国防科技图书出版基金

“十二五”国家重点出版规划项目

密码学与信息安全技术丛书

异构传感网密钥管理框架模型及协议

马春光 王九如 袁 琪 编著

Framwork, Model, and Protocols of Key Management for Heterogeneous Sensor Networks

国防工业出版社
National Defense Industry Press

国防科技图书出版基金

“十二五”国家重点出版规划项目
密码学与信息安全技术丛书

Framework, Model, and Protocols of Key Management for Heterogeneous Sensor Networks

异构传感网密钥管理框架模型及协议

马春光　王九如　袁　琪　编著

国防工业出版社
·北京·

图书在版编目（CIP）数据

异构传感网密钥管理框架模型及协议／马春光，王九如，袁琪编著. —北京：国防工业出版社，2015.12
（密码学与信息安全技术丛书）
ISBN 978-7-118-10702-9

Ⅰ. ①异… Ⅱ. ①马… ②王… ③袁… Ⅲ. ①传感器—密码—管理 Ⅳ. ①TP212

中国版本图书馆 CIP 数据核字（2015）第 304019 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）
腾飞印务有限公司印刷
新华书店经售

*

开本 710×1000　1/16　**印张** 13¼　**字数** 234 千字
2015 年 12 月第 1 版第 1 次印刷　**印数** 1—2000 册　**定价** 78.00 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
第七届评审委员会组成人员

主任委员	潘银喜			
副主任委员	吴有生	傅兴男	赵伯桥	
秘书长	赵伯桥			
副秘书长	邢海鹰	谢晓阳		
委员	才鸿年	马伟明	王小谟	王群书
（按姓氏笔画排序）	甘茂治	甘晓华	卢秉恒	巩水利
	刘泽金	孙秀冬	芮筱亭	李言荣
	李德仁	李德毅	杨　伟	肖志力
	吴宏鑫	张文栋	张信威	陆　军
	陈良惠	房建成	赵万生	赵凤起
	郭云飞	唐志共	陶西平	韩祖南
	傅惠民	魏炳波		

《密码学与信息安全技术丛书》编写委员会

前　言

2005 年，我们决定进行传感网密钥管理方面的研究，并投入当时几乎所有的研究力量开展相关工作。2011 年，我们申请的“异构传感器网络密钥管理机制研究”项目获得国家自然科学基金资助。2012 年，在国防科技图书出版基金资助下，我们的学术著作《异构传感器网络密钥管理》由国防工业出版社出版，这是我们阶段性研究成果的一次集中体现。

2012 年，我们开始重新审视传感网密钥管理这个“老”问题，力图找到“新”方法。经过多次讨论，我们决定从传感网异构性刻画方法入手，通过框架、模型、协议三个不同的层面，从宏观到微观，系统性地解决密钥管理这个传感网安全的首要问题。经过多年的持续研究，我们系统分析了各种异构因素对传感网密钥管理的影响，给出了一个通用的异构传感网密钥管理框架，构建了一个可形式化描述的异构传感网密钥管理策略模型，设计了若干基于不同方法和技术的异构传感网密钥管理协议，并对其性能和安全性进行了理论分析和仿真测试。

2014 年，在与国防工业出版社编辑的交流中，我谈到想将这些研究工作编撰成书的想法，得到了认同，并建议我们申请国防科技图书出版基金，我们欣然命笔。2015 年，我们得到批复，这本《异构传感网密钥管理框架、模型和协议》获得了国防科技图书出版基金的资助。本书是我们多年来在传感网密钥管理方面研究成果的一次系统性呈现。与 2012 年版《异构传感器网络密钥管理》相比较，本书对传感网异构性有了更明确的定义和刻画，对密钥管理管理框架和模型有了更形式化的描述，对密钥管理协议有了更客观的评价方法，所设计的密钥管理协议也更加广泛、更有针对性。

本书共 6 章内容，第 1 章概述，主要对异构无线传感器网络的异构性进行了定义和分类，并对传感网异构性进行了多维度细粒度的刻画。第 2 章密钥管理框架与模型，介绍了异构传感网密钥管理协议的评价指标，给出了一个通用的异构传感网密钥管理框架，对密钥管理策略模型进行了形式化，并给出了模型实例以及对其的求解和分析。第 3 章对称密钥管理协议，给出了三种基于对称密码技术的密钥管理协议，即，基于扰动技术的抗 LU 攻击的密钥管理协议、体现跨层设计思想的基于 E－G 的跨层密钥管理协议、利用网络动态异构性的

多阶段能量有效的密钥预分配协议。第4章基于单向累加器的密钥管理协议，从单向累加器可进行集合成员关系证明这一事实出发，给出了基于单向累加器的密钥管理协议、基于快速单向累加器的密钥管理协议、基于动态累加器的认证组密钥管理协议。第5章非对称密钥管理协议，通过节点身份信息的引入，给出了基于身份的密钥管理协议、基于多域身份基加密的密钥管理协议、基于属性的组密钥管理协议。第6章可认证密钥协商协议，面向异构传感网不同的应用场景，给出了适用于无线传感反应网络的基于身份可认证密钥协商协议、适用于多基站异构传感网的标准模型下安全的基于身份密钥协商协议。

本书是哈尔滨工程大学网络与信息安全研究团队（NSR@ HEU，http://machunguang. hrbeu. edu. cn）在传感网密钥管理方面多年研究成果的结晶，我的很多博士生、硕士生都付出了辛勤的工作，他们有的已经毕业，并在各自的工作岗位上崭露头角，有的正踏着师兄师姐的足迹，冒着哈尔滨的漫天飞雪，继续在传感网和物联网的研究领域里无悔前行。本书的第二作者王九如博士，常年从事传感网密钥管理方面的研究，是我们团队首个毕业的博士研究生，在本书的编撰和出版过程中，做了大量细致高效的工作。本书的第三作者袁琪博士，是我们团队现在进行传感网密钥管理研究的在读博士生，做了大量诸如本书申请立项等前期工作。感谢我们团队已毕业的博士研究生钟晓睿、付小晶，以及已毕业的硕士研究生尚志国、耿贵宁、张秉政、孙瑞华、于洪君、林相君、楚振江、戴膺赞、李蕾，他（她）们的学位论文和研究成果是本书素材的重要来源。感谢国防科技图书出版基金评审专家对本书所提的建议和意见。特别感谢杜均编辑在本书的立项、撰写和出版过程中给予的支持和帮助。

本书的编写得到了国家自然科学基金（61170241、61472097）、黑龙江省自然科学基金（F201229）、高等学校博士学科点专项科研基金资助课题（博导类）（20132304110017）、山东省自然科学基金（ZR2014FL012）、山东省科技发展计划（2013YD08002）研究成果的支持。

由于作者水平有限，书中难免出现各种疏漏和不当之处，殷切希望大家批评指正。您的任何建议、意见和批评，都是对我们和本书最大的支持，欢迎随时通过电子邮件（machunguang@ hrbeu. edu. cn）与我联系。

希望本书的出版能为推进我国传感网和物联网的安全研究尽微薄之力。

马春光

2015 年 11 月 26 日于哈尔滨工程大学

目　录

Contents