学校编码：10384　　分类号_____密级_____
学　　号：X2010221024　　UDC_____

厦门大学

工 程 硕 士 学 位 论 文

无线传感器网络密钥安全及其应用研究

Research on Key Security of Wireless Sensor Networks and Its Application

禹 谢 华

指导教师姓名：李 绍 滋　教 授
专 业 名 称：计 算 机 技 术
论文提交日期：2016 年　月
论文答辩时间：2016 年　月
学位授予日期：2016 年　月

答辩委员会主席：
评　阅　人：

2016 年　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：禹谢华

2016年8月7日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（√）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：[illegible]

2016年9月7日

摘　要

在无线传感器网络中，如果通信双方或某一方的密钥一旦丢失、被窃取或者泄露，就必将直接威胁到整个网络，无线传感器网络通信的安全性就将无法得以保证。众所周知，密钥在密码算法中是处于可变的部分，在一切采用了密码技术进行保护的信息系统中，其密钥的良好保护性将直接决定了系统安全性的高低。而密钥的管理研究是控制密钥的产生、分配、更新以及撤销等过程的重要依据，它在密码系统中起着决定性的作用，特别是针对特殊的无线WSN网络环境，安全密钥管理方案的研究就更显重要，已逐渐成为了目前研究WSN安全的基础和核心课题。

本文的主要目的是在充分研究和分析现有密钥管理方案的基础上，针对当前密钥管理方案中存在的各种缺陷和不足，提出一个符合当前网络评估指标的适合于无线WSN网络的密钥安全管理方案。本文的贡献点主要有以下三个方面，如下所示：

1．由无线WSN网络密钥管理方案领域的最新研究进展入手，对现有的密钥管理方案进行分类比较，给出了一个优良的无线WSN网络密钥管理方案所应具备的设计目标以及安全评估体系，为相关研究者设计符合规范的无线传感器网络安全密钥管理方案铺垫了理论基础。

2．提出了一种基于分簇策略的异构无线传感器网络安全密钥管理方案。作为一类特殊的无线WSN网络和一种新颖的信息获取平台，异构无线传感器网络具备了实时感知、监测和搜集复杂条件下的网络环境中不同监测对象的各种信息的功能。本文主要针对异构无线WSN网络中密钥的安全管理问题，提出了基于分簇策略的密钥管理设计方案。实验结果表明：提出的方案在节点抗捕获能力、续航性能及认证方式等方面均优于已有同类其他方案，能够有效的弥补当前安全密钥管理方案的缺陷和不足，从而在一定程度上实现异构无线传感器网络的安全通信。

3．设计实现了一种基于无线WSN网络的海洋环境安全监控系统。在对美国Crossbow（克尔斯博）无线传感器网络的软件构架和拓扑结构进行了深入分析和测试的基础上，结合卫星通信技术、计算机智能信息处理技术及互联网平台监控管理查询技术等，建立了适用于测量领海与公海气象水文要素和生态水质量参数

的海洋环境监控网络，同时能够轻松实现在线实时探测的任务，为我国海洋环境监控工作提供了新的途径和技术实现方式，具有较好的参考意义和极其广泛的应用前景。

最后，对论文的研究工作以及研究过程中所取得的部分成果进行了简单的概括和总结，在此基础上结合社会应用提出了研究工作中尚存在的部分疑难问题和不足之处，并结合目前国家科技最前沿的技术对可能的改进方案进行展望，明确以后进一步努力工作的目标和方向。

关键词：无线传感器网络；密钥安全；分簇策略；应用研究

Abstract

In wireless sensor networks, if the encryption keys of both sides or a key on one side of the communication has been lost, stolen or leaked, then it will be a direct threat to the entire network, and the security of the wireless sensor network communication will not be guaranteed. As we all know, the cipher algorithm of an encryption key is variable, and in all the information systems which use password protection, a well-protected encryption key will directly determine the level of security of the systems. The management research of the encryption key is an important basis in the process of controlling the key's generation, distribution, update and revocation. The encryption key plays a fundamental and decisive role in password systems, especially in a wireless sensor network(WSN) environment. Thus, the research on the security key management scheme becomes increasingly important, and has gradually become the foundation and core topic of the research on WSN security.

