物联网框架安全威胁及相应策略研究

李园园[1],毕晓冬[2],张永胜[1],韩贝贝[3]
(1. 山东师范大学 信息科学与工程学院,山东 济南 250014;
2. 山东警察学院,山东 济南 250014;
3. 山东大学 计算机科学与技术学院,山东 济南 250101)

摘 要:与传统的互联网相比,物联网具有更高的安全需求。在物联网环境下,基本的管理工作由智能设备软件去处理,使人们从繁琐的低层次管理中解脱出来,将更多的人力、物力投入到新技术的研发中,产生巨大的经济和社会效益。然而一旦物联网的安全受到威胁、遭到攻击,损失将是不可估量的。物联网的健康迅猛发展,安全保障是其重要的前提。通过对物联网的基本概念、结构框架、技术框架的阐述,分析了物联网的相关特征,针对物联网各层的特点,分析了感知层、网络层、应用层存在的安全问题,并提出了一些解决思路。

关键词:物联网;射频标识;基本框架;安全
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2011)12-0148-04

Framework and Security Threats on Internet of Things and Survey of Corresponding Strategies

LI Yuan-yuan[1],BI Xiao-dong[2],ZHANG Yong-sheng[1],HAN Bei-bei[3]
(1. School of Information Science and Engineering,Shandong Normal University,Jinan 250014,China;
2. Shandong Police College,Jinan 250014,China;
3. School of Computer Science and Technology,Shandong University,Jinan 250101,China)

Abstract:Compared with traditional Internet, Internet of Things(IoT) has higher security needs. In the context of IoT,the basic management work will be handled by intelligent device software,so that people are free from redious low-level management,pouring more human and material resources into research of new technologies,resulting in huge economic and social benefits. However,once IoT is at stake or attacked,the loss will be immeasurable. Security is the premise of rapid development of IoT. On the basis of concept,structure and technology framework of IoT,analyzed characteristics on IoT. Aiming at the characteristics of levels on IoT,analyzed the safety problems of perception layer,network layer and application layer,put forward relevant countermeasures for different security problems.

Key words:Internet of Things;RFID;basic framework;safety

0 引 言

物联网(Internet of Things,IoT)是把普通物品与互联网相连接,进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理的一种网络。2005年国际电信联盟(ITU)发布的《ITU互联网报告2005:物联网》描绘了"物联网"时代的图景[1]:当司机出现操作失误时汽车会自动报警;公文包会提醒主人忘带了什么东西;衣服会告诉洗衣机对颜色和水温的要求等等。物联网正迅速发展,改变着人们的学习、生活与工作方式,是继计算机、互联网和移动通信网之后的又一次信息产业浪潮。物联网与人类生产生活密切相关,可以提高经济效益,大大节约成本,为全球经济的发展提供技术动力,然而它的普及与发展要以安全为前提。目前,世界上很多国家都在投入巨资,深入研究探索物联网,而安全问题则成了制约物联网发展和普及的一个重要因素。基于物联网的安全问题,文中从物联网的层次结构为出发点,进一步探讨了其安全防范措施。

收稿日期:2011-05-13;**修回日期**:2011-08-21
基金项目:山东省自然科学基金(ZR2011FM019);山东省软科学研究计划(2010RKB03012)
作者简介:李园园(1986-),女,山东枣庄人,硕士研究生,研究方向为服务计算、信息安全;毕晓冬,副研究员,研究方向为网络信息安全。

1 物联网概述

1.1 物联网

物联网是一种无线传感网,它将各种信息传感设备,如射频识别(RFID)装置、红外感应器、全球定位系

统、激光扫描器等种种装置与互联网结合起来形成一个巨大网络[2]。通俗来讲,物联网就是将物体连接起来的网络,在这个网络中,所有物品通过射频识别等信息传感设备与互联网连接起来,无需人工干预就可实现人与物体、物体与物体之间的沟通与对话。

物联网包含两层意思[3]:第一,物联网是互联网、移动通信网和传感网等网络的融合,是在互联网基础之上的延伸和扩展的一种网络;第二,其用户端延伸和扩展到了任何物品与物品之间,进行信息交换和通信。实现物体信息的可感、可知、可传和可控是物联网的核心,物联网是将多种技术融合的新技术,是占领未来国内外信息产业高端的机遇。

1.2　物联网结构框架

物联网跟互联网的层次结构不同,从网络架构上可将其分为三层,最基础的是感知层,即通过传感技术随时随地获取物体本身或周边各种动态信息,这些构成了网络传递的基础数据;第二层是网络层,即将感应层感知到的信息通过无线或有线网络进行实时传送,在技术上必须保证无缝互联、可靠传递;第三层是应用层,通过中央处理器、网络云计算等技术,对收到的各种实时数据进行处理,实现对物体的智能化管理和控制,真正达到人与物的沟通。结构框架[4]如图 1 所示。

