

物联网技术及安全问题

朱新良^{1,2}

(1. 上海理工大学 光电信息与计算机工程学院, 上海 200093; 2. 上海理工大学 信息化办公室, 上海 200093)

摘要: 物联网被称为继计算机和互联网之后的第三次信息技术革命, 其应用无处不在, 而物联网的安全问题直接关系到它的广泛应用。从物联网的安全构架和特点出发, 阐述了物联网三层体系结构中存在的的核心问题, 提出了解决方案和涉及到的关键技术, 对感知层的安全措施进行了具体的阐述, 包括密钥管理算法、安全路由协议、数据融合技术以及身份认证和访问控制, 等等。最后介绍了物联网的典型应用和发展前景。

关键词: 信息技术; 物联网; 物联网安全; 感知层

中图分类号: TP 393

文献标志码: A

文章编号: 1009-895X(2015)02-0190-07

DOI: 10.13256/j.cnki.jusst.sse.2015.02.017

Technology and Security Issues of Internet of Things

Zhu Xinliang

(1. School of Optical-Electrical and Computer Engineering,

University of Shanghai for Science and Technology, Shanghai 200093, China;

2. Informatization Office of University of Shanghai For Science and Technology, Shanghai 200093, China)

Abstract: Internet of things is called the third IT revolution following the computer and the internet, and now it is everywhere. The security issues of the Internet of Things (IoT) are directly related to the wide application of its system. Beginning with introducing the architecture and features of IoT security, this paper expounds several security issues of IoT that exist in the three-layer system structure, and comes up with solutions coupled with key technologies involved. Among these safety measures concerned, those in perception layer are particularly elaborated, including key management and algorithm, security routing protocol, data fusion technology, as well as authentication and access control, etc. The paper also presents the typical application and future prospect of the internet of things.

Keywords: IT; Internet of Things; Internet of things security; perception layer

物联网是指通过各种信息传感设备, 如传感器、RFID(射频识别装置)技术、全球定位系统、红外传感器、激光扫描器、气体传感器等各种装置与技术, 实时采集其声、光、热、电、力学、化学、生物、位置等各种需要的信息, 与互联网结合

而形成的一个巨大网络^[1]。其目的是实现物与物、物与人、所有的物品与网络的联接, 便于识别、管理和控制。

随着网络技术和单片机技术的快速发展, 物联网应用的范围逐步从物流扩大到智能小区、智能交

收稿日期: 2014-06-23

作者简介: 朱新良(1982-), 男, 助理工程师。研究方向: 物联网技术、计算机应用技术。E-mail: zhuxl@usst.edu.cn

通、精细农业和其他领域。其功能也从传统的跟踪管理转变为智能控制,以满足更多的需求控制。根据欧洲智能系统集成技术平台(EPoSS)对“2020年的物联网”的分析,预测它的发展将经历四个阶段:2010年之前RFID被广泛应用于物流、零售和制药领域;2010—2015年物体互联;2015—2020年物体进入半智能化;2020年之后物体进入全智能化^[2]。

物联网作为一个多网的异构融合网络,不仅与传感器网络、移动通信网络和因特网有着相同的安全问题,还有其特有的如隐私保护问题、异构网络的身份认证和访问控制问题以及信息储存和管理问题,等等^[3],因此物联网与互联网不同,其安全问题的研究要更加复杂,需要有针对性的措施来解决各个方面的安全问题。

一、物联网的安全架构及其特点

物联网在不同应用领域都有其相应的工业标准和规范。物联网的统一构架虽尚未形成,但是许多组织已经发布了自己的物联网安全标准,如IEEE、欧洲电信标准协会(ETSI),等等。文献[4]给出了物联网安全标准的发展历程。虽然目前的物联网大多属于独立的小型网络,能够被利用的攻击漏洞相对较少,但是随着物联网技术的持续发展,多个独立的小型网络将会合并成一个大型网络,到那个时候将很难保证其安全性。这些安全问题是决定物联网发展的关键因素。

