第30卷 第4期 南京邮电大学学报(自然科学版) Vol. 30 No. 4
2010年8月 Journal of Nanjing University of Posts and Telecommunications(Natural Science) Aug. 2010

物联网安全特征与关键技术

杨 庚[1],许 建[2],陈 伟[2],祁正华[2],王海勇[2]
(1. 南京邮电大学 科技处,江苏 南京 210046
2. 南京邮电大学 计算机学院,江苏 南京 210046)

摘 要:物联网的安全与隐私保护问题直接关系到物联网服务能否得到真正的实际推广应用,从信息安全的机密性、完整性和可用性等三个基本属性出发,分析了物联网安全的特征和面临的安全问题,讨论了物联网安全的系统架构,以及一些安全关键技术,包括密钥管理、认证与访问控制、安全路由、隐私保护、入侵检测与容错容侵等,对其中的密钥管理和路由技术进行了较详细的讨论。

关键词:物联网;网络安全;信息安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-5439(2010)04-0020-10

Security Characteristic and Technology in the Internet of Things

YANG Geng[1], XU Jian[2], CHEN Wei[2], Qi Zheng-hua[2], WANG Hai-yong[2]
(1. Department of Technology, Nanjing University of Posts and Telecommunications, Nanjing, 210046
2. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing, 210046)

Abstract: Security and privacy are key issues for application in Internet of Things. Based on confidentiality, integrity and availability, this paper analyzes the security characteristics and problems in IOT. It discusses a framework and some techniques, including the key management, authentication, access control, security routing, privacy protecting, intrusion detecting and tolerance.

Key words: the Internet of Things; information security; network security

0 引 言

物联网(the Internet of Things, IOT)是近几年提出的概念,在实际应用中,可以把感应器、处理器和无线通信模块嵌入或装备到电网、铁路、桥梁、隧道、公路、建筑等各种物体中,使它们相互连接,构成物联网。它有两层意思: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。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。因此,物联网的核心是完成物体信息的可感、可知、可传和可控。

1999年美国麻省理工学院(MIT)成立了自动识别技术中心,构想了基于RFID的物联网的概念,提出了产品电子码(EPC)概念。通过EPC系统的发展不仅能够对货品进行实时跟踪、而且能够通过优化整个供应链给用户提供支持,从而推动自动识别技术的快速发展并能够大幅度提高消费者的生活质量。国际物品编码协会EAN和美国统一代码委员会成立EPC Global机构,负责EPC网络的全球化标准[1]。

2005年在突尼斯举行的信息社会世界峰会(WSIS)上,国际电联(ITU)发布了"ITU Internet Reports 2005: The Internet of Things"[2]。报告指出射频识别技术、传感器技术、纳米技术、智能嵌入技术

收稿日期:2010-07-10
基金项目:国家重点基础研究发展计划(973计划)(2011CB302903)、国家自然科学基金(60873231)、江苏省自然科学基金(BK2009426)、江苏省高校自然科学基金(08KJB520006)、江苏省普通高校研究生科研创新计划(CX09B_151Z)资助项目
通讯作者:杨 庚 电话:(025)85866917 E-mail:yangg@njupt.edu.cn

将到更加广泛的应用。根据ITU的描述,在物联网时代,通过在各种各样的日常用品上嵌入一种短距离的移动收发器,人类在信息与通信世界里将获得一个新的沟通维度,从任何时间任何地点的人与人之间的沟通连接扩展到人与物和物与物之间的沟通连接。另一方面,欧洲智能系统集成技术平台(EPoSS)在"Internet of Things in 2020"报告中也分析预测了未来物联网的发展将要经历四个阶段。

在产业界,2008年底IBM提出了"智慧地球"概念,随后,IBM大中华区在2009IBM论坛上公布了名为"智慧的地球"的最新策略。国际上多个国家和地区已经启动了相应的研究计划,如日本的U-Japan计划、韩国的U-Korea计划等。在我国,早在上世纪90年末也开始了传感网的研究,特别是近十年来在无线传感器网络方面,国内的高等院校、科研机构和相关企业都进行了较深入的研究,取得了一些成果。

从信息与网络安全的角度来看,物联网作为一个多网的异构融合网络,不仅存在与传感器网络、移动通信网络和因特网同样的安全问题,同时还有其特殊性,如隐私保护问题、异构网络的认证与访问控制问题、信息的存储与管理等。文献[3]认为数据与隐私保护是物联网应用过程中的挑战之一。在物联网中,RFID系统实现末端信息的感知,文献[4]讨论了在RFID系统中数据传输的密码算法问题,采用IC卡中的逻辑加密模块进行信息的加密。文献[5]设计了一种基于RFID的信息服务系统,主要是针对物流管理方面的应用。对物联网的安全和隐私保护问题,文献[6]进行了讨论,特别是讨论了涉及的法律问题。文献[7]提出了一个物联网服务安全模型,并分析了模型中的各个模块的功能。文献[8]对物联网的状况进行了分析,也讨论了安全问题。文献[9]对数据安全及隐私保护问题进行了研究。同时人们对相关的CPS(cyber-physical systems)和普适计算安全也进行了相关的研究。

本文将试图从信息安全的机密性、完整性和可用性等三个基本属性出发,分析物联网安全的特征和面临的安全问题,讨论物联网安全的系统架构,以及一些安全关键技术,特别对密钥管理和路由技术进行深入的讨论。

1　物联网安全特征与架构

信息与网络安全的目标是要达到被保护信息的机密性(confidentiality)、完整性(integrity)和可用性(availability)。在互联网的早期阶段,人们更关注基础理论和应用研究,随着网络和服务规模的不断增大,安全问题得以特显,引起了人们的高度重视,相继推出了一些安全技术,如入侵检测系统、防火墙、PKI等等。物联网的研究与应用处于初级阶段,很多的理论与关键技术有待突破,特别是与互联网和移动通信网相比,还没有展示出令人信服的实际应用,我们将从互联网的发展过程来探讨物联网的安全问题。

1.1　物联网安全特征

从物联网的信息处理过程来看,感知信息经过采集、汇聚、融合、传输、决策与控制等过程,整个信息处理的过程体现了物联网安全的特征与要求,也揭示了所面临的安全问题。

一是感知网络的信息采集、传输与信息安全问题。感知节点呈现多源异构性,感知节点通常情况下功能简单(如自动温度计)、携带能量少(使用电池),使得它们无法拥有复杂的安全保护能力,而感知网络多种多样,从温度测量到水文监控,从道路导航到自动控制,它们的数据传输和消息也没有特定的标准,所以没法提供统一的安全保护体系。

二是核心网络的传输与信息安全问题。核心网络具有相对完整的安全保护能力,但是由于物联网中节点数量庞大,且以集群方式存在,因此会导致在数据传播时,由于大量机器的数据发送使网络拥塞,产生拒绝服务攻击。此外,现有通信网络的安全架构都是从人通信的角度设计的,对以物为主体的物联网,要建立适合于感知信息传输与应用的安全架构。

三是物联网业务的安全问题。支撑物联网业务的平台有着不同的安全策略,如云计算、分布式系统、海量信息处理等,这些支撑平台要为上层服务管理和大规模行业应用建立起一个高效、可靠和可信的系统,而大规模、多平台、多业务类型使物联网业务层次的安全面临新的挑战,是针对不同的行业应用建立相应的安全策略,还是建立一个相对独立的安全架构?

