博弈论与无线传感器网络安全

GAME THEORY
MEETS WIRELESS SENSOR
NETWORKS SECURITY

沈士根 刘建华 曹奇英 著

清华大学出版社

博弈论与
无线传感器网络安全

GAME THEORY
MEETS WIRELESS SENSOR NETWORKS SECURITY

沈士根 刘建华 曹奇英 著

清华大学出版社
北京

内 容 简 介

本书以博弈论为理论分析工具，主要论述和分析无线传感器网络安全领域的若干关键问题。第1章介绍研究背景；第2章概述相关的博弈类型；第3章给出基于信号博弈的无线传感器网络入侵检测模型，确定何时启动入侵检测系统的最优策略；第4章描述基于演化博弈的无线传感器网络节点的信任模型，阐明节点信任演化动力学规律；第5章基于微分博弈给出无线传感器网络恶意程序传播的最优控制策略；第6章基于随机博弈和Markov链建立受攻击无线传感器网络可生存性模型，形成可生存性分析的理论和方法；第7章针对受攻击协调器节点，给出基于随机博弈的防御技术，再利用演化博弈实现协调器节点的选择；第8章阐述传感云数据外包中心访问控制系统的安全分析框架，给出基于证书认证博弈的安全优化策略；第9章基于随机演化联盟博弈给出受攻击虚拟传感云服务系统的自适应防御策略；第10章介绍无线传感器网络物理层安全技术，基于演化博弈中的复制动力学方程实现一种传感器节点保密率自适应调节的方法。

本书可作为高等院校、科研院所等从事网络安全、博弈论应用等研究人员的参考书。

图书在版编目(CIP)数据

博弈论与无线传感器网络安全/沈士根，刘建华，曹奇英著. —北京：清华大学出版社，2016
ISBN 978-7-302-41906-8

Ⅰ. ①博… Ⅱ. ①沈… ②刘… ③曹… Ⅲ. ①博弈论－应用－无线电通信－传感器－安全管理－研究 Ⅳ. ①TP212

中国版本图书馆CIP数据核字(2015)第259856号

责任编辑：闫红梅　赵晓宁
封面设计：常雪影
责任校对：梁　毅
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954
印 刷 者：三河市君旺印务有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：13　　**字　数**：323千字
版　　次：2016年3月第1版　　**印　次**：2016年3月第1次印刷
印　　数：1～1000
定　　价：39.00元

产品编号：066929-01

前言

FOREWORD

无线传感器网络(Wireless Sensor Networks)由大量部署在监测区域内的廉价微型传感器节点组成,通过无线网络通信传输方式形成一个自组织、自适应、多跳的智能网络系统,其目的是协作地实时监测、感知和采集各种环境或监测对象的信息(如温度、湿度、气压等),再通过基站发送给管理者。当前,其在工农业、城市管理、生物医疗、环境监测、军事等众多领域已被公认具有十分广阔的应用前景。

无线传感器网络作为一种任务型网络,不仅要进行数据的传输,而且要进行数据融合、任务的协同控制等。如何保证任务执行的机密性、数据产生的可靠性以及数据传输的安全性,就成为无线传感器网络安全需要全面考虑的内容。可以说,安全问题是制约无线传感器网络发展和应用的一个关键因素。

博弈论是研究两个或多个参与者谋略和决策问题的理论,能为无线传感器网络安全的研究提供新颖的思路。无线传感器网络具有自组织、无控制中心、动态拓扑、资源有限等主要特点,这些特点决定了每个节点在通信时都会有自己的决策。那么,当节点需要做出决策时,哪一种是最优的?节点也许会表现自私而寻求只对自身有益的决策,甚至会表现恶意而选择破坏网络性能的决策。利用非合作博弈对这些情况进行研究能找到很好的答案。当然,这里的非合作博弈包括了多种形式,如信号博弈、随机博弈、微分博弈等。另外,还可以选择演化博弈对节点行为的动态演化进行研究。

