ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.9, No.1, January 2013.
E-mail: info@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

物联网安全关键技术研究

马 卫

（中南民族大学，湖北 武汉 430074）

摘要：物联网的安全问题直接关系到物联网技术的发展和应用，在讨论了物联网体系架构的基础上，分析了物联网的安全需求，并对物联网安全的关键技术进行了研究，希望为建立可靠安全的物联网体系提供一定的参考作用。

关键词：物联网；安全需求；感知层

中图分类号：TP393　　文献标识码：A　　文章编号：1009-3044(2013)01-0029-03

Research on the Key Technology of the Security of the Internet of Things

MA Wei

(South-Central University for Nationalities, Wuhan 430074,China)

Abstract: Security issue of the IoT is directly related to the development and application. On the basis of discussion on the architecture of the IoT, the paper analyze the security needs of it, and give the further study on the key technology, expect to provide certain reference to the establishment of reliable and secure networking system.

Key words: internet of things; security needs; sensing layer

随着计算机网络和通信技术的发展，一种新的网络——物联网应运而生，物联网是通过射频识别(RFID)装置、红外感应器、全球定位系统、激光扫描器、传感器节点等信息传感设备，按约定的协议，把任何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、监控和管理等功能的一种网络[1]。它是继计算机、互联网与移动通信网络之后，全球信息产业的又一次科技浪潮。物联网的核心是完成物体信息的可感、可知、可传和可控。它给高速信息化生活带来了极大的便利，但与此同时，物联网的安全问题也给人们带来了极大的挑战，因为物联网的安全直接关系到物联网技术的发展和应用的推广。

目前，物联网安全问题已经成了人们关注的焦点，研究物联网的安全具有非常重要的现实意义。文献[2-5]都从物联网的基本概念和体系架构入手，强调物联网安全的重要性，并从物联网的多层结构出发分析各层的安全需求以及具有可行性的一些安全措施。但文献均停留在概括性分析层面，并没有深入探讨物联网安全的核心技术，而且对相关技术应用于物联网的普遍性没有进行分析评论。

本文在讨论了物联网体系架构的基础上，分析了物联网的安全需求，并对物联网安全的关键技术进行了研究，希望为建立可靠安全的物联网体系提供一定的参考作用。

1 物联网体系架构

物联网作为一种庞大复杂的聚合性系统，具备三个显著特征，一是各种感知技术的全面应用，即利用RFID、传感器、二维码等不同类型的感知技术，按一定频率周期性的采集物体的信息；二是建立基于互联网的多网融合网络，实现数据的可靠传递；三是具有智能处理能力，物联网将传感器和智能处理相结合，利用数据挖掘、模式识别、云计算等各种智能计算技术，对海量的数据和信息进行分析和处理，对物体实施智能控制。

目前，在业界，EPCGlobal物联网体系结构是最具有代表性的物联网架构之一[6]。它将物联网大致划分为三个层次，底层是具有全面感知能力的感知层，第二层是进行传输数据的网络层，最上层则是面向用户的应用层，如图1所示。

在物联网体系架构中，下层是为上层服务的，每一层都有自己的功能，具体描述如下。

感知层的主要功能是识别物体和采集信息。它一般包括数据采集和短距离数据通信两个子层。首先数据采集子层通过传感器、二维码、RFID等不同类型的技术获取物理世界中的数据信息；然后短距离数据通信子层通过蓝牙、红外、ZigBee等短距离数据传输技术将数据传送到网关或接入广域承载网络。

网络层的主要功能是将感知到的数据进行安全可靠的传输。它是在现有网络的基础上，对多种网络进行融合和扩展，利用多种网络传输技术将来自感知层的数据通过基础承载网络传输到应用层。