Based on the full research and the analysis of existing security key management schemes, and in view of their various defects and deficiencies, the main purpose of this thesis is to put forward a secure key management scheme which is suitable for the current network evaluation index and fits the wireless sensor networks. The three main contributions of the thesis are as follows:

1. Based on the latest research progress of security key management schemes in wireless sensor networks, this thesis talks about the classification and comparison of existing management schemes. It provides an excellent design goal and a security evaluation system of the WSN management schemes which serve as the theoretical basis for relevant researchers who want to design a WSN security key management scheme that conforms to the norm.

2. Based on clustering scheme, this thesis has put forward a secure key management scheme for Heterogeneous Wireless Sensor Network. As a special kind of WSN and a new information acquisition platform, heterogeneous wireless sensor

networks have the function of real-time monitoring, sensing and collecting various information of monitoring objects in complex network areas. This thesis mainly proposes an effective design scheme for the security management of keys in heterogeneous wireless sensor networks. The experimental data shows that the key management scheme based on clustering scheme proposed in this thesis is superior to other schemes in the aspect of node anti-capture capability, endurance performance, authentication method, and so on. It can effectively make up for the defects and deficiencies of the current security key management scheme, so it can realize a secure communication of heterogeneous wireless sensor networks to some extent.

3. Based on the wireless sensor network, this thesis has put forward a safety monitoring system for marine environment. Based on the analysis and testing of the software architecture and topological structure of American Crossbow wireless sensor networks, combining satellite communication technology, computer intelligent information processing technology and the monitoring, management and query technology of Internet platform, this thesis talks about the establishment of a network for marine environmental monitoring which is suitable for the measurement of the meteorological and hydrological factors and ecological water quality parameters of the territorial sea and the high seas. At the same time, the network can easily realize the task of online real-time detection, and provides a new approach and technique in the implementation of a marine environmental monitoring in China. Thus, it has good referential meaning and has a very broad prospect for application.

At the end of this thesis, a brief summary about the research work and some partial results was made. On this basis, some existing problems and deficiencies in the research, particularly with regards to its social applications, were put forward. Coupled with the bright prospect of our country’s advancement on the latest cutting edge technologies, some possible improvements and an established direction for further research work in the future were determined.

Key Words: Wireless Sensor Networks; Key Security; Clustering strategy; application research

目　录

Content

第一章 绪 论

1.1 课题的研究背景及意义

1.1.1 课题背景

二十一世纪是信息爆炸的时代，信息时代的到来使得信息的及时、有效获取成为人们日常生活中极其重要的组成部分。小到购物shopping、出门旅游，大到结婚嫁娶、购房炒股和买卖黄金外汇等，无一不跟信息的迅速和准确获取有着紧密的联系。近年来，随着计算机网络通信技术、单片机技术、微机控制技术、微电子电系统(MEMS)技术和无线WSN技术的飞速发展和日趋成熟，信息的获取已经不再单一。而科技的普及和进一步发展使得低功耗、低成本和功能丰富的微型无线传感器的实验和大规模实施成为了可能。这些无线传感器虽然体积很小，但却功能强大，他们不仅具有在恶劣环境中进行感知、获取和无线传输数据的能力，还能够及时对提取的物理环境信息进行初步计算、汇聚处理和相互协同合作等的能力，从而构成了一种非常新颖的信息搜集和传输模式——无线传感器网络(Wireless Sensor Networks，简称WSN)。

