Key Management for Heterogeneous Sensor Networks

异构传感器网络密钥管理

■ 马春光 著

国防工业出版社
National Defense Industry Press

异构传感器网络密钥管理

Key Management for Heterogeneous Sensor Networks

马春光 著

国防工业出版社

·北京·

图书在版编目(CIP)数据

异构传感器网络密钥管理/马春光著. —北京:国防工业出版社,2012.1

ISBN 978-7-118-07727-8

Ⅰ.①异… Ⅱ.①马… Ⅲ.①传感器—网络—密码—管理 Ⅳ.①TP212

中国版本图书馆 CIP 数据核字(2011)第 221550 号

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

国防工业出版社印刷厂印刷

新华书店经售

*

开本 850×1168 1/32 印张 7¾ 字数 165 千字

2012 年 1 月第 1 版第 1 次印刷 印数 1—4000 册 定价 36.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777 发行邮购:(010)88540776

发行传真:(010)88540755 发行业务:(010)88540717

致 读 者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分，又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展，加强社会主义物质文明和精神文明建设，培养优秀科技人才，确保国防科技优秀图书的出版，原国防科工委于1988年初决定每年拨出专款，设立国防科技图书出版基金，成立评审委员会，扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是：

1. 在国防科学技术领域中，学术水平高，内容有创见，在学科上居领先地位的基础科学理论图书；在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖，内容具体、实用，对国防科技和武器装备发展具有较大推动作用的专著；密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值，密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作，负责掌握出版基金的使用方向，评审受理的图书选题，决

定资助的图书选题和资助金额，以及决定中断或取消资助等。经评审给予资助的图书，由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就，积累和传播科技知识的使命。在改革开放的新形势下，原国防科工委率先设立出版基金，扶持出版科技图书，这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物，是对出版工作的一项改革。因而，评审工作需要不断地摸索、认真地总结和及时地改进，这样，才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金
评审委员会

国防科技图书出版基金
第六届评审委员会组成人员

前 言

2005 年,在我拿到北京邮电大学密码学博士学位到哈尔滨工程大学工作时,开始思考:我在科研方面应该做点什么? 如何将自己的专业特长在哈尔滨工程大学发挥出来? 这是一个关乎自己在科研上如何安身立命的问题。作为一名研究生导师,从被人指导到指导别人,这种角色的变换使我不得不思考:什么研究方向能令学生感兴趣? 什么研究方向可以让他们在毕业若干年后还能为当初的选择感到满意? 这是一名导师必须为学生考虑的问题。

我综合考虑自己的专业特长、研究兴趣、学校特色,脑海里浮现出几个关键词:密码学、信息安全、下一代网络、军工背景。我再将它们进行组合,一个研究方向兀立眼前:无线传感器网络安全。

2006 年,我的导师杨义先教授让我为《中国计算机学会通讯》"文明与野蛮的较量——信息系统安全"专辑写点东西,我选择了"无线传感器网络安全"这个题目。当时,我正和我的研究团队讨论实验室的定位问题,大家都认为无线传感器网络安全内涵丰富、应用广泛,既有科学问题,又有应用前景。我和我的第一个研究生查阅、总结、分析了国内外文献,完成了《无线传感器网络安全》一文,发表在 2006 年第 6 期的《中国计算机学会通讯》上,是国内比较早的关于传感器网络安全的综述。

完成综述后,我们发现:无线传感器网络安全涉及的知识领

域很多，要想在此研究领域有所作为，必须结合自身特点，由具体的问题开始，以点带面，争取突破。我从我的博士专业“密码学”入手，很自然想到了密钥管理。于是，决定从“无线传感器网络密钥管理”这个题目开始无线传感器网络安全的研究工作。恰逢此时，在哈尔滨举行第一届中国传感器网络学术会议（CWSN'07），我和我的研究生写的《无线传感器网络密钥管理问题研究综述》被会议录用，这是国内比较早的关于无线传感器网络密钥管理的综述。