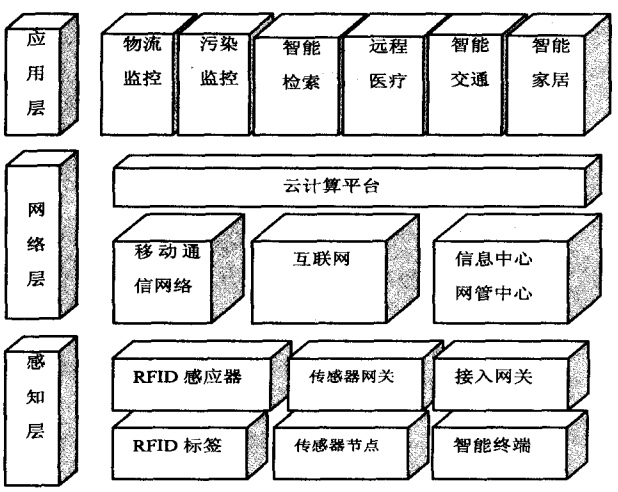

图 1　物联网结构框架

1.3　物联网技术框架

物联网是一个由感知层、网络层和应用层共同构成的大规模信息系统。它具备三大特征:全面感知、可靠传递和智能处理[5],完成这些功能需要的技术包括感知层技术、网络层技术、应用层技术以及公共技术。

(1)感知层:数据采集与感知是感知层的主要任务,通过传感器、二维识别码[6]、RFID 和 GPS 实时定位等技术采集各类标识、物理量以及音视频数据,然后通过短距离传输、自组织组网等技术实现数据的初步处理。

(2)网络层:网络层主要功能是通过传感网、移动网和互联网进行感知信息的可靠传输。发展已较成熟的移动通信、互联网技术基本可满足其传输需要。

(3)应用层:应用层主要功能体现在两个方面:将网络层传输的信息进行跨域协同互通;智能教育、智能交通、智能医疗等不同行业的应用服务。

(4)公共技术:顾名思义,属三层共用的技术,并不约束在某一层,它包括标识与解析、安全技术、网络管理和 QoS 管理。

1.4　物联网区别于互联网的特征

物联网的发展离不开互联网,然而与传统的互联网相比,物联网有其自己的特征:

(1)物联网在专用性不同的应用领域中是不同的,例如物联网在智能检索领域不同于在远程医疗领域,智能交通领域不同于智能家居领域,环境监测领域不同于汽车电子领域。物联网的应用需求必须通过专用联网技术来实现,这是因为不同的应用领域对网络应用需求与服务质量要求是不同的,而且物联网中的大部分节点资源受限。互联网虽然可以高效地实现全球的网络数据传输,但同时也不可避免地带来了一系列问题,如安全性、服务质量等。物联网的应用特殊性以及其他特征,使得它无法再复制互联网成功的技术模式[7]。

(2)要求网络的高度稳定与可靠。由于物联网直接涉及关键领域的关键设备,必须保证其网络的可靠与稳定。如在远程医疗卫生领域,物联网必须是稳定可靠的,如果网络像互联网一样,时常中断,传输的数据信息时常阻塞等,哪怕是一位数据的误传与延迟,都极大可能地危及病人的生命安全。

(3)严格的机密性与可控性。在物联网的应用领域中,绝大多数的应用关联着个人隐私或组织机构内部的秘密(如病人的病历或公司内部的客户资料等)。物联网必须提供严格的机密性与可控性,以保护个人的隐私、机构的秘密。物联网的终端用户可以严密地控制物联网中信息的发现、采集、传输与查询,以防止隐私或秘密的泄露或窃取给个人或机构造成伤害,将危险降到最低。

综合上述物联网的特征,可见物联网的安全要求比互联网要高。

2　物联网各层的安全威胁及相应策略

2.1　感知层

感知,顾名思义,就是对信息的感知,进而进行信息的采集。智能感知是物联网感知层的主要功能,包括信息采集、捕获和物体识别。

物联网感知层主要采用 RFID 技术,物品被嵌入 RFID 芯片后,不仅物品的主人能够方便地感知到,其

他人也能进行感知。当被感知的信息通过无线网络被传输时,其安全性相当脆弱。怎样在感知、传输和应用过程中保证信息的安全是一个十分重要的问题。

2.1.1 感知层面临的主要安全威胁

(1)安全隐私[8]。

RFID 是物联网的关键技术,在物联网系统中 RFID 标签会被嵌入任何物品中,比如人们的日常生活用品,而用品的拥有者不一定能觉察,从而导致用品的拥有者不受控制地被扫描、定位和追踪,这不仅涉及到技术问题,而且还涉及到法律问题[9]。如何在物联网中最大限度地保护个人安全隐私是物联网安全面临的重要问题。