(一) 物联网的安全架构

物联网的结构通常被分为三层,即感知层、网络层和应用层,而有些系统会采用网络支持技术(如网络处理技术、计算技术、中间件技术,等等)作为处理层。文献[5]将物联网体系架构分为三层,总结了有关物联网的安全体系问题并对其进行需求分析。文献[6]提出了一种未来物联网架构的典型模型(U2IoT),其中包含了人类中枢神经系统和社会结构的概念。本节探讨的是物联网的三层体系结构。其结构图如图1所示。

(二) 物联网的特点

物联网具备三个基本特点:全面感知、可靠传输和智能处理。全面感知是指通过感知层的传感器节点随时随地获取对象信息;可靠传输是指通过无

线或有线网络将对象的信息实时、安全和完整地传输到数据中心;智能处理是指在数据被最终提交到应用终端之前,由中间件对收集的信息进行分析和处理。

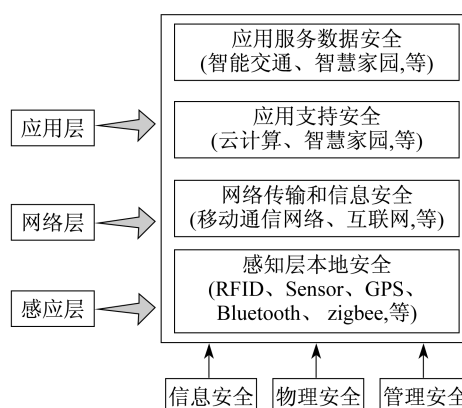


图1 物联网安全层次架构

Fig.1 IOT security architecture

二、物联网的安全问题

物联网的特点能揭示出其相关的安全问题,这些安全问题为:1)感知层数据信息采集和传输的安全问题。传感器节点具有种类多和高异质性的特点,且通常具有单一的结构和单处理器,这些特点使其不可能具备复杂的安全防护能力。2)网络层的传统安全问题。目前的网络安全体系虽已成熟,但仍存在许多的攻击漏洞。例如,大量的恶意节点同时发送数据引起的DoS(Denial of Service)攻击,等等。因此需要建立具体的网络以适应物联网的信息传输。3)应用层的安全问题。物联网在不同应用领域都会存在许多复杂和多样的安全问题。4)安全与成本之间的矛盾问题。如果每个传感器节点的成本太低,那么就会存在大量的低性能节点,这些节点将会降低传感器网络安全,相反高质量节点能够提高安全性,但是网络的维护成本将提高。5)传感器节点性能问题。传感器节点的处理性能较低,必须采用轻量级的加密算法和安全认证来保证其安全性。6)非对称性问题。相对于网络终端,网关节点的数据处理能力非常弱,这就需要有高效的安全管理措施来协调网络的非对称性。7)复杂度问题。物联网应用的类型决定了其安全问题的数量和复杂度,因此,应该综合考虑每一层的安全问题。以上前三个是传统的安全问题,其他的为新问题^[7]。

这些安全问题非常复杂并且处理起来相当困难,因此需要了解不同层的各种安全问题和潜在攻击。考虑到该系统是一个整体,安全问题在刚开始设计的时候就应该被解决。因此,文献[8]提出了灰色关联算法在物联网安全状态评估中的应用,它将常见的几种网络攻击行为作为安全因素,通过使用灰色关联分析法来量化某段时间内网络攻击行为对该网络所产生的相对影响,进而实现对整个网络所处的安全环境与状态的定量评估,并且给出了基于灰色关联算法的物联网信息安全状态评估的具体步骤。下面将讨论每一层的安全问题。

(一) 感知层的安全问题

目前感知层主要的感知设备包括 RFID 模块、zigbee 模块等各种无线传感器设备。由于数据信息被采集时,信息传输方式主要是通过无线网络来传输,因此信号被暴露在公共场所。如果此信号缺乏有效的保护措施,就会很容易被监控、截获和干扰。由于大部分无线传感设备被部署在非受控区域,因此攻击者很容易获得并控制这些设备,或者从物理上毁坏它们。例如,DPA(微分功率分析)就是一种非常有效的攻击。

