物联网安全架构与关键技术

李志清

(广州行政学院 信息网络中心,广州 广东 510070)

摘 要: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,分析了物联网安全需求和面临的安全问题,提出了物联网安全的系统架构,并对一些安全关键技术进行了深入研究,希望为建立物联网可靠的信息安全体系提供参考依据。

关键词:物联网;信息安全;安全架构;密钥管理机制;安全路由协议

中图分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2011)09-0054-03

Security architecture and technology in the Internet of things

Li Zhiqing

(Guangzhou Administration Institute, Information and Network Center, Guangzhou 510070, China)

Abstract: Based on confidentiality, integrity and availability, this paper analyzes the security demand and problems in IoT. It proposes a security framework and discusses some techniques in depth, expecting to offer a reference for the establishment of reliable security systems of information for the IoT in the future.

Key words: Internet of things; information security; security architecture; key management mechanism; secure routing protocol

物联网IoT(Internet of Things)指的是将各种信息传感设备(如射频识别、红外感应器、全球定位系统、激光扫描器等)与互联网结合起来而形成的一个巨大网络[1]。物联网的信息安全问题是关系物联网产业能否安全可持续发展的核心技术之一,必需引起高度重视。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。参考文献[2]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,参考文献[3]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。参考文献[4]讨论了物联网的安全和隐私保护问题,特别讨论了所涉及的法律问题。参考文献[5]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。参考文献[6]对物联网的状况进行了分析,也讨论了安全问题。参考文献[7]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,探讨物联网安全方面的需求及其面临的安全威胁,研究物联网安全的系统架构,对一些关键安全技术进行深入的讨论。

1 物联网的安全需求

信息与网络安全的目标是要达到被保护信息的机密性、完整性和可用性。随着网络和服务规模的不断增大,安全问题越来越引起人们的高度重视,相继推出了一些安全技术,如防火墙、入侵检测系统、PKI等。物联网的研究与应用仍处于初级阶段,很多的理论与关键技术还有待突破,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。

信息隐私是物联网信息机密性的直接体现,例如,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。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，而对感知网络的密钥管理更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。物联网与许多应用领域的物理设备相关联，要保证网络的稳定可靠，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、网络环境和应用需求的多样性，其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。

2 物联网的安全架构

中国移动总裁王建宙指出，物联网应具备三个特征：全面感知、可靠传递和智能处理[8]。尽管对物联网概念还有其他一些不同的描述，但内涵基本相同。因此在分析物联网的安全性时，也相应地将其分为三个逻辑层，即感知层、传输层和处理层。除此之外，在物联网的综合应用方面还应该有一个应用层，它是对智能处理后的信息的利用。在某些框架中，尽管智能处理与应用层都可能被作为同一逻辑层进行处理，但从信息安全的角度考虑，将应用层独立出来更容易建立安全架构。本文结合物联网 DCM 模式提出物联网的安全架构，如图 1 所示。

图 1 物联网安全架构

物理安全层：保证物联网信息采集节点不被欺骗、控制、破坏。

信息采集安全层：防止采集的信息被窃听、篡改、伪造和重放攻击，主要涉及传感技术和 RFID 的安全。在物联网层次模型中，物理安全层和信息采集安全层对应于物联网的感知层安全。感知层采用的安全技术包括：高速密码芯片、密码技术、PKI 公钥基础设施等。

信息传输安全层：保证信息传递过程中数据的机密性、完整性、真实性和可用性，主要是电信通信网络的安全，对应于物联网的传输层安全。传输层采用的安全技术包括：虚拟专用网、无线网安全、安全路由、防火墙、安全域策略等。

信息处理安全层：保证信息的处理和储存安全等，主要是云计算安全和中间件安全等，对应于物联网中处理层安全。处理层采用的安全技术包括：内容分析、病毒防治、攻击监测、应急反应、战略预警等。

信息应用安全层：保证信息的私密性和使用安全等，主要是个体隐私保护和应用安全等，对应于物联网中应用层安全。应用层采用的安全技术包括：身份认证、可信终端、访问控制、安全审计等。

3 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，对其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。

3.1 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。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；二是如何解决传感器网络的密钥管理问题，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：(1)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。(2)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，但在传感器网络环境中对汇聚点的要求就比较高，尽管可以在传感器网络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，使传感器网络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：密钥生成或更新算法的安全性、前向私密性、后向私密性和可扩展性、抗同谋攻击、源端认证性和新鲜性[9]。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基于密钥分配中心方式、预分配方式和基于分组分簇方式三类。

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,Tiny PK[10]在使用 Tiny OS 开发环境的 MICA 2 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 Tiny Sec 密钥的分发。参考文献[11]首次在 MICA 2 节点上基于椭圆曲线密码 ECC(Ellipse Curve Cryptography)实现了 Tiny OS 的 Tiny Sec 密钥的分发,参考文献[12]和[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及应用前景。

3.2 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、基于标识的移动通信网和传感网的路由算法,因此至少需要解决两个问题:多网融合的路由问题以及传感器网络的路由问题。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;后者是由于传感器网络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、计算能力和存储容量都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。抗击这些攻击可采用链路层加密和认证、身份验证、双向链路认证、多径路由技术等方法。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、TEEN 等)以及基于位置信息的路由(如 GPSR、GEAR 等)。

没有物联网的安全就没有它的广泛应用。目前我国物联网的发展还处于初级阶段,关于物联网的安全研究任重而道远。由于传感器网络的资源局限性,对其安全问题的研究难度增大,因此,传感器网络的安全研究将是建立物联网安全体系的重要组成部分。总体来说,未来的物联网安全研究主要集中在开放的物联网安全体系、物联网个体隐私保护模式、终端安全功能、物联网安全相关法律的制定等几个方面。

参考文献

[1] International Telecommunication Union. The Internet of things[R]. ITU Report,2005.

[2] ITU. The Internet of Things [EB/OL]. http://www.itu.int/internetofthings, [2010-07-03].

[3] 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.

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

[5] LEUSSE P, PERIORELLIS P, DIM ITRAKOST, et al. Self managed security cell, a security model for the Internet of Things and Services [C]. Proceedings of the 2009 First International Conference on Advances in Future Internet. Piscataway: IEEE, 2009: 47-52.

[6] MULLIGAN G. The Internet of Things: here now and coming soon[J]. IEEE Internet Computing,2010,14(1):36-37.

[7] HAMAD F, SMALOV L, JAMES A. Energy-aw are security in commerce and the Internet of things [J]. IEEE, Technical Review, 2009, 26(5):357-362.

[8] 王建宙.从互联网到"物联网"[J].通信世界,2009,33(9).

[9] 裴庆祺,沈玉龙,马建峰.无线传感器网络安全技术综述[J].通信学报,2007,28(8):113-122.

[10] WATRO R, KONG D. Tiny PK: securing sensor networks with public key technology [C]. Proceedings 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, RA IVIO O. Realizing robust user authentication in sensor networks [C]. Proceedings of the Work shop on Real-World Wireless Sensor Networks (REALWSN 2005). [S..l]: Stockholm, 2005:135-142.

[12] MALAND J, WELSH M, SMITHM D. A public-key in frastructure for key distribution in Tiny OS 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.

(收稿日期:2011-01-02)

作者简介:

李志清,男,1981 年生,硕士,讲师,主要研究方向:网络与信息安全技术。