另一方面可以从安全的机密性、完整性和可用性来分析物联网的安全需求。信息隐私是物联网信息机密性的直接体现,如感知终端的位置信息是物联网的重要信息资源之一,也是需要保护的敏感信息。另外在数据处理过程中同样存在隐私保护问题,如基于数据挖掘的行为分析等等,要建立访问控

制机制,控制物联网中信息采集、传递和查询等操作,不会由于个人隐私或机构秘密的泄露而造成对个人或机构的伤害。信息的加密是实现机密性的重要手段,由于物联网的多源异构性,使密钥管理显得更为困难,特别是对感知网络的密钥管理是制约物联网信息机密性的瓶颈。

物联网的信息完整性和可用性贯穿物联网数据流的全过程,网络入侵、拒绝攻击服务、Sybil 攻击、路由攻击等都使信息的完整性和可用性受到破坏。同时物联网的感知互动过程也要求网络具有高度的稳定性和可靠性,物联网是与许多应用领域的物理设备相关连,要保证网络的稳定可靠,如在仓储物流应用领域,物联网必须是稳定的,要保证网络的连通性,不能出现互联网中电子邮件时常丢失等问题,不然无法准确检测进库和出库的物品。

因此,物联网的安全特征体现了感知信息的多样性、网络环境的多样性和应用需求的多样性,呈现出网络的规模和数据的处理量大,决策控制复杂,给安全研究提出了新的挑战。

1.2 物联网安全架构

图 1 显示了物联网的层次架构,感知层通过各种传感器节点获取各类数据,包括物体属性、环境状态、行为状态等动态和静态信息,通过传感器网络或射频阅读器等网络和设备实现数据在感知层的汇聚和传输;传输层主要通过移动通信网、卫星网、互联网等网络基础实施,实现对感知层信息的接入和传输;支撑层是为上层应用服务建立起一个高效可靠的支撑技术平台,通过并行数据挖掘处理等过程,为应用提供服务,屏蔽底层的网络、信息的异构性;应用层是根据用户的需求,建立相应的业务模型,运行相应的应用系统。在各个层次中安全和管理贯穿于其中。

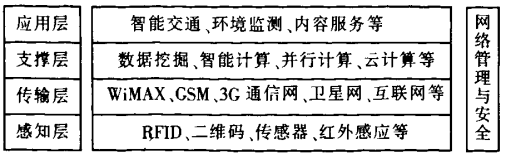

图 1 物联网的层次结构

图 2 为物联网在不同层次可以采取的安全。以密码技术为核心的基础信息安全平台及基础设施建设是物联网安全,特别是数据隐私保护的基础,安全平台同时包括安全事件应急响应中心、数据备份和灾难恢复设施、安全管理等。安全防御技术主要是为了保证信息的安全而采用的一些方法,在网络和通信传输安全方面,主要针对网络环境的安全技术,如 VPN、路由等,实现网络互连过程的安全,旨在确保通信的机密性、完整性和可用性。而应用环境主要针对用户的访问控制与审计,以及应用系统在执行过程中产生的安全问题。

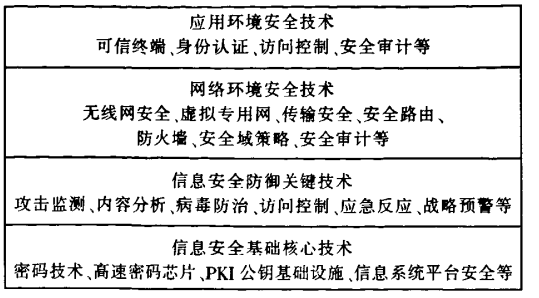

图 2 物联网安全技术架构

2 物联网安全关键技术

作为一种多网络融合的网络,物联网安全涉及到各个网络的不同层次,在这些独立的网络中已实际应用了多种安全技术,特别是移动通信网和互联网的安全研究已经历了较长的时间,但对物联网中的感知网络来说,由于资源的局限性,使安全研究的难度较大,本节主要针对传感网中的安全问题进行讨论。

2.1 密钥管理机制

密钥系统是安全的基础,是实现感知信息隐私保护的手段之一。对互联网由于不存在计算资源的限制,非对称和对称密钥系统都可以适用,互联网面临的安全主要是来源于其最初的开放式管理模式的设计,是一种没有严格管理中心的网络。移动通信网是一种相对集中式管理的网络,而无线传感器网络和感知节点由于计算资源的限制,对密钥系统提出了更多的要求,因此,物联网密钥管理系统面临两个主要问题:一是如何构建一个贯穿多个网络的统一密钥管理系统,并与物联网的体系结构相适应;二是如何解决传感网的密钥管理问题,如密钥的分配、更新、组播等问题。

实现统一的密钥管理系统可以采用两种方式:一是以互联网为中心的集中式管理方式。由互联网的密钥分配中心负责整个物联网的密钥管理,一旦传感器网络接入互联网,通过密钥中心与传感器网络汇聚点进行交互,实现对网络中节点的密钥管理;二是以各自网络为中心的分布式管理方式。在此模

式下,互联网和移动通信网比较容易解决,但在传感网环境中对汇聚点的要求就比较高,尽管我们可以在传感网中采用簇头选择方法,推选簇头,形成层次式网络结构,每个节点与相应的簇头通信,簇头间以及簇头与汇聚节点之间进行密钥的协商,但对多跳通信的边缘节点、以及由于簇头选择算法和簇头本身的能量消耗,使传感网的密钥管理成为解决问题的关键。

无线传感器网络的密钥管理系统的设计在很大程度上受到其自身特征的限制,因此在设计需求上与有线网络和传统的资源不受限制的无线网络有所不同,特别要充分考虑到无线传感器网络传感节点的限制和网络组网与路由的特征。它的安全需求主要体现在:

(1) 密钥生成或更新算法的安全性:利用该算法生成的密钥应具备一定的安全强度,不能被网络攻击者轻易破解或者花很小的代价破解。也即是加密后保障数据包的机密性。

(2) 前向私密性:对中途退出传感器网络或者被俘获的恶意节点,在周期性的密钥更新或者撤销后无法再利用先前所获知的密钥信息生成合法的密钥继续参与网络通信,即无法参加与报文解密或者生成有效的可认证的报文。

(3) 后向私密性和可扩展性:新加入传感器网络的合法节点可利用新分发或者周期性更新的密钥参与网络的正常通信,即进行报文的加解密和认证行为等。而且能够保障网络是可扩展的,即允许大量新节点的加入。

(4) 抗同谋攻击:在传感器网络中,若干节点被俘获后,其所掌握的密钥信息可能会造成网络局部范围的泄密,但不应对整个网络的运行造成破坏性或损毁性的后果即密钥系统要具有抗同谋攻击。

(5) 源端认证性和新鲜性:源端认证要求发送方身份的可认证性和消息的可认证性,即任何一个网络数据包都能通过认证和追踪寻找到其发送源,且是不可否认的。新鲜性则保证合法的节点在一定的延迟许可内能收到所需要的信息。新鲜性除了和密钥管理方案紧密相关外,与传感器网络的时间同步技术和路由算法也有很大的关联。

根据这些要求,在密钥管理系统的实现方法中,人们提出了基于对称密钥系统的方法和基于非对称密钥系统的方法。在基于对称密钥的管理系统方面,从分配方式上也可分为以下三类:基于密钥分配中心方式、预分配方式和基于分组分簇方式。典型的解决方法有 SPINS 协议、基于密钥池预分配方式的 E-G 方法和 q-Composite 方法、单密钥空间随机密钥预分配方法、多密钥空间随机密钥预分配方法、对称多项式随机密钥预分配方法、基于地理信息或部署信息的随机密钥预分配方法、低能耗的密钥管理方法等。与非对称密钥系统相比,对称密钥系统在计算复杂度方面具有优势,但在密钥管理和安全性方面却有不足。例如邻居节点间的认证难于实现,节点的加入和退出不够灵活等。特别是在物联网环境下,如何实现与其他网络的密钥管理系统的融合是值得探讨的问题。为此,人们将非对称密钥系统也应用于无线传感器网络,TinyPK[10] 在使用 TinyOS 开发环境的 MICA2 节点上,采用 RSA 算法实现了传感器网络外部节点的认证以及 TinySec 密钥的分发。文献[11]首次在 MICA2 节点上基于椭圆曲线密码 ECC(ellipse curve cryptography)实现了 TinyOS 的 TinySec 密钥的分发,文献[12-13]对基于轻量级 ECC 的密钥管理提出了改进的方案,特别是基于圆曲线密码体制作为公钥密码系统之一,在无线传感器网路密钥管理的研究中受到了极大的重视,具有一定的理论研究价值与应用前景。

近几年作为非对称密钥系统的基于身份标识的加密算法(identity-based encryption, IBE)引起了人们的关注。该算法的主要思想是加密的公钥不需要从公钥证书中获得,而是直接使用标识用户身份的字符串。最初提出这种基于身份标识加密算法的动机是为了简化电子邮件系统中证书的管理。当 Alice 给 Bob 发送邮件时,她仅仅需要使用 Bob 的邮箱 bob@company.com 作为公钥来加密邮件,从而省略了获取 Bob 公钥证书这一步骤。当 Bob 接收到加密后的邮件时,联系私钥生成中心(private key generator),同时向 PKG 验证自己的身份,然后就能够得到私钥,从而解密邮件。

然而,在 Shamir 提出 IBE 算法后的很长一段时间都没有能找到合适的实现方法。直到 2001 年,可实用的 IBE 算法由 Boneh 等提出,算法利用椭圆曲线双线性映射(bilinear map)来实现。基于身份标识加密算法具有一些特征和优势,主要体现在:(1)它的公钥可以是任何唯一的字符串,如 E-mail、身份证或者其它标识,不需要 PKI 系统的证书发放,使用起来简单;(2) 由于公钥是身份等标识,所以,基于身份标识的加密算法解决了密钥分配的问题;(3)基于身份标识的加密算法具有比对称加密算法更高的加密强度。在同等安全级别条件下,比其它公钥

加密算法有更小的参数,因而具有更快的计算速度和更小的存储空间。

IBE 加密算法一般由四部分组成:系统参数建立、密钥提取、加密和解密。表 1 为 EPCglobal 网络(electronic product code)的节点标识的格式,共 96 比特长度,类似于网卡的 MAC 地址,而传感器网络的节点一般都有身份标识,采用基于身份的密钥系统,就可以以此为公钥,实现感知信息的加密和解密,文献[13]对 IBE 算法在无线传感器网络中的应用进行了分析,包括密钥的分配、更新等过程。IBE 算法的复杂性主要在计算双线性对上,寻求简单适用的双线性对的计算方法是 IBE 算法能否广泛应用的关键。

表 1 EPCglobal 网络标签身份长度与表示内容

Header	Filter Value	Partition	Company Prefix	Item Reference	Serial Number
8 bits	3 bits	3 bits	20~40 bits	4~24 bits	38 bits
			Combined length:44 bits		

2.2 数据处理与隐私性

物联网的数据要经过信息感知、获取、汇聚、融合、传输、存储、挖掘、决策和控制等处理流程,而末端的感知网络几乎要涉及上述信息处理的全过程,只是由于传感节点与汇聚点的资源限制,在信息的挖掘和决策方面不占居主要的位置。物联网应用不仅面临信息采集的安全性,也要考虑到信息传送的私密性,要求信息不能被篡改和非授权用户使用,同时,还要考虑到网络的可靠、可信和安全。物联网能否大规模推广应用,很大程度上取决于其是否能够保障用户数据和隐私的安全。

就传感网而言,在信息的感知采集阶段就要进行相关的安全处理,如对 RFID 采集的信息进行轻量级的加密处理后,再传送到汇聚节点。这里要关注的是对光学标签的信息采集处理与安全,作为感知端的物体身份标识,光学标签显示了独特的优势,而虚拟光学的加密解密技术为基于光学标签的身份标识提供了手段,基于软件的虚拟光学密码系统由于可以在光波的多个维度进行信息的加密处理,具有比一般传统的对称加密系统有更高的安全性,数学模型的建立和软件技术的发展极大地推动了该领域的研究和应用推广。