几种常见的攻击^[9]:

(1) 节点捕获。关键节点(如网关节点)很容易被攻击者控制,可能会导致所有信息的泄漏,包括组通信密钥、无线电密钥、匹配密钥,等等,进而威胁到整个网络的安全。

(2) 伪节点和恶意数据。攻击者给系统添加一个节点,并为其输入伪代码或数据,该节点会阻碍实时数据的传输并剥夺能量受限节点的睡眠,进而导致宝贵的节点能量的消耗,从而潜在控制或摧毁整个网络。

(3) DoS(拒绝服务)攻击。DoS攻击是无线传感器网络和互联网中最常见的攻击,它会导致网络资源的消耗殆尽并使服务失效。

(4) 延时攻击。通过分析用于执行加密算法所需要的时间来获取关键信息。

(5) 路由威胁。通过欺骗、篡改或重发路由信息,攻击者可以创建路由环路来产生或阻碍网络传输、延长或缩短来源路径、形成错误信息、增加终端到终端的延迟,等等。

(6) 重放攻击。攻击者发送一个目的主机已接受过的数据包,来取得系统的信任,主要用于身份认证过程和破坏认证的正确性。

(7) SCA(边信道攻击)。攻击者针对设备在运行过程中侧信道信息的泄露而对加密设备进行的攻击,如时间消耗、电力消耗或电磁辐射,等等。

(8) 海量节点认证问题。需要解决物联网海量节点认证的效率问题。

此外,移动智能终端将是物联网感知层的一个重要的组成部分,所以其安全性不容忽视。目前,市场上大部分智能手机都是以安卓操作系统为主,然而根据安卓系统发展的特点,大多数安卓手机存在安全验证和短信诈骗漏洞的高风险。此外,几乎所有的安卓软件都具有一些如扫描手机内存、上传用户地址簿、定位和收集用户隐私的功能,因此,对于智能手机用户的隐私保护也是一个需要解决的问题。

(二) 网络层的安全问题

(1) 传统网络问题。通信网络的安全问题将对数据机密性和完整性构成威胁。虽然现有的通信网络具有相对完整和安全的保护措施,但是仍有一些常见的问题,包括网络非法入侵、信息窃听、保密性缺失、完整性破坏、DoS攻击、中间人攻击、病毒入侵、漏洞攻击,等等。

(2) 兼容性问题。现有的互联网安全体系结构是以人的角度设计的,并不一定适用于机器之间的通信,利用现有的安全机制将会分裂物联网机器之间的逻辑关系。由于接入网络的方式有多种,这种异质性使得安全性、互操作性和网络协调性变得糟糕,并且容易产生安全漏洞。

(3) 群集安全问题。包括网络阻塞、DoS攻击、身份验证问题,等等。由于物联网设备的数量巨大,如果使用现有的验证模式来验证设备,将会产生巨大的数据流量而造成网络阻塞。现有的IP技术不适用于海量节点验证,因为在大量设备之间的相互验证会导致关键资源的严重浪费。

(4) 隐私泄露问题。随着信息检索技术和社会工程的发展,黑客很容易就能收集到大量特定用户的隐私信息。

(三) 应用层的安全问题

物联网在不同的应用领域,其应用层也具有不同的安全问题。虽然物联网应用层的构架至今还没有统一的标准,但是一些企业已经实施了物联网的M2M(机器到机器)模式,如智能小区、智能家居、医疗,等等。文献[10]提出了智能家居安防

系统的设计方案。文献[11]给出了一些基于6LoWPAN (IPv6的低功耗WPAN) 构架的解决方案来支持医疗感测系统。虽然应用层的安全问题比较复杂和繁琐,但仍可以总结出一些常见的安全问题。

(1) 数据访问权限、身份认证。由于不同的应用会有不同的用户而每个应用也会有大量的用户,因此,需要采取高效的身份验证技术以防止非法用户的介入,同时也应该考虑到垃圾邮件和恶意信息的识别和处理。

