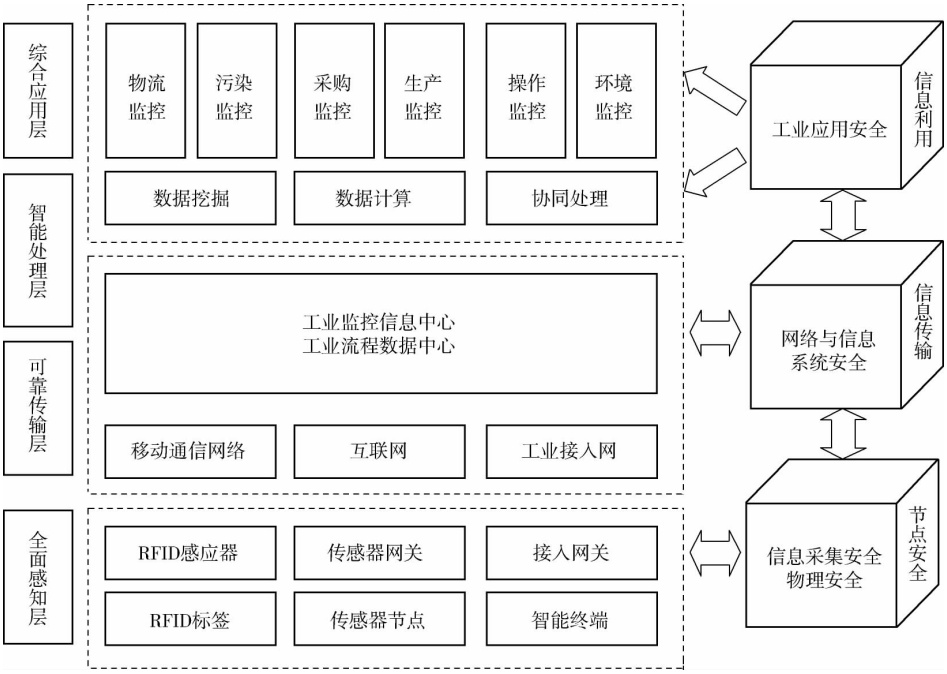

图 1　工业物联网层次化安全防护体系

Fig. 1　Hierarchical security system of industrial IOT

2.1　感知层的安全架构

物联网感知层的任务是实现智能感知外界信息功能,包括信息采集、捕获和物体识别.RFID(射频识别)装置、多类型传感器装置(如超声、红外、湿度、

温度、速度等)、图像捕获装置(摄像头)、GPS 装置(全球定位系统)、激光扫描仪等都是该层的典型设备.其中具体涉及多项关键技术,包括传感器技术、RFID 技术、自组织网络技术、短距离无线通信技术、低能耗路由技术等.

传感器作为工业物联网最基础的设备单元,能否高效地完成工业物联网信息的采集任务,关系到整个工业物联网感知环节的成败.由于传感网络本身具有无线链路比较脆弱,网络拓扑动态变化,节点计算能力、存储能力和能源有限、无线通信过程中易受到干扰等特点,所以传统安全机制无法应用到传感网络中.

目前常见的传感器网络安全技术主要包括以下几个层面:① 基本安全框架.安全框架主要有安全协议、参数化跳频等.② 密钥分配.传感器网络的密钥分配主要采用轻量级的密码算法与协议,以随机预分配的模型开展.③ 安全路由.当前的安全路由技术常加入容侵策略作为应对方法.④ 入侵检测技术.入侵检测技术主要包括被动监听检测和主动检测两类,常作为信息安全的第二道防线[2].

除上述安全保护技术外,由于工业物联网节点常受到资源限制,且呈现高密度冗余散布状态,故无法在每个节点上运行全功能入侵检测系统(IDs),这也对整体安全防护效果产生了影响.因此需要进一步研究如何在传感网中合理分布 IDs,最终提高系统的鲁棒性.由于网络攻击者在控制网内节点后,会在感知层内恶意散播虚假信息,蓄意破坏网络环境的稳定性,因此需要对可疑节点开展行为评估,建立相关的信任模型,降低恶意行为的影响和破坏.此外,感知层安全设计还需要考虑建立感知节点与外部网络的互信机制,保障感知信息安全传输.