本书以博弈论为理论分析工具,主要分析和解决无线传感器网络安全领域的若干关键问题。

第1章从无线传感器网络安全的需求出发,说明博弈论与无线传感器网络安全之间的相互关系。

第2章给出博弈论的基本概念,介绍适合不同情况的博弈类型,为后续章节博弈论的应用和相关工作的比较提供知识准备。

第3章应用信号博弈描述并分析恶意传感器节点和无线传感器网络入侵检测系统之间的交互过程。在每个独立的阶段,建立"阶段入侵检测博弈"模型,分别得到该模型的纯策略贝叶斯均衡和混合策略贝叶斯均衡。随着博弈的重复,通过构建"多阶段动态入侵检测博弈"来反映恶意传感器节点和入侵检测代理之间的交互活动,得到相应的完美贝叶斯均衡,再在此基础上实现入侵检测启动最优策略的机制和算法。

第4章利用演化博弈研究和分析传感器节点间的信任决策过程,根据各个传感器节点能选择不同策略的实际情况建立"无线传感器网络信任博弈"模型,通过整合激励机制参数来说明激励机制对传感器节点选择动作的影响,使用复制动态动力学方程探索博弈模型的

演化稳定策略，从而揭示无线传感器网络中各传感器节点间的信任演化原理。

第5章扩展经典流行病理论使之适合无线传感器网络恶意程序传播现状，并引入不同的参数来揭示无线传感器网络恶意程序传播过程。然后将恶意程序在无线传感器网络传播时“无线传感器网络系统”和“恶意程序”之间的决策交互过程看作优化控制问题，建立相应的微分博弈模型，在“恶意程序”动态改变其策略的前提下，得到“无线传感器网络系统”的最优控制策略，为控制无线传感器网络恶意程序传播的机制设计提供理论基础。

第6章从可靠度和可用度两方面评估受攻击无线传感器网络的可生存性属性。由于恶意攻击者总是故意发动恶意攻击行为，通过随机博弈给出这些理性恶意攻击者采取恶意攻击的期望概率，将聚簇无线传感器网络看作一个串—并系统，再利用连续时间马尔可夫链对受攻击传感器节点生命期的所有状态建立模型，基于可靠性理论得到计算受攻击传感器节点平均无故障时间、可靠度、生存期和稳态可用度的计算公式，实现受攻击无线传感器网络的可生存性评估。

第7章以最小化从源到目的节点的数据包分发平均跳数并且延长网络生命期为目标，提出了基于博弈论和模糊逻辑的协调器节点选择算法。在此算法中，先使用随机博弈对攻击进行动态响应，然后通过模糊逻辑选择通信质量较好的节点作为协调器节点，提高网络的服务质量和安全性。

第8章阐述了基于动态证书博弈的认证系统框架。在证书认证博弈交互过程中，通过认证代理补偿一定的信任度来激励传感云用户出示更多的证书，以提高其信任度。传感云用户和认证协调器通过平衡证书泄露和信任补偿之间的关系来决定是否用户能够操作外包数据。其中，认证协调器决定每次博弈信任度，认证代理决定信任度分配，再将动态证书博弈系统框架模型化为三阶段博弈，并使用迭代博弈学习方法证明信任协同的稳定性。与传统的基于属性和本体的访问控制系统相比，基于动态证书博弈的认证系统框架提高了安全效用和认证性能。

第9章提出了基于随机演化联盟博弈框架的受攻击虚拟传感云服务系统安全机制。在博弈的每一阶段，虚拟传感云服务提供者能够观察到服务组合节点的虚拟容量和攻击者采取的攻击策略，根据这些观察，决定需分配的虚拟容量值来保证可靠安全的服务组合。虚拟传感云服务提供者通过 minimax-Q 和演化联盟形成算法，自适应地变化防御策略，形成可靠安全的服务组合对攻击者进行动态防御。与随机博弈和演化联盟博弈相比，随机演化联盟博弈框架在动态虚拟的安全服务组合过程中获得了较好的性能。

第10章通过扩展经典窃听信道模型，针对聚簇无线传感器网络提出了传感器节点和其对应簇头节点之间的保密率计算方法，构建了一个非合作保密率博弈模型，以反映传感器节点之间的交互关系。利用演化博弈思想，建立了传感器节点自适应选择发射功率的机制，提出了传感器节点保密率的自适应调节算法，为保证无线传感器网络数据的保密性提供了新途径。