(2) 数据保护和恢复。由于通信数据涉及到用户个人隐私,而数据保护机制和数据处理算法却不够完美,因此很可能会导致数据丢失,甚至造成灾难性的损害。海量节点管理也是造成数据丢失的原因之一。

(3) 海量数据处理能力。在具有大量节点、海量数据传输和复杂环境的情况下,一旦数据处理能力和适应能力不能够满足需求,就会导致网络中断和数据丢失。

(4) 应用层软件漏洞。由于程序员是用非标准代码来编写软件,这会导致在软件中存在缓冲区溢出漏洞等问题,黑客可以利用这些漏洞来实施他们的计划。

三、物联网的安全措施

物联网作为一个多网的异构融合网络,其安全性涉及到各个网络不同层的安全问题,其中每个独立的网络,如移动通信网、互联网,等等,又运用了多种安全技术,同时物联网的感知层需要克服资源的多样性和网络的异质性问题,这些因素增加了安全性研究的难度。本节介绍了物联网不同层的安全措施,其中重点介绍了感知层的安全措施。

(一) 感知层的安全措施

由于RFID和WSN是物联网感知层的一个重要部分,因此下面将分别介绍它们的安全措施。

1. RFID的安全措施^[12]

(1) 访问控制。防止用户的隐私泄露,以保护RFID标签内的信息不被任意读取,其中包括标签失效、芯片保护、天线能量分析,等等。

(2) 数据加密。对RFID系统的数据安全性,使用适当的算法来加密RFID信号。文献[13]提出

了一种以移位计算为基础的、非线性的密码算法,实现了RFID系统的数据加密。在保障数据高速传输的条件下,该密码算法使用很少的计算能力,就能够实现非常高的安全性。

(3) 基于IPSec的安全信道。IPSec协议组提供两种安全机制:认证和加密。认证机制使IP通信的数据接收方能够确认数据发送方的真实身份。加密机制通过对数据进行编码来保证数据的机密性,以防数据在传输过程中被窃听和篡改。

(4) 密码技术方案。密码技术不仅能够实现用户隐私保护,而且能保证RFID系统的机密性、真实性和完整性。其安全通信协议包含了基于哈希函数、随机数的机制、服务器数据检索、逻辑算法和重新加密机制。

(5) 物理安全方案。SCA是物理安全的主要问题,而DPA是SCA常用的手段。防止DPA的各种策略能够被分为两种:隐蔽和掩蔽,隐蔽可以消除能源消耗的数据依赖性,而掩蔽使得加密设备在运行过程中可以随机地产生中间值。

2. 无线传感器网络的安全措施

由于WSN是物联网感知层的一个重要组成部分,并且数据在自由空间中传输,攻击者很容易就能截获和分析数据,因此,需要根据不同的攻击手段,来采取相应的保护措施。

(1) 密钥管理。无线传感器网络密钥管理的安全性需求设计主要体现在密钥生成或算法更新、向前隐私性、向后隐私性和可扩展性、抗共谋攻击、源认证和数据新鲜性的安全性,其主要有四个密钥分配协议即简单密钥分配协议、密钥预分配协议、动态密钥管理协议和分级密钥管理协议。

(2) 密钥算法。密钥算法主要包括对称密钥算法和非对称密钥算法,非对称密钥算法主要使用RSA (Ron Rivest, Adi Shamir, Len Adleman 三位天才的名字) 和ECC (椭圆曲线密码编码学) 加密算法;对称密钥算法主要使用Skipjack和RC5加密算法,由于感知层节点的处理能力比较差,而对称算法相比非对称算法具有计算量小、代码短和能耗低的特点,因此,对称密钥算法广泛应用与无线传感器网络。文献[14]提出了基于轻量级设备的ECC密钥管理改进方案,使密钥管理研究在无线传感器网络方面得到了广泛的关注。

(3) 安全路由协议。高效的安全路由协议算法通常采用的机制包括集群机制、数据融合机制、

多跳路由机制、密钥机制,等等。安全路由技术中广泛采用 SPINS 安全框架协议^[15-16],包括 SNEP(安全网络加密)协议和 μ TESLA(微型基于时间高效流损失容忍认证)协议,其中 SNEP 协议用于实现机密性、完整性、新鲜性和点对点的认证, μ TESLA 协议用于实现单点到多点的广播认证。