数据处理过程中涉及到基于位置的服务与在信息处理过程中的隐私保护问题。ACM 于 2008 年成立了 SIGSPATIAL(Special Interest Group on Spatial Information),致力于空间信息理论与应用研究。基于位置的服务是物联网提供的基本功能,是定位、电子地图、基于位置的数据挖掘和发现、自适应表达等技术的融合。定位技术目前主要有 GPS 定位、基于手机的定位、无线传感网定位等。无线传感网的定位主要是射频识别、蓝牙及 ZigBee 等。基于位置的服务面临严峻的隐私保护问题,这既是安全问题,也是法律问题。欧洲通过了《隐私与电子通信法》,对隐私保护问题给出了明确的法律规定。

基于位置服务中的隐私内容涉及两个方面,一是位置隐私,二是查询隐私。位置隐私中的位置指用户过去或现在的位置,而查询隐私指敏感信息的查询与挖掘,如某用户经常查询某区域的餐馆或医院,可以分析该用户的居住位置、收入状况、生活行为、健康状况等敏感信息,造成个人隐私信息的泄漏,查询隐私就是数据处理过程中的隐私保护问题。所以,我们面临一个困难的选择,一方面希望提供尽可能精确的位置服务,另一方面又希望个人的隐私得到保护。这就需要在技术上给以保证。目前的隐私保护方法主要有位置伪装、时空匿名、空间加密等。

2.3 安全路由协议

物联网的路由要跨越多类网络,有基于 IP 地址的互联网路由协议、有基于标识的移动通信网和传感网的路由算法,因此我们要至少解决两个问题,一是多网融合的路由问题;二是传感网的路由问题。前者可以考虑将身份标识映射成类似的 IP 地址,实现基于地址的统一路由体系;后者是由于传感网的计算资源的局限性和易受到攻击的特点,要设计抗攻击的安全路由算法。

目前,国内外学者提出了多种无线传感器网络路由协议,这些路由协议最初的设计目标通常是以最小的通信、计算、存储开销完成节点间数据传输,但是这些路由协议大都没有考虑到安全问题。实际上由于无线传感器节点电量有限、计算能力有限、存储容量有限以及部署野外等特点,使得它极易受到各类攻击。

无线传感器网络路由协议常受到的攻击主要有以下几类:虚假路由信息攻击、选择性转发攻击、污水池攻击、女巫攻击、虫洞攻击、Hello 洪泛攻击、确认攻击等。表 2 列出了一些针对路由的常见攻击,表 3 为抗击这些攻击可以采用的方法。针对无线传感器网络中数据传送的特点,目前已提出许多较为有效的路由技术。按路由算法的实现方法划分,有洪泛式路由,如 Gossiping 等;以数据为中心的路由,如 Directed Diffusion, SPIN 等;层次式路由,如

LEACH(low energy adaptive clustering hierarchy)、TEEN(threshold sensitive energy efficient sensor network protocol)等;基于位置信息的路由,如GPSR(greedy perimeter stateless routing)、GEAR(geographic and energy aware routing)等。

表2　路由协议的安全威胁

路由协议	安全威胁
TinyOS信标	虚假路由信息、选择性转发、污水池、女巫、虫洞、*HELLO*泛洪
定向扩散	虚假路由信息、选择性转发、污水池、女巫、虫洞、HELLO泛洪
地理位置路由	虚假路由信息、选择性转发、女巫
最低成本转发	虚假路由信息、选择性转发、污水池、女巫、虫洞、HELLO泛洪
谣传路由	虚假路由信息、选择性转发、污水池、女巫、虫洞
能量节约的拓扑维护(SPAN、GAF、CEC、AFECA)	虚假路由信息、女巫、HELLO泛洪
聚簇路由协议(LEACH、TEEN)	选择性转发、HELLO泛洪

表3　传感器网络攻击和解决方案

攻击类型	解决方法
外部攻击和链路层安全	链路层加密和认证
女巫攻击	身份验证
HELLO泛洪攻击	双向链路认证
虫洞和污水池	很难防御,必须在设计路由协议时考虑,如基于地理位置路由
选择性转发攻击	多径路由技术
认证广播和泛洪	广播认证,如μTESLA

表4列出了针对安全威胁而设计的相关安全路由算法,下面主要讨论两个路由协议。

TRANS(trust routing for location-aware sensor networks)是一个建立在地理路由(如GPSR)之上的安全机制,包含两个模块:信任路由(trust routing module)和不安全位置避免(insecure location avoidance module),其中信任路由模块TRM安装在汇聚节点和感知节点,不安全位置避免模块ILAM仅安装在汇聚节点。另一种容侵的安全路由协议为INSENS(intrusion-tolerant routing protocol for wireless sensor networks),INSENS包含路由发现和数据转发两个阶段。在路由发现阶段,基站通过多跳转发向所有节点发送一个查询报文,相邻节点收到报文后,记录发送者的ID,然后发给那些还没收到报文的相邻节点,以此建立邻居关系。收到查询报文的节点同时向基站发送自己的位置拓扑等反馈信息。最后,基站生成到每个节点有两条独立路由路径的路由转发表。第二阶段的数据包转发就可以根据节点的转发表进行转发。

表4　各种安全协议所能实现的安全目标

协议名称	认证	完整性	机密性	新鲜度	审计性	可靠性	自我恢复能力
SEIF[14]	√	√	√	√		好	
MVMP[15]	√	√	√			好	√
INSENS[16]	√	√	√	√		有限的	
DENG[17]	√	√	√	√		中	
JERT[18]		√	√			好	√
Ling & Znati[19]		√	√	√		好	√
Chan[20]			√			好	
SEER[21-22]						中	
H-SPREAD[23]		√	√	√		好	√
PRSA[24]					√	中	√
TRANS[25]	√		√	√		中	√
SeRINS[26]	√	√	√	√	√	中	√
Lee & Choi[27]	√	√	√			中	√
Abu-Ghazaleh[28]	√	√	√		√	中	√
Zhang[29]	√	√	√	√		中	√
Ramaswami[30]					√	中	√
Song[31]					√	好	√
Zhao[32]						有限的	√
ESRS[33]	√		√	√	√	-	√
Lu[34]			√			有限的	
SAODV-MAP[35]	√	√	√	√	√	中	
SecMR[36]	√	√	√	√		可变的	
Lee[37-38]		√	√			好	
Chen and Leneutre[39]		√	√			好	
SELDA[40]			√		√	中	
SIGF[41]	√		√	√		可变的	√