本书是作者多年研究博弈论和无线传感器网络安全的成果，其中，沈士根教授负责撰写第1～6章和第10章，刘建华博士负责撰写第7～9章，曹奇英教授负责统稿及理论指导。

作者的研究工作得到了国家自然科学基金项目(61272034,61572014)、浙江省自然科学基金项目(LY16F020028)、中央财政《无线 Mesh 网络若干关键技术研究创新团队建设项目》等项目的资助。在本书的撰写过程中,绍兴文理学院机械与电气工程学院、嘉兴学院数理与信息工程学院、东华大学计算机科学与技术学院给予了大力支持,在此一并表示感谢。

由于作者水平所限,加之博弈论在网络安全中的应用研究处于不断发展和变化之中,书中错误和不足之处在所难免,恳请专家、读者予以指正。

作 者

2015 年 8 月

目录

CONTENTS

第 1 章

绪　论

本章从无线传感器网络的研究背景和无线传感器网络安全的需求出发，说明博弈论与无线传感器网络安全之间的关系，给出本书的组织结构。

1.1　研究背景

微电子技术、计算技术和无线网络通信等技术的发展，促进了低功耗多种类传感器的快速发展，使其在微小体积内能够实现信息收集、数据计算和无线网络传输等多种功能。无线传感器网络(Wireless Sensor Networks)就是由大量部署在监测区域内的廉价微型传感器节点组成的，通过无线网络传输方式形成的一个多跳的自组织、自适应的智能网络系统，其功能是合作地感知、收集并处理网络覆盖区域中各类对象(如温度、湿度、气压等)的信息，再发送给管理者。因此，组成一个传感器网络的 3 个主要要素是传感器节点、感知对象和管理者。如果说因特网构成了逻辑上的信息世界，改变了人与人之间的沟通方式，那么，无线传感器网络就是将客观上的物理世界与逻辑上的信息世界融合在一起，改变人类与自然界的交互方式。人们可以通过无线传感器网络直接感知物理世界中各类对象信息，从而极大地扩展现有网络的功能和人类认识物理世界的能力。美国商业周刊和 MIT 技术评论在预测未来技术发展的报告中，分别将无线传感器网络列为 21 世纪最有影响力的 21 项技术和改变世界的十大技术之一[1]。研究结果[2-5]表明，无线传感器网络具有十分广阔的应用前景，在工农业、城市管理、生物医疗、环境监测、军事等众多领域都有实际与潜在的实用价值。

无线传感器网络经历了一个长期的发展过程。在 20 世纪 70 年代，出现的第一代传感器网络主要利用点对点传输技术以及专门的控制器将传统的传感器连接起来，从而形成了无线传感器网络的雏形。随后，电子、计算机等学科的不断发展和进步，使传感器网络也具备了获取多种对象信息的综合处理能力，并采用串/并接口与传感控制器相连，构成了具有信息收集和综合处理能力的第二代传感器网络。第三代传感器网络形成于 20 世纪 90 年代后期和 21 世纪初，开始采用能够智能获取多种对象信息信号的传感器，通过现场总线连接传感控制器，形成局部智能化传感器网络。第四代传感器网络是目前科研工作者的研究热点之一，该网络采用大量具有多功能、多对象信号获取能力的传感器，尤其重要的变化是传感器之间采用可靠的无线网络传输协议进行连接，从而形成高效、健壮的无线传感器网络，这是传感器网络发展的一个巨大飞跃[6]。这将使传感器网络进一步发展，应用范围得到极大的扩展。

从科研的角度来看，无线传感器网络的研究起始于20世纪90年代末期。自1999年将中间件(Middleware)技术引入无线传感器网络中之后，就有很多科研院所开始从不同的侧面进行研究。那时，大多数开展的基于无线传感器网络特性的中间件研究和开发工作都主要集中在如何延长传感器网络的生命期以及如何充分提高传感器网络的有限资源利用等方面。在美国，康奈尔大学、加州大学伯克利分校等是较早开始无线传感器网络基础理论和关键技术研究的高校。此后，大家都认识到无线传感器网络具有巨大的实际应用价值，世界许多国家的军事部门、工业界和学术界都对这种网络表现出极大的关注。美国自然科学基金委员会(US National Science Foundation)于2003年制订了无线传感器网络的研究计划，大力支持无线传感器网络基础理论和关键技术的研究。由于无线传感器网络潜在的军事用途，美国国防部(US Department of Defense)对此也高度重视，把无线传感器网络作为一个重要的研究领域，设立了一系列的项目从事军事传感器网络的研究；美国英特尔(Intel)公司、微软(Microsoft)公司等信息业巨头也开始了无线传感器网络方面的研究工作；其他如意大利、俄罗斯、法国、日本、英国、德国等科技发达国家也对无线传感器网络表现出了极大的兴趣，纷纷展开了相关的科学研究工作[7]。