(4) 入侵检测技术。IDS(入侵检测系统)可对网内的节点行为进行监测,及时发现可疑节点行为。

(5) 身份认证和访问控制技术。认证技术主要包括基于轻量级的公钥认证技术、PSK(预共享密钥)、随机密钥预分配认证技术、利用辅助信息认证技术、基于单向哈希函数认证技术,等等;访问控制技术主要包括基于非对称密码系统和对称密码系统的访问控制技术。

(6) 物理安全设计。主要包括节点设计和天线设计,节点设计包括硬件结构设计和安全芯片选择、芯片连接、射频电路设计、数据采集单元设计;天线设计应符合良好的通信距离、高适应性、稳定性,等等。

通常单一措施无法解决感知层的安全问题,需要多种措施一起使用。

(二) 网络层的安全措施

在目前的物联网结构中,网络层是以互联网或通信网络为基础而存在的,有些因素危及互联网信息安全的同时,也会破坏物联网的信息服务,但是,由于传统的网络路由方式单一,并且其主要目的不是针对安全性,所以传统的网络通信技术不能完全适应物联网,又由于物联网的节点安排随意、自主、能量受限制和通信不可靠,这将会导致物联网基础设施和动态拓扑的瓦解,攻击者就可以很容易发动攻击。

需采取的安全措施如下:

(1) 构建物联网与互联网、移动通信网络相融合的网络安全体系结构,并针对不同的网络架构,需要建立专门的认证结合机制、终端到终端的认证和密钥协议机制、PKI(公钥基础设施)、无线网络的 WPKI、安全路由、入侵检测,等等,又由于数据量巨大,网络可用性也需考虑,此外,还应加强网络层的跨域认证和跨网认证。

(2) 建设物联网网络安全统一防护平台,完成对终端安全管控、安全授权、应用访问控制、协同处理、终端态势监控与分析等管理。

(3) 提高物联网系统各应用层次之间的安全应用与保障措施,重点规划异构网络集成、功能集成、软硬件操作界面集成及智能控制、系统级软件和安全中间件等技术应用。

(4) 建立全面的物联网网络安全接入与应用访问控制机制,满足物联网终端产品的多样化网络安全需求。

(5) 应用网络虚拟化技术,可以极大减少网络管理的复杂性和误操作的可能性。

随着下一代网络(NGN)的发展,作为物联网中传输承载网络中的 IPv6 建设也随之展开。文献[17]给出了基于 IPv6 的信息安全产品的发展趋势,并详细讨论了 IPv6 网络的安全机制和安全产品的应用。

(三) 应用层的安全措施

物联网应用层的应用具有多样性和不确定性,体现了不同的应用环境需要有不同的安全措施。

1. 技术方面

(1) 跨异构网络的认证和密钥协议。包括基于对称密钥的密码系统、基于公钥的密码系统(证书或 PKI)和认证转移技术。

(2) 个人信息的保护。包括指纹技术、数字水印、匿名认证、门限密码,等等。

(3) 避免软件漏洞。软件设计中采用相关技术避免完全漏洞,在上线运行前应进行漏洞扫描。

2. 非技术方面

(1) 提高安全意识。让用户意识到信息安全的重要性,并知道如何正确使用物联网服务,以减少机密信息的泄漏。

(2) 加强信息安全管理。包括资源管理、物理安全信息管理、密码管理,等等。

四、物联网典型应用

物联网可以广泛应用于社会和生活的各个方面。下面介绍其不同领域中的典型应用。

(一) 在城市交通中的应用

首先它能够用于为司机自动收费。如果车辆安装了有源 RFID 标签的话,司机就无需停车来支付费用,因为读卡器会自动收集车辆信息和计算司机

的停车费用。

其次，物联网能够用于城市的智能交通管理。当RFID读卡器被安装在城市道路的主要路口时，大量的车辆实时信息被自动收集并发送到交通管理中心，从而在道路发生交通堵塞时，交通管理中心可以通过调整路口的交通指示灯来缓解交通压力。