(2)信号泄露与干扰。

感知层采用的主要技术是 RFID,RFID 的传输是基于无线通信信道的,这在无形中方便了非法用户的攻击。攻击者可以采取多种方式进行攻击,如:非法截取通信数据;发射干扰信号堵塞通信链路,使读写器过载,出现拒绝服务攻击,从而使标签数据不能被正常地接收;通过假冒身份向 RFID 发送数据来篡改和伪造数据。假如在身份系统中,非法攻击者通过感知节点之间信息的交流获取到用户的隐私或者一些机密信息,进而伪造用户的身份进行一些非法的活动,其后果不言而喻,危害巨大。

(3)节点的伪装。

节点数量庞大的物联网中,感知层的节点和设备大都暴露在开放的环境中,节点分散冗余且大范围撒布,攻击者可以很容易地接触到节点,进而获得节点的身份和密码信息,假冒身份与其它节点进行通信,进行非法的行为或恶意的攻击。如:监听用户信息、发布虚假信息、置换设备、发起 DoS 攻击等。

(4)感知网络的安全。

一般来说,物联网中感知节点众多,而它们的操作完全依靠自身携带的电池供电,能量有限,因而节点的通信能力、范围以及对感知信息的处理必会受到一定的限制,数据的采集及节点间信息的传输定然会受到影响,自身安全保护能力薄弱。随着信息技术的发展,物联网渐渐地走进了人们的生活,感知网络更是遍及人类生活的各个领域,其网络结构复杂多样,而节点之间信息的处理和传输又没有统一的安全规则,故而很难建立一套完整的安全体系。

2.1.2 感知层的主要安全防范措施

(1)数据的机密性是否得到保障是安全隐私是否能得到维护的重要判断标准之一。只有通过严格的密钥管理和身份认证机制才能满足只有经过授权的用户才能访问相应的标志数据的机密性要求。

(2)信息泄露问题可通过屏蔽信号和数字水印来解决。一方面,可以通过加密传输信息或者采取技术手段加强授权验证和对节点的大量访问请求作出限制等方法来防止信息的泄露。另一方面,当有泄密出现的时候,要及时发现泄密的标签并且采取相应的措施来使标签失效,使信息的泄露达到最少。在更加重要的场合,当有异常情况发生的时候,节点要能够自动启动封锁或者自毁程序,从而使得攻击者无法得到有用的信息。

(3)节点被控制无法避免的根本原因是节点和攻击者之间的不对称性。有些场合可以通过加强节点和汇聚节点之间以及节点和网络之间的认证来进行合法性验证,从而达到阻止未授权的阅读器读取信息的目的,使得即使节点被未授权者操纵也不会泄露太多有用的信息。在一些重要场合,也可以通过让相邻节点彼此作为对方的认证来发现非法节点或者通过校验节点的存储设备的方式来排除非法设备,从而减少节点被控制情况的发生。

2.2 网络层

网络层主要借助一些网络基础设施(如互联网、PSTN 网络等)来进行大范围的信息传输,将感知层采集的信息传送到各个节点以实现物品与物品间的远距离、大范围通信,信息的传输会经过各种不同的网络,因而安全问题至关重要。

2.2.1 网络层面临的主要安全威胁

(1)物联网架构开放,复杂多样的网络及终端设备本身存在安全隐患,各设备的性能与对网络的需求不同,难以设计统一的安全方案。

(2)网络层功能本身的实现中需要的技术与协议(网络存储、异构网络技术等)存在安全缺陷,特别在异构网络信息交换方面,易受到异步、合谋攻击等。

(3)网络层负责信息的传输,易受到路由攻击、虫洞攻击、女巫攻击、陷洞攻击等。

2.2.2 网络层的主要安全防范措施

(1)节点认证、数据机密性、完整性、数据流机密性、DDOS 攻击的检测与预防[10]。

(2)在无线网络的通信中,不同的 AKA 机制会给跨网认证带来威胁,因此要建立一种统一、兼容、一致的认证方案。

(3)为了保证端到端与节点到节点的机密性,要强化认证机制、密钥管理及协商机制、机密性算法选取机制等。

(4)密码体制只可抵御一部分攻击,需引入能及时发现并报告系统中未授权或异常现象的入侵检测技术作为第二道防线。

2.3 应用层

应用层包括应用服务和信息处理两个方面,应用

服务是对智能处理后的信息的利用。应用层包含的应用领域较广泛,如:智能家居[11]、智能电网、智能交通、环境监控等,因此应用层的安全问题主要来自各类新业务及应用的相关业务平台。