简而言之，无线传感器网络就是一种由大量具有数据的感知和搜集能力，具备有数据的无线传输、通信，信息的简单计算和处理的能力，体积细小的无线传感器节点所组成的无线式自组织网络系统[1]。这种网络系统主要以数据信息资源为中心，其优势就在于能够在非常恶劣的环境条件中，依靠大量部署在极端条件下、以动态自组织协作配合工作的传感器节点感知周围环境、并回传所采集到的各类信息，供人类参考、预测和规划的制定等。当前，随着微电子技术的高速发展和制造工艺的进一步提高，传感器也朝着微型化、智能化和集成化的方向发展。在人们的生活实际应用中，大部分的数据采集均会遇到采集点众多、采集范围大、地势险峻而致使不易布线等难题，传统的通过总线方式连接的传感器网络，已经无法满足当前的实际需求及应用。于是，融合了多种先进科技的无线传感器网络便应运而生。这种新型WSN中的节点间距不大，且一般情况下都是以多跳(multi hop)的方式进行数据的无线通信、传输及处理。每一个传感器节点既可以通过设置网关与互联网Internet进行通信，使得用户能够远程进行访问控制，更重要的

是其节点还可以在独立的环境下进行运作，实现真正意义上的“无处不在的计算”的现代科技观念[2]。

无线传感器网络是继上一代因特网科技之后的又一项IT热点技术，具有难以想象的应用前景，已经引起了全球科学界、商业界甚至是军事和工业界的广泛关注。著名的MIT技术评论将无线WSN网络技术列入了对未来世界有深远意义的世界十大新科技之一[3]，并把他称为是继Internet因特网之后，将对二十一世纪的人类在生活方式方面产生巨大影响的最重要的IT热门科技之一。不仅如此，美国各级军事部门上下，尤其是美国的国防部也对无线传感器网络产生了空前的高度关注，随即提出了美军二十一世纪的C4ISRT综合功能战斗系统及战略管理计划，其中就设立了一大批与军事传感器网络相关的研究课题，其主旨便在于提高部队在实战当中“感知敌方情报并及时处理信息的能力”、“综合并快速反应战争局势的能力”和“截获并破译情报信息的能力”、“辨识情报真伪并能够有效利用的能力”等，把无线传感器网络的研究推向了未来军事战况研究的最顶端[4]。我国也十分重视无线传感器网络的研究，中国“未来二十年技术预见研究”提出的一百五十七个科研课题中就有七项直接涉及无线WSN网络。2006年初的时候，我国政府在《国家中长期科学与技术发展规划纲要》中就明确指出了在未来的十五年里要大力促进和发展无线传感器网络技术。尤其是在发展信息技术所确定的3个前沿方向中，就有两项（自组织网络技术和智能感知技术）与无线传感器网络研究直接相关的，足以看出国家对无线WSN网络技术的重视程度。除此之外，国家自然科学基金委员会也已经跟上了步伐，近年来在该领域设立了很多的重点课题和研究项目，以推动学术界在无线传感器网络基础理论方面的研究[5、6]。可见，无线传感器网络技术的研究正处于二十一世纪新科技的最前沿，目前仍然有着很多值得广大科研机构和IT爱好者探讨和挖掘的热点内容，已经成为一个极其重要和相当热门的新的研究方向。

随着WSN的应用范围越来越广，WSN的安全问题也显得日益突出，行之有效的无线传感器网络安全机制的缺失已逐渐让WSN的应用步入了瓶颈，应用难以前行。因此，如何提高WSN的安全性已成为无线传感器网络进一步有效发展需要解决的一个至关重要的问题。在通信安全方面，由于其无线通信模式，使得它不再拥有传统网络中节点有较强计算能力、通信能力、存储能力和交互能力等的优势，而

其节点自身资源受限的特点，致使其在受到各种类型的外界攻击下容易发生节点受损和链路失效的情况；在网络规划方面，传感器节点一般部署在野外或极其恶劣的环境中，且在部署后就不再甚至根本无法进行人工维护，彻彻底底的只能依赖传感器网络节点相互之间的联络运作，从而以随机自组织的方式进行无线通信联网。

以上种种因素都很容易导致其节点被信息窃取或受到外部的攻击等，其安全问题就显得尤为突出[7]。因此，作为一项极具挑战性和现实性的研究课题，要解决好无线传感器网络中的通信安全问题，就必须全面、深入的考虑好节点的资源消耗问题、无线网络传输的拓扑结构形式、传感器节点的最大生存空间和时间、节点的抗毁性及自我修复等问题，也只有这样，才能设计出科学、合理且行之有效的无线WSN通信安全方案。