此外，物联网还能用于跟踪定位车辆。对于交通管理而言，可以记录往来车辆的数量以及何时何地达到交通峰值；如果发生车辆盗窃案件，物联网将帮助警察快速定位车辆位置，及时找回失窃车辆。

（二）在医疗保健中的应用

物联网技术在医疗保健领域也有许多应用，这些应用有病患追踪、病情识别和验证以及生命体征信息的感知和收集。

病患跟踪可以在医院门口使用，医院可以使用这些数据来控制进入医院的人数，该技术也可以用于住院病人的跟踪。病患识别可以用来减少伤害病人的事故发生（如错误的药物/剂量/时间/程序，等等），也可以用来查找病人所有的电子医疗看病记录。

通过RFID技术，无线传感器就能监测病患的生命体征，包括血压、心跳速率，等等，便于医生获取病人的实时信息，从而可以在病人处于病危时，能立即抢救。

（三）在物流中的应用

主要应用在基于RFID的产品可追溯系统、基于全球定位系统（GPS）的智能配送可视化网络、全自动的物流配送中心以及基于智能配货的物流网络化公共信息平台。使用分析和模拟软件可以优化从原材料至成品的供应链网络。帮助企业确定生产设备的位置，优化采购地点，也能帮助制定库存分配战略，降低成本、减少碳排放，改善服务。

（四）在电网中的应用

智能电网将物联网运用在发电、输电、变电、配电和用电环节，使用双向通信、高级传感器和分布式计算机来改善电力交换和使用的效率，提高可靠性。以前因发电量不平稳难以接入电网的风电、太阳能等分布式能源可以用于补助主网发电。智能电网实时监控用户的电力负荷，赋予消费者选择电价和能源类型的权利。

（五）在生态监控中的应用

物联网在生态监视中主要应用于饮用水源地、城市大气、危废品转移及流域管理与生态补偿。通过视频感知或RFID技术，或生物、声学、光学、化学、红外及卫星等等传感器进行全面感知，通过可靠传输，到达信息处理中心，利用虚拟现实、生态分析、决策支持系统（DSS）、云计算等智能处理实现智能监视。

（六）在数字家庭中的应用

如果简单地将家庭里的消费电子产品链接起来，那么只是一个多功能遥控器控制所有终端，仅仅实现了电视与电脑、手机的连接，这不是发展数字家庭产业的初衷。只有在连接家庭设备的同时，通过物联网与外部的服务连接起来，才能真正实现服务与设备互动。有了物联网，就可以在办公室指挥家中的电器操作运行，在下班回家途中，家里的饭菜已经煮熟，洗澡的热水已经烧好，个性化电视节目将会准点播放，家庭设施能够自动报修，冰箱里的食物能够自动补货。

（七）在食品安全控制中的应用

食品安全是国计民生的重中之重。通过标签识别和物联网技术，可以随时随地对食品生产过程进行实时监控，对食品质量进行联动跟踪，对食品安全事故进行有效预防，极大提高了食品安全的管理水平。

五、我国物联网产业的发展前景

物联网产业在世界范围内被公认为第三次信息产业浪潮，我们国家若想抓住这样的历史机遇，需要政府、企业、高校多方协作，共同发展。

首先，政府引导，扶持政策先行。物联网产业的发展离不开政府的重视与扶持。政府可考虑增设专门机构，统领大局进行协调、整合，带动多方力量共同参与物联网的发展，并且有针对性地出台一系列方针政策，大力推动行业标准制定，指明产业发展的方向。目前，我国正在加紧制定中的财税、投融资等金融配套政策，就将有助于解决困扰物联网产业的融资难问题，给整个产业带来重大利好。