2.2 传输层的安全架构

传输层主要实现信息的转发和传送,它将感知层获取的信息传送到远端,为数据在远端进行智能处理和分析决策提供强有力的支持.

在工业物联网中,传输层安全结构的设计必须兼顾高效性、特异性和兼容性.首先,传输层感知数据和控制指令具有很强的时效性,为了获得更高的处理效率,应该在密码协议设计时适当降低安全等级;其次,工业网络中异构网络数量众多,相对于通用安全结构,其网络性能各不相同,防御网络攻击的能力也相差巨大,因此需要针对网络特异性设计专用安全协议;最后,为了实现异构网络的无缝对接,必须确保安全协议的兼容性与一致性,这也是安全结构设计中相当关键的指标.

传输层安全结构一般有两个子层:① 点对点安全子层.该子层主要的作用是保证网络数据在逐跳传输过程中的安全,具体涉及的安全机制包括节点间的相互认证、逐跳加密以及跨网认证.② 端到端安全子层.该子层主要的作用是实现端到端的机密性并确保网络稳定、可用,具体涉及的安全机制包括端到端认证及密钥协商、管理和密码算法选取以及拒绝服务攻击的检测与防御.

此外,网络通信模式以及物联网本身的架构、接入方式和各种设备之间均存在巨大差异,加之工业物联网的接入层采用各种无线接入技术,诸如有线网,WiFi,WiMax 等,其异构性十分突出,因此还需要设计针对单播、广播、组播的专用安全机制,确保为终端提供移动性管理,保证异构网络间节点的无缝漫游和服务的无缝移动.

2.3 处理层的安全架构

工业物联网的处理层之所以能够高效处理海量数据并开展网络行为智能决策,其核心特点在于"协同"及"智能".所谓"协同",是指异构平台的协作计算,如何分离信息内容与信息来源,实现协作过程中数据所有者的隐私保护,是处理层安全结构设计的关键所在.所谓"智能",主要是指信息的自动处理,以此实现对海量数据的过滤、分类、识别和处理.如何提高恶意信息的识别能力,提升智能处理技术对恶意信息的检测能力是处理层安全结构设计的另一个重要任务.此外,如何根据数据的来源、时效性、可靠性建立数据可信度的量化机制,真正实现加密数据的高效挖掘,也是处理层安全机制所必须解决的现实问题.

目前处理层的安全机制包括:垃圾信息、恶意代码的检测与过滤、安全多方协同计算和安全云计算、计算平台的访问授权和灾难备份、数据的可信度量化、隐私保护和安全数据挖掘、可靠认证机制等.

2.4 综合应用层的安全结构

工业物联网应用是技术跨界结合的典范,其应用层充分体现了智能处理的特点,涉及信息技术与工业技术的紧密结合,包括业务管理、中间件、数据挖掘等先进技术.由于涉及众多行业,因此工业物联网面临广域范围的海量数据压力,系统内的信息处理和业务控制策略在安全性和可靠性方面也面临巨大挑战,特别是业务控制、管理和认证机制、中间件以及隐私保护等安全问题显得尤为突出.应用层安全结构的设计必须遵循差异化服务的原则.工业物

联网应用系统种类繁多,安全需求各不相同,同一安全服务对于不同用户涵义也可能完全不同.因此根据企业和用户需求提供具有针对性的安全服务,是应用层安全结构设计的核心理念.

在物联网发展过程中,大量的数据涉及到隐私问题,而应用于工业中必然会对企业商业机密造成影响,如何设计不同场景、不同等级的隐私保护技术是当前工业物联网安全技术研究重点.当前隐私保护方法主要有假名技术、密文验证(包括同态加密)技术、门限密码技术、叛逆追踪技术等[3].