2.4　认证与访问控制

认证指使用者采用某种方式来"证明"自己确实是自己宣称的某人,网络中的认证主要包括身份认证和消息认证。身份认证可以使通信双方确信对方的身份并交换会话密钥。保密性和及时性是认证的密钥交换中两个重要的问题。为了防止假冒和会话密钥的泄密,用户标识和会话密钥这样的重要信息必须以密文的形式传送,这就需要事先已有能用于这一目的的主密钥或公钥。因为可能存在消息重放,所以及时性非常重要,在最坏的情况下,攻击者可以利用重放攻击威胁会话密钥或者成功假冒另一方。

消息认证中主要是接收方希望能够保证其接收的消息确实来自真正的发送方。有时收发双方不同时在线,例如在电子邮件系统中,电子邮件消息发送到接收方的电子邮件中,并一直存放在邮箱中直至接收方读取为止。广播认证是一种特殊的消息认证形式,在广播认证中一方广播的消息被多方认证。

传统的认证是区分不同层次的,网络层的认证就负责网络层的身份鉴别,业务层的认证就负责业务层的身份鉴别,两者独立存在。但是在物联网中,业务应用与网络通信紧紧地绑在一起,认证有其特殊性。例如,当物联网的业务由运营商提供时,那么就可以充分利用网络层认证的结果而不需要进行业务层的认证;或者当业务是敏感业务如金融类业务时,一般业务提供者会不信任网络层的安全级别,而使用更高级别的安全保护,那么这个时候就需要做业务层的认证;而当业务是普通业务时,如气温采集业务等,业务提供者认为网络认证已经足够,那么就不再需要业务层的认证。

在物联网的认证过程中,传感网的认证机制是重要的研究部分,无线传感器网络中的认证技术主要包括基于轻量级公钥的认证技术、预共享密钥的认证技术、随机密钥预分布的认证技术、利用辅助信息的认证、基于单向散列函数的认证等。

(1) 基于轻量级公钥算法的认证技术。鉴于经典的公钥算法需要高计算量,在资源有限的无线传感器网络中不具有可操作性,当前有一些研究正致力于对公钥算法进行优化设计使其能适应于无线传感器网络,但在能耗和资源方面还存在很大的改进空间,如基于 RSA 公钥算法的 TinyPK 认证方案,以及基于身份标识的认证算法等。

(2) 基于预共享密钥的认证技术。SNEP 方案中提出两种配置方法:一是节点之间的共享密钥,二是每个节点和基站之间的共享密钥。这类方案使用每对节点之间共享一个主密钥,可以在任何一对节点之间建立安全通信。缺点表现为扩展性和抗捕获能力较差,任意一节点被俘获后就会暴露密钥信息,进而导致全网络瘫痪。

(3) 基于单向散列函数的认证方法。该类方法主要用在广播认证中,由单向散列函数生成一个密钥链,利用单向散列函数的不可逆性,保证密钥不可预测。通过某种方式依次公布密钥链中的密钥,可以对消息进行认证。目前基于单向散列函数的广播认证方法主要是对 μTESLA 协议的改进。μTESLA[42] 协议以 TESLA 协议为基础,对密钥更新过程,初始认证过程进行了改进,使其能够在无线传感器网络有效实施。

访问控制是对用户合法使用资源的认证和控制,目前信息系统的访问控制主要是基于角色的访问控制机制(role-based access control, RBAC)及其扩展模型。RBAC 机制主要由 Sandhu 于 96 年提出的基本模型 RBAC96 构成,一个用户先由系统分配一个角色,如管理员、普通用户等,登录系统后,根据用户的角色所设置的访问策略实现对资源的访问,显然,同样的角色可以访问同样的资源。RBAC 机制是基于互联网的 OA 系统、银行系统、网上商店等系统的访问控制方法,是基于用户的。对物联网而言,末端是感知网络,可能是一个感知节点或一个物体,采用用户角色的形式进行资源的控制显得不够灵活,一是本身基于角色的访问控制在分布式的网络环境中已呈现出不向适应的地方,如对具有时间约束资源的访问控制,访问控制的多层次适应性等方面需要进一步探讨;二是节点不是用户,是各类传感器或其他设备,且种类繁多,基于角色的访问控制机制中角色类型无法一一对应这些节点,因此,使 RBAC 机制的难于实现;三是物联网表现的是信息的感知互动过程,包含了信息的处理、决策和控制等过程,特别是反向控制是物物互连的特征之一,资源的访问呈现动态性和多层次性,而 RBAC 机制中一旦用户被指定为某种角色,他的可访问资源就相对固定了。所以,寻求新的访问控制机制是物联网、也是互联网值得研究的问题。

基于属性的访问控制(attribute-based access control, ABAC)是近几年研究的热点,如果将角色映射成用户的属性,可以构成 ABAC 与 RBAC 的对等关系,而属性的增加相对简单,同时基于属性的加密算法可以使 ABAC 得以实现。ABAC 方法的问题是对较少的属性来说,加密解密的效率较高,但随着属性数量的增加,加密的密文长度增加,使算法的实用性受到限制,目前有两个发展方向:基于密钥策略和基于密文策略,其目标就是改善基于属性的加密算法的性能。

2.5 入侵检测与容侵容错技术

容侵就是指在网络中存在恶意入侵的情况下,网络仍然能够正常地运行。无线传感器网络的安全隐患在于网络部署区域的开放特性以及无线电网络的广播特性,攻击者往往利用这两个特性,通过阻碍网络中节点的正常工作,进而破坏整个传感器网络的运行,降低网络的可用性。无人值守的恶劣环境

导致无线传感器网络缺少传统网络中的物理上的安全,传感器节点很容易被攻击者俘获、毁坏或妥协。现阶段无线传感器网络的容侵技术主要集中于网络的拓扑容侵、安全路由容侵以及数据传输过程中的容侵机制。

无线传感器网络可用性的另一个要求是网络的容错性。一般意义上的容错性是指在故障存在的情况下系统不失效、仍然能够正常工作的特性。无线传感器网络的容错性指的是当部分节点或链路失效后,网络能够进行传输数据的恢复或者网络结构自愈,从而尽可能减小节点或链路失效对无线传感器网络功能的影响。由于传感器节点在能量、存储空间、计算能力和通信带宽等诸多方面都受限,而且通常工作在恶劣的环境中,网络中的传感器节点经常会出现失效的状况。因此,容错性成为无线传感器网络中一个重要的设计因素,容错技术也是无线传感器网络研究的一个重要领域。目前相关领域的研究主要集中在:

(1) 网络拓扑中的容错。通过对无线传感器网络设计合理的拓扑结构,保证网络出现断裂的情况下,能正常进行通信。

(2) 网络覆盖中的容错。无线传感器网络的部署阶段,主要研究在部分节点、链路失效的情况下,如何事先部署或事后移动、补充传感器节点,从而保证对监测区域的覆盖和保持网络节点之间的连通。

(3) 数据检测中的容错机制。主要研究在恶劣的网络环境中,当一些特定事件发生时,处于事件发生区域的节点如何能够正确获取到数据。

文献[21]提出了一种无线传感器网络中的容侵框架。该框架包括三个部分:

(1) 判定恶意节点:主要任务是要找出网络中的攻击节点或被妥协的节点。基站随机发送一个通过公钥加密的报文给节点,为了回应这个报文,节点必须能够利用其私钥对报文进行解密并回送给基站,如果基站长时间接收不到节点的回应报文,则认为该节点可能遭受到入侵。另一种判定机制是利用邻居节点的签名。如果节点发送数据包给基站,需要获得一定数量的邻居节点对该数据包的签名。当数据包和签名到达基站后,基站通过验证签名的合法性来判定数据包的合法性,进而判定节点为恶意节点的可能性。

(2) 发现恶意节点后启动容侵机制:当基站发现网络中的可能存在的恶意节点后,则发送一个信息包告知恶意节点周围的邻居节点可能的入侵情况。因为还不能确定节点是恶意节点,邻居节点只是将该节点的状态修改为容侵,即节点仍然能够在邻居节点的控制下进行数据的转发。

(3)通过节点之间的协作,对恶意节点做出处理决定(排除或是恢复):一定数量的邻居节点产生编造的报警报文,并对报警报文进行正确的签名,然后将报警报文转发给恶意节点。邻居节点监测恶意节点对报警报文的处理情况。正常节点在接收到报警报文后,会产生正确的签名,而恶意节点则可能产生无效的签名。邻居节点根据接收到的恶意节点的无效签名的数量来确定节点是恶意节点的可能性。通过各个邻居节点对节点是恶意节点性测时信息的判断,选择攻击或放弃。

根据无线传感器网络中不同的入侵情况,可以设计出不同的容侵机制,如无线传感器网络中的拓扑容侵、路由容侵和数据传输容侵等机制。前面讨论的路由协议 INTRSN 就是具有路由容侵的情况。

2.6　决策与控制安全

物联网的数据是一个双向流动的信息流,一是从感知端采集物理世界的各种信息,经过数据的处理,存储在网络的数据库中;二是根据用户的需求,进行数据的挖掘、决策和控制,实现与物理世界中任何互连物体的互动。在数据采集处理中我们讨论了相关的隐私性等安全问题,而决策控制又将涉及到另一个安全问题,如可靠性等。前面讨论的认证和访问控制机制可以对用户进行认证,使合法的用户才能使用相关的数据,并对系统进行控制操作。但问题是如何保证决策和控制的正确性和可靠性。

在传统的无线传感器网络网络中由于侧重对感知端的信息获取,对决策控制的安全考虑不多,互联网的应用也是侧重与信息的获取与挖掘,较少应用对第三方的控制。而物联网中对物体的控制将是重要的组成部分,需要进一步更深入的研究。

3　结　论

物联网的安全和隐私保护是物联网服务能否大规模应用的关键,物联网的多源异构性使其安全面临巨大的挑战,就单一网络而言,互联网、移动通信网等已建立了一些列行之有效的机制和方法,为我们的日程生活和工作提供了丰富的信息资源,改变了人们的生活和工作方式。相对而言,传感网的安全研究仍处于初始阶段,还没有提供一个完整的解决方案,由于传感网的资源局限性,使其安全问题的

研究难度增大,因此,传感网的安全研究将是物联网安全的重要组成部分。同时如何建立有效的多网融合的安全架构,建立一个跨越多网的统一安全模型,形成有效的共同协调防御系统也是重要的研究方向之一。

目前在无线传感器网络安全方面,人们就密钥管理、安全路由、认证与访问控制、数据隐私保护、入侵检测与容错容侵、以及安全决策与控制等方面进行了相关研究,密钥管理作为多个安全机制的基础一直是研究的热点,但并没有找到理想的解决方案,要么寻求更轻量级的加密算法,要么提高传感器节点的性能,目前的方法距实际应用还有一定的距离,特别是至今为止,真正的大规模的无线传感器网络的实际应用仍然太少,多跳自组织网络环境下的大规模数据处理(如路由和数据融合)使很多理论上的小规模仿真失去意义,而在这种环境下的安全问题才是传感网安全的难点所在。

参考文献:

[1] http://www.epcglobalinc.org/

[2] CONTI J P. The Internet of things[J]. Communications Engineer, 2006,4(6):20-25.

[3] ITU. The Internet of Things. [EB/OL]. (2005-12-17)[2010-07-03]. http://www.itu.int/internetofthings.

[4] 王小妮,魏桂英. 物联网RFID系统数据传输中密码算法研究[J]. 北京信息科技大学学报:自然科学版,2009,24(4):75-78.
WANG Xiaoni, WEI Guiying. Cipher algorithm in data transmission of RFID system on the internet for things[J]. Journal of Beijing Information Science and Technology University (Natural Science), 2009,24(4):25-78. (in Chinese)

[5] 宁焕生,张瑜,刘芳丽,等. 中国物联网信息服务系统研究[J]. 电子学报,2006,34(12):2514-2517.
NING Huansheng, ZHANG Yu, LIU Fangli, et al. Research on China Internet of Things' Services and Management[J]. Acta Electronica Sinica, 2006,34(12):2514-2517. (in Chinese)

[6] WEBER R H, Internet of Things-New security and privacy challenges[J]. Computer Law & Security Review, 2010,26:23-30

[7] LEUSSE P, PERIORELLIS P, DIMITRAKOS T, et al. Self Managed Security Cell, a security model for the Internet of Things and Services[C]// Proc of the 2009 First International Conference on Advances in Future Internet. Piscataway: IEEE, 2009, 47-52

[8] MULLIGAN G. The Internet of Things: Here Now and Coming Soon [J]. Internet Computing, 2010, 1:36-37.

[9] HAMAD F, SMALOV L, JAMES A. Energy-aware security in M-commerce and the Internet of Things[J]. IETE, Technical review, 2009,26(5):357-362.

[10] WATRO R, KONG D, et al. TinyPK: Securing sensor networks with public key technology[C]// Proc of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM press, 2004:59-64.