其次，重视人才，攻克技术难关。技术的不成熟是当前阻碍我国物联网产业发展的最根本问题。

隐私保护与信息安全方面的隐患都是由技术的不完善带来的。技术的突破要依靠人才,因此重视人才建设显得尤为重要。我国在加大本土专业人才培养力度的同时,可引进海外高层次创新人才和团队,努力创造有利于人才发展的宽松环境。此外,各级政府也可考虑设立物联网专项基金,对攻克核心技术、做出突出贡献的团体和个人,给予重大的物质奖励与精神支持。通过整合多方力量,尽快突破物联网核心技术难关。

再次,加强宣传,刺激市场需求。在物联网产业发展的早期,社会公众对这一新概念不熟悉不理解,大部分采取“敬而远之”的态度,造成该产业的市场需求并不迫切。若想刺激市场需求,必须首先加强宣传,可选择在各大电视台播出以物联网为主题的公益广告,让老百姓对这一概念熟悉起来,然后再通过物联网公共服务项目的推广,使该产业逐渐走进寻常老百姓的日常生活之中,提高公众对这一新兴产业的感知与接收程度。

六、结束语

物联网安全的发展是物联网的一个重要组成部分,本文分别阐述了物联网安全架构中每一层存在的问题和解决的措施,但是物联网作为一个由多层集成的大系统,许多安全问题都来自系统集成,如隐私保护在每一层中都有涉及到。因此,作为物联网安全技术的应用,我们必须通过分析特定的条件来应用不同的组合技术,而不是学术性地将其固定在一定范围内。总之,物联网的安全构架仍处在探索阶段,它的安全性正面临着比预期更加严峻的挑战。

参考文献:

- [1] Atzori L, Lera A, Morabito G. The internet of things; a survey [J]. Computer Networks, 2010, 54 (15): 2787-2805.
- [2] 王慧强,吕宏武. 物联网安全关键技术及其应用研究[J]. 大庆师范学院学报, 2012, 32(6): 5.
- [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] 孙梦梦,刘元安,刘凯明. 物联网中的安全问题分析及其安全机制研究[J]. 保密科学技术, 2011(11): 61-66.
- [5] 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.
- [6] Ning H S, Liu H. Cyber-Physical-Social based security architecture for future internet of things [J]. Scientific Research, 2012(2): 1-7.
- [7] 孙建华,陈昌祥. 物联网安全初探[J]. 通信技术, 2012, 45(7): 100-102.
- [8] 高洪波. 灰色关联算法在物联网安全状态评估中的应用[J]. 制造业自动化, 2012, 34(11): 23-25.
- [9] 李善仓,张克旺. 无线传感器网络原理与应用[M]. 北京:中国机械工业出版社, 2008.
- [10] 杨广学,李凤娇,慕香永,等. 基于物联网的家居安防系统设计[J]. 计算机应用, 2010, 30(S2): 300-302.
- [11] Jara A H, Zamora M A, Skarmeta A F G. HWSN6: hospital wireless sensor networks based on 6lowpan technology: mobility and fault tolerance management [C] // International Conference on Computational Science and Engineering, Vancouver, BC: IEEE, 2009: 879-884.
- [12] 李磊,陈静. 物联网感知层中 RFID 系统安全解决方案[J]. 网络安全技术与应用, 2011(6): 34-36.
- [13] 王小妮,魏桂英. 物联网 RFID 系统数据传输中密码算法的研究[J]. 北京信息科技大学学报(自然科学版), 2009, 24(4): 75-78.
- [14] 杨庚,王江涛,程宏兵,等. 基于身份加密的无线传感器网络密钥分配方法[J]. 电子学报, 2007, 35(1): 180-185.
- [15] Perri g A, Szewczyk R, Tygar J D, et al. Spins: security protocols for sensor networks [J]. Wireless Networks, 2002, 8(5): 521-534.
- [16] Liu D, Ning P. Multi-level μ tesla: a broadcast authentication system for distributed sensor networks [D]. North Carolina: North Carolina State University, 2003.
- [17] 沈亮,张艳,顾健. 物联网网络层中基于 IPv6 的信息安全产品发展趋势研究[C] // 信息网络安全, 2012(8): 38-40.

(编辑: 巩红晓)