应用层的主要功能是将感知和传输来的数据进行分析和处理，并通过多种方式进行人机交互，它是物联网的终极目标，也是物

收稿日期：2012-11-24

本栏目责任编辑：冯蕾

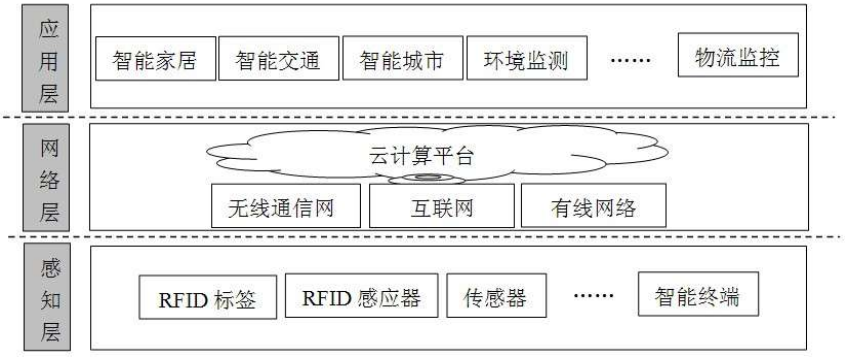

图1 物联网体系架构

联网作为深度信息化网络的重要体现。它一般包括应用程序和终端设备两个子层。

2 物联网安全需求

物联网不同于现有通信网络,其结构更复杂,系统更庞大,因而存在着不同于现有通信网络更多的安全问题。由于物联网在很多场合都使用无线传输技术,这种传输方式使传输的信息处于完全公开暴露的状态,很容易被窃取和干扰,这将直接影响到物联网体系的安全。同时物联网还可能带来许多个人隐私泄露。虽然相继推出了一些安全技术,如防火墙、入侵检测系统、PKI 等等,

但物联网的研究与应用才刚刚起步,很多的理论与关键技术有待完善和突破,特别是与互联网和移动通信网相比,物联网存在一些特殊的安全问题,下面将从物联网的三层架构来分析物联网的安全需求。

2.1 感知层安全需求

在最底层的感知层,由于传感器节点受到能量和功能的制约,其安全保护机制较差,并且由于传感器网络尚未完全实现标准化,其中消息和数据传输协议没有统一的标准[7],从而无法提供一个统一完善的安全保护体系。因此,传感器网络除了可能遭受同现有网络相同的安全威胁外,还可能受到恶意节点的攻击、传输的数据被监听或破坏、数据的一致性差等安全威胁。

2.2 网络层安全需求

由于物联网中的通信终端呈指数增长,而现有的通信网络承载能力有限,当大量的网络终端节点接入现有网络时,将会给通信网络带来更多的安全威胁。首先,大量终端节点的接入肯定会带来网络拥塞,而网络拥塞会给攻击者带来可趁之机,从而对服务器产生拒绝服务攻击;其次,由于物联网中的设备传输的数据量较小,一般不会采用复杂的加密算法来保护数据,从而可能导致数据在传输的过程中遭到攻击和破坏;最后,感知层和网络层的融合也会带来一些安全问题。

2.3 应用层安全需求

物联网的应用领域非常广泛,渗透到了现实中的各行各业,由于物联网本身的特殊性,其应用安全问题除了现有网络应用中常见的安全威胁外,还存在更为特殊的应用安全问题。。在实际应用中,大量使用无线传输技术,而且大多数设备都处于无人值守的状态,使得信息安全得不到保障,很容易被窃取和恶意跟踪。而隐私信息的外泄和恶意跟踪给用户带来了极大地安全隐患。

3 物联网安全关键技术

物联网作为多网融合的聚合性复杂系统,比互联网面临更多的安全问题,而且其安全问题涉及到网络的不同层次,虽然现有的网络安全机制可以解决部分的安全问题,但更多的安全问题还是需要对现有网络中的安全机制进行改进或完善,或者提出全新的安全机制[8]。针对物联网中新的安全需求,下面对物联网中的若干关键安全问题进行了深入的分析和研究。

3.1 认证机制

现有网络的认证机制主要考虑的是人与人之间的通信安全,在一定程度上并不适用于物联网。对于物联网的认证机制,应该根据业务的归属分类考虑是否需要进行业务层的认证,如果是由运行商提供的业务,并且能够提供可靠地业务运行平台,或者是业务本身对数据的安全性要求不高,则可以不进行业务认证。如果是由第三方提供的业务,并且不能保证业务层的数据安全,或者业务本身对数据的安全性要求较高,则需要进行业务认证。

3.2 密钥管理

在物联网的安全体系中,为保证节点间的通信安全,必须采取一定的安全措施。在所有的安全机制中,密钥是系统安全的基础,是网络安全及信息安全保护的关键[9]。物联网中有限的软硬件资源,对密钥管理提出了更高的要求。因此,物联网中密钥管理方案的设计,既要能够适应复杂的传感器网络环境,又要能够便于网络运营商控制管理网络。目前关于密钥管理协议的研究主要有两个方向,一是基于对称密钥体制的密钥管理协议;二是基于非对称密钥体制的密钥管理协议。前者虽然能满足基本的安全需求,但是其抗攻击能力较弱。而后者虽然安全性能更好,但是其复杂度较高、开销大。所以,物联网的密钥管理主要需要考虑两个问题:一是如何构建一个适应物联网体系结构,并且具有可扩展性、有效性和抗攻击能力的密钥管理系统;二是如何有效的管理密钥。