[11] BENENSON Z, GEDICKE N, RAIVIO O. Realizing robust user authentication in sensor networks[C]//Proc of the Workshop on Real-World Wireless Sensor Networks (REALWSN 2005). [S. l.]: Stockholm, 2005. 135-142.

[12] MALAN D J, WELSH M, SMITH M D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography [C]// 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks. Piscataway: IEEE, 2004:71-80.

[13] 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.
YANG Geng, WANG Jiangtao, CHENG Hongbing, et al. An identity-based key distribution scheme for WSNs[J]. Chinese Journal of Electronic, 2007,35(1):180-185. (in Chinese)

[14] OUADJAOUT A, CHALLAL Y, LASLA N, et al. SEIF: Secure and efficient intrusion-fault tolerant routing protocol for wireless sensor networks[C]// Proc of the Third International Conference on Availability, Reliability and Security (ARES 2008). Piscataway: IEEE, 2008:503-508.

[15] MA R, XING L D, MICHEL H E. A new mechanism for achieving secure and reliable data transmission in wireless sensor networks [C]// Proc of the 2007 IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability. Piscataway: IEEE, 2007:274-279.

[16] DENG Jing, HAN R, MISHRA S. Insens: Intrusion tolerant routing for wireless sensor networks[J]. Computer Communications, 2006, 29(2):216-230.

[17] DENG Jing, HAN R, MISHRA S. Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks[C]// Proceedings of the 2004 IEEE International Conference on Dependable Systems and Networks. Piscataway: IEEE, 2004:637-646.

[18] DENG Jing, HAN Y S. Multipath key establishment for wireless sensor networks using just-enough redundancy transmission[J]. IEEE Trans on Dependable and Secure Computing, 2008, 5(3): 177-190.

[19] LING Hui, ZNATI T. End-to-end pairwise key establishment using multipath in wireless sensor network [C] // Proceedings of the IEEE Global Communications Conference (GLOBECOM 2005). New York: IEEE, 2005.

[20] CHAN H, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[C]//Proc of the 2003 IEEE Symposium on Security and Privacy (SP'03). New York: IEEE, 2003: 197-213.

[21] NASSER N, CHEN Y. Secure multipath routing protocol for wireless sensor networks[C]// Proc of the 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07). Piscataway: IEEE, 2007:12.

[22] NASSER N, CHEN Y. SEEM: Secure and energy-efficient mul-

tipath routing protocol for wireless sensor networks[J]. Computer Communications,2007,30(11/12):2401 - 2412.

[23] LOU W,KWON Y. H-SPREAD:A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks[J]. IEEE Transactions on Vehicular Technology,2006,55(4) :1320 - 1330.

[24] AL-WAKEEL S S,AL-SWAILEMM S A. PRSA:A path redundancy based security algorithm for wireless sensor networks[C] // IEEE Wireless Communications and Networking Conference(WCNC 2007). New York:IEEE,2007.

[25] TANACHAIWIWAT S,DAVE P,BHINDWALE R,et al. Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks[C] // Proceedings of IEEE Workshop on Energy-Efficient Wireless Communications and Networks (EWCN). New York:IEEE,2004

[26] LEE S,CHOI Y. A secure alternate path routing in sensor networks [J]. Computer Communications,2006,30(1):153 - 165.

[27] LEE S,CHOI Y. A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks[C] // Proceedings of the Fourth ACM Workshop on Security of Ad hoc and Sensor Networks(SASN'06). Piscataway:IEEE,2006:59 - 70.

[28] ABU-GHAZALEH N, KANG K, LIU K. Towards resilient geographic routing in WSNs[C] // Proceedings of the First ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks. Piscataway:IEEE,2005:71 - 78.

[29] ZHANG Y,YANG J,VU H T. The interleaved authentication for filtering false reports in multipath routing based sensor networks [C] // Proceedings of the 20th International IEEE Parallel and Distributed Processing Symposium (IPDPS'06). Piscataway: IEEE,2006.

[30] RAMASWAMI S S,UPADHYAYA S. Smart handling of colluding black hole attacks in MANETs and wireless sensor networks using multipath routing[C] // Proceedings of the 2006 IEEE Workshop on Information Assurance. Piscataway:IEEE,2006:253 - 260.

[31] SONG Ning,QIAN Lijun,LI Xiangfang. Wormhole attacks detection in wireless ad hoc networks:a statistical analysis approach[C] // Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium. Piscataway:IEEE,2005.

[32] ZHAO L,DELGADO-FRIAS J G. Multipath routing based secure data transmission in adhoc networks[C] // IEEE International Conference on Wireless and Mobile Computing,Networking and Communications(WiMob 2006). Piscataway:IEEE,2006.

[33] LIAO Chengfu,LU Yungfeng,PANG Aichun,et al. A secure routing protocol for wireless embedded networks[C] // Proceedings of the 14th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications. Piscataway: IEEE,2008.

[34] LU F,GENG L,CHIA L T,et al. Secure multi-path in sensor networks[C] // Proceedings of the Fifth International Conference on Embedded Networked Sensor Systems(SenSys '07). New York: Acm,2007:413 - 414.

[35] VAIDYA B,PYUN J Y,PARK J A,et al. Secure multipath routing scheme for mobile ad hoc network[C] // Proceedings of the Third IEEE International Symposium on Dependable,Autonomic and Secure Computing. Piscataway:IEEE,2007.

[36] MAVROPODI R,KOTZANIKOLAOU P,DOULIGERIS C. SecMR-secure multipath routing protocol for ad hoc networks[J]. Ad Hoc Networks,2007,5(1):87 - 99.

[37] LEE P P C,MISRA V,RUBENSTEIN D. Distributed algorithms for secure multipath routing in attack-resistant networks[J]. IEEE/ACM Trans on Networking,2007,15(6):1490 - 1501.

[38] LEE P P C,MISRA V,RUBENSTEIN D. Distributed algorithms for secure multipath routing[C] // Proc IEEE INFOCOM. Piscataway: IEEE,2005:1952 - 1963.

[39] CHEN L,LENEUTRE J. On multipath routing in multihop wireless networks:security,performance,and their tradeoff[J]. EURASIP Journal on Wireless Communications and Networking,2009,2009: 60 - 72.

[40] OZDEMIR S. Secure and reliable data aggregation for wireless sensor networks[C] // ICHIKAWA H. LNCS. Heidelberg: Springer Verlag,2007,4836:102 - 109.

[41] WOOD A D,FANG Lei,STANKOVIC J A,et al. Sigf:A family of configurable,secure routing protocols for wireless sensor networks [C] // Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks(SASN). New York:ACM,2006:35 - 48.