2.3.1　*应用层面临的主要安全威胁*

(1)恶意代码以及各类软件系统自身漏洞、可能的设计缺陷,黑客,各类病毒是物联网应用系统的重要威胁。

(2)物联网涉及范围广,目前海量数据信息处理和业务控制策略方面的技术还存在着安全性和可靠性的问题。

2.3.2　*应用层的主要安全防范措施*

应用层的安全从读取控制、用户认证、使用的不可抵赖性[12]等几个方面考虑。

相应的安全措施包括:

(1)在应用层设备中嵌入身份认证机制,对不同的用户赋予不同的权限,进而对数据进行访问控制,阻断非授权用户对资源的非法访问。

(2)对网络层传来的数据进行过滤,以防止恶意代码、病毒等不良信息对应用层的破坏。

(3)物联网用户在使用物联网和电脑时提高个人隐私保护意识,用户在删除重要的文件或处理废弃的电脑时,一定要对文件和电脑硬盘做不可恢复性处理[13]。

(4)定时进行系统安全漏洞检查,实行攻击监控、备份与恢复机制。

3　结束语

物联网安全问题制约了它的广泛应用,关于物联网的安全机制在业界也没有统一的方案,文中通过对物联网各层的不同特点与面临威胁的分析,在数据安全与隐私保护、节点安全保护与认证、信息安全通信、访问控制与系统安全保障策略等方面提出了各层的安全防范措施。当然,物联网的安全不仅是一个技术问题,还需要有一系列与之配套的政策、法律法规和完善的安全管理制度。

参考文献:

[1] The Internet of Things[EB/OL]. 2009-09-06. http://www.itu.int.

[2] International Telecommunication Union. The Internet of Things[R]. [s.l.]:[s.n.],2005.

[3] 杨　庚,许　建,陈　伟,等. 物联网安全特征与关键技术[J]. 南京邮电大学学报(自然科学版),2010,30(4):20-29.

[4] 王志良. 物联网现在与未来[M]. 北京:机械工业出版社,2010.

[5] 陈柳钦. 物联网:国内外发展动态及亟待解决的关键问题[EB/OL]. 2010. www.chinavalue.net/Article/Archive/2010/8/10/192271_13.html.

[6] 吴　同. 浅析物联网的安全问题[J]. 网络安全技术与应用,2010(8):7-8.

[7] 沈苏彬,范曲立,宗　平,等. 物联网的体系结构与相关技术研究[J]. 南京邮电大学学报(自然科学版),2009,29(6):1-10.

[8] 李志华,许榕生. 物联网安全保卫战[J]. 计算机世界,2010(26):1-4.

[9] 四大关键技术保卫物联网安全不受威胁[EB/OL]. 2010-07-19. http://miit.ccidnet.com/art/32559/20100719/2120335_1.html.

[10] 武传坤. 物联网安全架构初探[J]. 中国科学院院刊,2010,25(4):411-419.

[11] Taylor A,Harper R,Swan L,et al. Homes that make us smart[J]. Personal and Ubiquitous Computing,2007,11(5):383-393.

[12] 叶　青. 物联网安全问题技术分析[J]. 网络安全技术与应用,2010(10):32-33.

[13] 聂学武,张永胜,骆　琴,等. 物联网安全问题及其对策研究[J]. 计算机安全,2010(11):4-6.

(上接第 147 页)

information[J]. IEEE Transactions on Information Theory,2006,52(4):489-509.

[5] Tropp J,Gilbert A C. Signal recovery from random measurements via orthogonal matching pursuit[J]. IEEE Transactions on Information Theory,2007,53(12):4655-4666.

[6] Masudo N,Aihara K. Cryptosystems based on space discretization of chaotic maps[J]. IEEE Trans on Circuits and Systems-I,2002,49(1):28-40.

[7] Chen Y,Liao X F,Wong K W. Chosen plaintext attack on a cryptosystem with discretized skew tent map[J]. IEEE Trans on Circuits and Systems-II,2006,53(7):527-529.

[8] 邓绍江,李传东. 混沌理论及其在密码学中的应用[J]. 重庆建筑大学学报,2003(5):82-83.

[9] 岑翼刚,陈晓方,岑丽辉,等. 基于单层小波变换的压缩感知图像处理[J]. 通信学报,2010,31(8A):52-55.

[10] 张　锐. 基于压缩感知理论的图像压缩初步研究[J]. 电脑与技术,2010,6(4): 58-59.

[11] 罗军辉. MATLAB7.0 在图像处理中的应用[M]. 北京:机械工业出版社,2005.

[12] 李传目,洪联系,万　春. 基于混沌序列的图像分块加密方法[J]. 计算机技术与发展,2007,17(8):51-54.