密钥管理主要研究密钥的产生、分发、储存、更新、销毁等整个生命周期中的管理问题。在 Kerchhoff 假设下，作为唯一秘密的密钥的管理问题显然是任何密码系统安全性的核心。现代密码学的发展史也充分说明了这一点。1976 年，Diffie 和 Hellmen 在对对称密码密钥管理问题的研究过程中，提出了 DH 密钥协商协议，创造性地开辟了密码学研究的一个全新分支——公钥密码体制。1993 年，美国政府出于可直接侦听通信的目的，颁布了 EES 标准，提出了密钥托管（Key Escrow）政策，希望用这种办法加强政府对密码使用的调控管理。在传统的 Internet 上，有比较成熟的密钥管理机制，如基于 KDC（密钥分发中心）的对称密码密钥管理机制、基于 CA（数字证书）的公钥密码体制密钥管理机制。但因为传感器网络固有的一些特性，如节点资源受限、无固定基础设施、节点容易受损、部署环境复杂等，使这些密钥管理机制不能直接使用。

一直以来，大多数研究都假定“传感器网络是由资源受限节点通过自组织方式形成的同构网络”。我们认为，这种狭义的同构性假设制约了本领域研究者学术思想的创新，限制了许多新技术的应用，也将影响传感器网络的应用。具体到密钥管理问题，这种假设限制了诸如公钥密码、层次化密钥管理模型、可信计算

等密码学和信息安全的理论与技术在传感器网络中的应用。在很多应用场景，传感器网络的节点是可以有、也应该有差别的。网络本身，无论是数据链路层、网络层、传输层、应用层，也是有差别的。我们以为，异构性是传感器网络的自然属性，特别是当传感器网络作为物联网感知层而存在时，这种异构特性更为突出。

本书从传感器网络的异构性出发，比较全面、系统地论述了异构传感器网络密钥管理的关键理论和技术问题，主要内容包括：异构传感器网络相关概念、异构性、密钥管理模型、静态密钥管理协议、动态密钥管理协议、基于公钥的密钥管理协议等。

全书共6章，每章都包含了作者近年的科研成果。第1章主要对异构传感器网络、异构传感器网络安全问题、异构传感器网络密钥管理协议的分类评测标准等基础知识做简要阐述。第2章从节点异构性、链路异构性、协议异构性等多个维度，细粒度地刻画了传感器网络的异构性问题，并综合这些异构特性，给出了一种异构传感器网络代价最小模型。第3章针对异构传感器网络的异构特性和网络攻击类型，首先给出一种异构传感器网络密钥管理框架，然后分别设计了一种静态密钥管理模型和一种动态密钥管理模型，最后给出了一套用于密钥管理模型评测的指标体系。第4章在第3章提出的静态密钥管理模型的基础上，给出了3种具有代表性的密钥管理协议，即基于组合设计的密钥管理协议、基于部署知识的密钥管理协议和基于密钥原材料的密钥管理协议。第5章在第3章提出的动态密钥管理模型的基础上，针对不同的攻击类型，针对态密钥管理侧重的密钥恢复、密钥更新、密钥重建等，提出了3种不同的密钥管理协议——可抵御串谋攻击的密钥管理协议、可认证的会话密钥管理协议和可认证的广播密钥管理协议。第6章对公钥密码体制在异构传感器网络密钥管理中的应用进行了评述，并且给出了一个基于身份密码体制的可

认证密钥协商协议，给出了一个基于属性密码体制的可认证密钥协商协议。

本书是哈尔滨工程大学网络与信息安全研究团队（http://machunguang.hrbeu.edu.cn）多年研究成果的结晶。本书是网络与交换技术国家重点实验室（北京邮电大学）开放课题（编号：SKLNST－2009－1－10）、国家博士后科学基金（编号：20070410896）、黑龙江省政府博士后资助经费项目（编号：LBH－Z06027）、黑龙江省博士后科研启动基金部分研究成果的总结。本书的编写得到了国家自然科学基金（编号：60973027、61073042、61170241）的支持。在写作过程中，博士生王九如、钟晓睿、付小晶，硕士生武朋、楚振江、戴膺赞等提供了丰富的资料并做了非常细致的整理和编辑工作。感谢哈尔滨工程大学王慧强教授、张国印教授、黄少斌教授，三位教授亦师亦友，对本书的研究工作给予了很多支持。特别感谢北京邮电大学杨义先教授、温巧燕教授，北京航空航天大学刘建伟教授，南开大学贾春福教授，他们审阅了本书的目录和部分初稿，提出了宝贵的意见。还要感谢国防工业出版社王京涛编辑在本书的立项、撰写、出版过程中给予的支持和帮助。

限于作者水平，书中难免有疏漏和不当之处，希望大家批评指正，欢迎通过电子邮件（machunguang@hrbeu.edu.cn）与我联系。

希望本书能为推进我国传感网和物联网的安全研究尽微薄之力。

目　录

Contents