[42] LIU D,NING P. Multi-level μTESLA:A broadcast authentication system for distributed sensor networks[J]. ACM Transactions on Embedded Computing Systems(TECS),2004,3(4):800 - 836.

作者简介:

杨　庚(1961 -),男,江苏建湖人。南京邮电大学科技处处长,教授,博士生导师。(见本刊2010年第2期第94页)

许　建(1980 -),男,江苏徐州人。南京邮电大学计算机学院讲师,博士研究生。主要研究方向为信息安全、无线自组织网络等。

陈　伟(1979 -),男,江苏连云港人。南京邮电大学计算机学院讲师。主要研究方向为网络安全。

祁正华(1975 -),女,陕西宝鸡人。南京邮电大学计算机学院讲师,博士研究生。主要研究方向为信息安全和网格计算。

王海勇(1979 -),男,江苏连云港人。南京邮电大学计算机学院博士研究生。主要研究方向为信息安全、视频压缩、多媒体通信等。

(责任编辑:宋福明)

物联网安全特征与关键技术

作者： 杨庚， 许建， 陈伟， 祁正华， 王海勇， YANG Geng， XU Jian， CHEN Wei， Qi Zheng-hua， WANG Hai-yong

作者单位： 杨庚,YANG Geng(南京邮电大学,科技处,江苏,南京,210046)， 许建,陈伟,祁正华,王海勇,XU Jian,CHEN Wei,Qi Zheng-hua,WANG Hai-yong(南京邮电大学,计算机学院,江苏,南京,210046)

刊名： 南京邮电大学学报（自然科学版） ISTIC

英文刊名： JOURNAL OF NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS(NATURAL SCIENCE)

年，卷(期)： 2010,30(4)

参考文献(42条)

1. WEBER R H Internet of Things-New security and privacy challenges 2010

2. 宁焕生;张瑜;刘芳丽 中国物联网信息服务系统研究[期刊论文]-电子学报 2006(12)

3. 王小妮;魏桂英 物联网RFID系统数据传输中密码算法研究[期刊论文]-北京信息科技大学学报(自然科学版) 2009(04)

4. TANACHAIWIWAT S;DAVE P;BHINDWALE R Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks 2004

5. AL-WAKEEL S S;AL-SWAILEMM S A PRSA:A path redundancy based security algorithm for wireless sensor networks 2007

6. BENENSON Z;GEDICKE N;RAIVIO O Realizing robust user authentication in sensor networks 2005

7. WATRO R;KONG D TinyPK:Securing sensor networks with public key technology 2004

8. CONTI J P The Internet of things[外文期刊] 2006(06)

9. LIU D;NING P Multi-level μTESLA:A broadcast authentication system for distributed sensor networks [外文期刊] 2004(04)

10. WOOD A D;FANG Lei;STANKOVIC J A Sigf:A family of configurable,secure routing protocols for wireless sensor networks 2006

11. OZDEMIR S Secure and reliable data aggregation for wireless sensor networks 2007

12. CHEN L;LENEUTRE J On multipath routing in multihop wireless networks:security,performance,and their tradeoff 2009

13. HAMAD F;SMALOV L;JAMES A Energy-aware security in M-commerce and the Internet of Things 2009(05)

14. MULLIGAN G The Internet of Things:Here Now and Coming Soon 2010

15. LEUSSE P;PERIORELLIS P;DIMITRAKOS T Self Managed Security Cell,a security model for the Internet of Things and Services 2009

16. ITU The Internet of Things 2010

17. LEE P P C;MISRA V;RUBENSTEIN D Distributed algorithms for secure multipath routing 2005

18. LEE P P C;MISRA V;RUBENSTEIN D Distributed algorithms for secure multipath routing in attack-resistant networks 2007(06)

19. MAVROPODI R;KOTZANIKOLAOU P;DOULIGERIS C SecMR-secure multipath routing protocol for ad hoc networks[外文期刊] 2007(01)

20. VAIDYA B;PYUN J Y;PARK J A Secure multipath routing scheme for mobile ad hoc network 2007

21. LU F;GENG L;CHIA L T Secure multi-path in sensor networks 2007

22. LIAO Chengfu;LU Yungfeng;PANG Aichun A secure routing protocol for wireless embedded networks 2008

23. ZHAO L;DELGADO-FRIAS J G Multipath routing based secure data transmission in adhoc networks 2006

24. SONG Ning;QIAN Lijun;LI Xiangfang Wormhole attacks detection in wireless ad hoc networks:a statistical analysis approach 2005

25. RAMASWAMI S S;UPADHYAYA S Smart handling of colluding black hole attacks in MANETs and wireless sensor networks using multipath routing 2006

26. ZHANG Y;YANG J;VU H T The interleaved authentication for filtering false reports in multipath routing based sensor networks 2006

27. ABU-GHAZALEH N;KANG K;LIU K Towards resilient geographic routing in WSNs 2005

28. LEE S;CHOI Y A resilient packet-forwarding scheme against maliciously packet-dropping nodes in sensor networks 2006

29. LEE S;CHOI Y A secure alternate path routing in sensor networks[外文期刊] 2006(01)

30. LOU W;KWON Y H-SPREAD:A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks[外文期刊] 2006(04)

31. NASSER N;CHEN Y SEEM:Secure and energy-efficient multipath routing protocol for wireless sensor networks[外文期刊] 2007(11/12)

32. NASSER N;CHEN Y Secure multipath routing protocol for wireless sensor networks 2007

33. CHAN H;PERRIG A;SONG D Random key predistribution schemes for sensor networks 2003

34. LING Hui;ZNATI T End-to-end pairwise key establishment using multipath in wireless sensor network 2005

35. DENG Jing;HAN Y S Multipath key establishment for wireless sensor networks using just-enough redundancy transmission[外文期刊] 2008(03)

36. DENG Jing;HAN R;MISHRA S Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks 2004

37. DENG Jing;HAN R;MISHRA S Insens:Intrusion tolerant routing for wireless sensor networks[外文期刊] 2006(02)

38. MA R;XING L D;MICHEL H E A new mechanism for achieving secure and reliable data transmission in wireless sensor networks 2007

39. OUADJAOUT A;CHALLAL Y;LASLA N SEIF:Secure and efficient intrusion-fault tolerant routing protocol for wireless sensor networks 2008

40. 杨庚;王江涛;程宏兵 基于身份加密的无线传感器网络密钥分配方法[期刊论文]-电子学报 2007(01)

41. MALAN D J;WELSH M;SMITH M D A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography 2004

42. 查看详情