2.5　控制系统的安全架构

物联网应用于工业领域后与工业控制系统是密不可分的,因此在设计工业物联网层次化的安全架构时也需要考虑到与控制系统安全的联动作用.工业物联网信息安全主要解决在大规模、高混杂、协同自治的工业网络环境下如何安全采集、处理和共享海量的网络信息,其重点在于提升现有体系内的安全机制层级,关注保护用户隐私、高效处理海量加密数据等方面.与此同时,有关控制安全的研究主要针对在开放互连、松散耦合的网络化系统结构下的安全控制机制和结构,其热点聚焦于如何克服网络攻击对控制系统估计和控制算法的影响.

目前控制系统的安全技术包括健壮网络控制、鲁棒估计、分步式估计、容错控制.在控制领域,因尚未形成成熟的理论分析模型,目前只能借用传统的时延、干扰和故障模型研究其安全威胁,并用容错控制、分布式估计、鲁棒估计等实现安全控制[4].

3　工业物联网安全防护产品开发建议

工业物联网安全防护系列产品框架可分为 4 个层次:① 应用安全.主要包括应用访问控制、信息内容过滤和网络安全审计等.② 网络安全,即传输安全.包括信息加密和认证、网络隔离交换、异常流量监控、攻击防御、信令和协议过滤及信息溯源等.③ 终端安全.包括主机防火墙、防病毒和存储加密等.④ 安全管理.应用以上相关理念和技术所进行的常规安全机制.围绕这些适用于工业物联网安全防护的措施,可开发出相应的软硬件安全产品.

3.1　基于工业物联网安全防护的设备开发

基于网络安全防护设备研究,重点关注网络边界(网关、无线网络入口等网络接入点)的入侵防范.一方面开发适用于工业物联网的防火墙设备、入侵检测设备、主动安全漏洞扫描设备、现场设备保护模块等,将设备安装在现场传感层网与通信网相连接的骨干网络上,并通过监听报文,发送扫描探测报文以及加密报文等方式,实现防御网络入侵攻击、检测系统安全漏洞、日志记录、数据传输安全及入侵报警等功能;另一方面开发安全接入设备,具备身份安全认证、权限控制、数据加解密、安全传输等功能.

3.2　基于工业物联网安全防护的软件开发

基于网络内部主机、设备自身安全(系统、软件、协议安全等)防护的软件研究,开发适用于工业物联网的入侵检测、漏洞扫描等软件.该类软件可用于工业物联网的安全防护,通过用户的访问行为特征、设备信息采集、漏洞探测扫描等方式,实现防御恶意软件破坏、扫描系统安全漏洞、阻止软件及数据的非法访问、日志记录及分析以及入侵报警等功能.

4　结语

工业物联网的安全问题正成为制约物联网全面发展的重要因素.面对工业物联网信息安全缺乏,开展工业物联网安全防护研究,建立工业物联网安全防护体系,可为企业工业物联网安全架构提供参考,同时对保障国家重要基础工业和社会关键服务,如电力、能源等国家基础领域的动态信息安全都具有重要意义.更重要的是,不能再走 IT 网络和工业控制系统先建设后安全的老路,必须将工业物联网安全防护的研究与物联网的工业应用同步进行,使工业物联网真正成为“安全”的网络.

参考文献:

[1] 丁超,杨立君,吴蒙. IoT/CPS 的安全体系结构及关键技术[J]. 中兴通讯技术,2011,17(1):11-16.

[2] 臧劲松. 物联网安全性能分析[J]. 计算机安全,2010(6):51-52.

[3] 范红,邵华,李程远,等. 物联网安全技术体系研究[J]. 电信网技术,2011(9):5-8.

[4] 杨金翠. 物联网环境下的控制安全关键技术研究[D]. 北京:北京邮电大学,2013.

[5] 谭建平,柔卫国,余敏,等. 基于物联网的一体化安全防范技术体系研究[J]. 湖南理工学院学报:自然科学版,2011,24(4):46-51.

[6] 宋慧欣. 破解“工业控制系统信息安全”迷局[J]. 自动化博览,2012(7):30-35.

[7] 朱云龙. 物联网应用促进工业化水平持续提升[J]. 世界电信,2011(7):50-53.

(责任编辑:吉美丽)