3.3 安全路由协议

路由协议的设计与应用是维护物联网安全的关键因素之一,而现有的路由协议主要考虑的是节点间数据的有效传输,忽视了对数据本身的安全考虑。由于物联网中路由既跨越了基于IP地址的互联网,又跨越了基于标识的移动通信网和传感器网络,物联网中的路由协议的设计就更加复杂,不仅需要考虑多网融合的路由问题,还要顾及传感器网络的路由问题。对于多网融合,可以考虑基于IP地址的统一路由体系;而对传感器网络,由于其节点的资源非常有限,抗攻击能力很弱,设计的路由算法要具有一定的抗攻击性,不仅实现可靠路由,更要注重路由的安全性。

3.4 恶意代码防御

由于平台、应用、设备的多样性和公开性,物联网的复杂性远远大于传统的因特网,这给有效防止恶意代码的攻击带来了新的挑战。在物联网中,大多数终端设备都直接暴露于无人看守的场所,一旦受到恶意代码的攻击,将会迅速蔓延开来。因此,恶意代码对物联网的威胁比普通网络更大。

物联网中的恶意代码防御可在现有网络恶意代码防御机制的基础上,结合分层防御的思想,以便从源头控制恶意代码的复制和传播,进一步加强恶意代码的防御能力。

4 结束语

物联网的安全问题是物联网服务能否得到大规模应用的重要保障,而物联网的复杂结构使其安全面临巨大的挑战,如何在现有网络安全技术的基础上,进一步改进和完善物联网的安全机制将具有重大意义。

参考文献:

[1] ITU Internet Reports 2005: The Internet of Things[Z].International Telecommunication Union, 2005.
[2] 李志清.物联网安全问题研究[J].计算机安全, 2011, (10):57-59.
[3] 李振汕.物联网安全问题研究[J].信息网络安全,2010,(12):1-3.
[4] 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.
[5] 彭朋, 韩伟力, 赵一鸣,等.基于 RFID 的物联网安全需求研究[J].计算机安全, 2011, (1): 75-79.
[6] ITU. The Internet of Things [EB/OL]. http://www.itu.int/internetofthings. [2010-07-03].
[7] 郭楠,徐全平.传感器网络国际标准化综述[J].信息技术与标准化,2009(11).
[8] 焦文娟.物联网安全—认证技术研究[D].北京邮电大学,2010(1).
[9] 杨庚,许建,陈伟. 物联网安全特征与关键技术[J].南京邮电大学学报,2010,8,(4).

(上接第24页)

2)形成适应信息时代要求的高等学校教学、科研、管理及校园文化生活的新形态,构建适应信息社会要求的高校的办学新模式。

3)数字校园中教学资源的构建需要学科教师的积极参与,不断提高自身的信息素养和信息技术能力,勇于尝试新的教学方法与教学手段。

4)处理好校园网络基础、教学与管理支撑平台、网络教学资源、资源与知识数据库管理、一线教学应用、以及应用效果评价之间的关系,特别是提高应用和评价的质量。

5)加速松散耦合的教学与教学管理"一体化"环境的构建。尽可能的采用规范的标准框架体系,为各种数字资源提供统一的检索界面,建立各数字资源之间的联系,将数字资源整合为一个相互联系的有机整体,最大限度地发挥数字资源的效益。

6)构建校级、省级和国家极标准化的分布式优质网络教学资源中心。

6 总结与展望

资源中心的构建在数字校园建设中占有十分重要的地位。该文结合数字校园资源中心构建的实践,探讨了资源中心在支持网络教与学、实现资源的共享与知识管理、资源自我扩充以及与其它数字校园应用支撑平台相结合等方面的现实意义。提出了注重"共享、聚合、交互"的资源构建理念,并对资源中心软件平台的若干设计原则和关键问题进行了探讨。由于我国高校层次和办学条件和方向不同,在进行数字资源架构时,需要注意从规划、建设、应用、管理等各方面进行有目标有计划有组织分阶段分层次地建设,使之真正成为便捷化,网络化、个性化的服务型数字资源,为使用者更加优良的服务环境。

参考文献:

[1] http://baike.baidu.com/view/959300.htm.
[2] 韩锡斌,杨娟,陈刚.基于知识管理的大学数字校园的概念、架构和策略[J].中国远程教育,2005(8).
[3] 余胜泉,朱凌云,曹晓明.教育资源管理的新发展[J].中国电化教育,2003(9):96-99.