1.1.2 研究意义

无线传感器网络是集合了现代通信技术、网络技术、传感器技术和微电子系统技术等众多现代科技相结合的产物，可以通过非常灵活的方式或方法从所部署的环境区域中收集各种感应数据信息，从而形成一个分布式数据采集、处理和传输的网络系统，是一项既可以应用于实时监控又可以运用于有效侦察的高科技“隐形手段”，前景应用不可想象。除此之外，无线传感器网络的特点还促使其可以在任意时间、不同地点和复杂恶劣的环境条件下获取大量感知到的相关信息，可以广泛应用于军事科研、医疗保健、环境和交通监测、灾难救助、森林防火、候鸟迁徙及跟踪，甚至人体心脏监视等领域[8]。

随着无线传感器网络科技的进一步发展，应用范围的逐渐增广扩大，无线传感器网络节点的处理能力日趋增强，通过传感器收集、处理和传输的数据信息种类也越来越多，无论是军事科研的高保密通信，还是最为平常的商用或民用的数据信息处理，都迫切需要保证其数据传输、存储的高度安全性。如在商业应用上，居民小区内的无线安防网络；军事方面，在敌控区部署无线传感器网络，从而能够悄无声息的监视敌方的军事设施及战场布局[9]。

由于WSN网络节点的诸多特点，使它极易受到来自方方面面的攻击。在日常生活及实际的应用场景中，攻击者通常都会采取多种方法相结合的方式来进行攻

击，这使得无线传感器网络的安全防范变得难上加难。在众多的攻击案例中，攻击者不仅可以针对现有的无线传感器网络协议的缺陷和不足来达到攻击节点的目的，也可以使用相对传感器网络节点更为强大的设备进行全面攻击。因此，这就要求我们在无线传感器网络相关的研究和设计中，充分考虑其资源受限的问题和不足，提供出相对较为可靠的防御和检测算法，组建起一条相对安全的无线网络安全通信框架，从而最大限度的避免或降低由于节点被损坏或信息被窃取所造成的数据信息损失[10]。

另一方面，在其通信安全问题的分析、研究、实验和实现的过程中，无线传感器网络自身资源受限的窘况也带来了不少的难题，有一些甚至还属于学科前沿尚未取得成功的技术。如：能够在传统有线网络中广泛使用的Encryption/decryption机制、节点的authentication方法及attack和defense机制等，这一系列在有线网络中已经很成熟的技术却都是无法直接应用到当前的无线WSN网络中来的。究其本质上的原因，就在于在传统有线网络安全机制的部署中，传感器节点能源消耗的问题几乎可以忽略，节点计算和存储信息的时间和空间复杂度到底能有多大的问题也不会对网络结构的拓扑结构及实际部署有任何的影响。而在无线传感器网络中的情况则截然不同，这就要求研究者们必须设计出相对轻负载的加/解密算法、认证机制以及入侵检测算法，并设计出相应的安全密钥管理的策略及方案[11]。

如何在权衡资源负载和安全保障之后，编写出行之有效的安全算法，在节点资源受限、缺乏集中式管理、各节点高度依存且相互协作的无线WSN网络中来说，如何能够完成数据的及时获取和实时有效且安全的传输，是当前亟待解决的难点问题之一[12]。国内当前对无线WSN网络等问题的研究，其实还处于刚刚起步的理论和概念的初级研究阶段，探讨的范围也仅仅局限于部分的高校和研究所范围内。不过，作为一门正在逐步兴起且有望为人类生活提高质量的先进科学技术——无线传感器网络，对于国内和国际上所有国家的科技研究者而言，在其网络安全方面的研究和实践水平的差距也没多大。而随着我国基础科学的逐步发展，尖端科技方面所取得的一次又一次的突破，及时并广泛的展开这项对我们人类未来的生活有着深远影响的前沿科技的理论研究和科学实践，对我们整个发展中的国家的社会、经济发展以及国际政治地位的提高都将有着重大的战略意义。