我国的中国科学院上海微系统研究所、计算所、软件研究所、沈阳自动化所、电子所和合肥智能技术研究所等科研机构，清华大学、北京大学、哈尔滨工业大学、西北工业大学、北京邮电大学、南京邮电大学、国防科技大学等高等院校在国内较早开展了传感器网络的研究，之后有更多的科研院所加入到无线传感器网络的基础研究和开发工作中来。

通常，典型的无线传感器网络包括传感器节点(Sensor Node)、汇聚节点(Sink Node)和管理节点[5]。大量的传感器节点以随机撒播的方式部署在监测区域内部或附近，能够通过自组织的方式互联成网络。各类传感器节点监测到的数据信息沿着其他传感器节点(如簇头)逐跳地进行传输，并在传输过程中不同节点的监测数据信息可能被多个节点进行处理，再经过多跳后传递到汇聚节点，最后通过互联网传输到管理节点。管理者可通过管理节点对传感器网络进行管理和配置，收集监测数据和发布监测信息等任务[8,9]。

但由于无线传感器网络感知、收集和传输数据的性能受到环境和节点自身特点的约束，在实际应用中存在诸多不足之处，主要体现在以下几个方面。

1. 电源能量有限

传感器节点体积微小，通常携带能量十分有限的电池[10]。这些能量主要被传感器模块、处理器模块和无线通信模块等消耗。随着集成电路工艺的发展，传感器和处理器模块的功率消耗将会变得越来越低，绝大部分能量消耗在无线通信模块上。其中，无线通信模块具有接收、发送、睡眠、空闲4种状态。空闲状态意味着无线通信模块一直在监听无线信道的状况，检查是否有数据信息发送过来，而睡眠状态则意味着关闭无线通信模块。相比较而言，无线通信模块在数据发送时能量消耗最大，空闲时少于发送状态的能量消耗，而处于睡眠状态时能量消耗最少[1]。由于一个无线传感器网络中的传感器节点个数多、分布区域广，而且部署环境复杂，有些部署区域甚至人员都不能到达，所以通过更换电池的方式来补充能源往往不现实。这就对科研工作者提出了无线传感器网络多方面节能的需求。

2. 通信能力有限

传感器节点能量有限的现状决定了它有限的通信能力。无线网络通信的能耗与通信距离的关系密切，随着通信距离的增加，能量消耗将成倍增加。考虑到传感器节点网络覆盖区

域大的特点，无线传感器网络通常采用多跳路由传输机制。这就要求在满足无线传感器网络通信连通度的前提下应尽量减少单跳通信距离。另外，由于节点能量的不断变化，受障碍物等自然环境的影响，无线网络通信性能会经常变化，导致通信中断[1]。这就对科研工作者提出了多方面减少数据通信的需求。

3. 计算和存储能力有限

作为一种微型嵌入式设备，传感器节点价格低、功耗小，这些限制必然导致其配备的微处理器能力比较弱，存储器容量比较小。而传感器节点需要完成监测数据的采集和转换、数据的管理和处理、应答汇聚节点的任务请求和节点控制等多种工作[1]。为了完成各种任务，这就对科研工作者提出了多方面减少数据计算和存储的需求。

因此，目前针对无线传感器网络的大量科研工作都是为了解决上述的不足进行展开。

实际上，无线传感器网络作为任务型的网络，不仅要进行数据的传输，而且要进行数据采集和融合、任务的协同控制等。如何保证任务执行的机密性、数据产生的可靠性、数据融合的高效性以及数据传输的安全性，就成为无线传感器网络安全需要全面考虑的内容。可以说，安全问题是制约无线传感器网络发展的一个非常关键因素[11-14]。

博弈论是研究两个或多个参与者谋略和决策问题的理论[15]，在我国古代故事如王戎辩李、孙膑赛马、破釜沉舟、空城计等中就充满了博弈论的思想。博弈论分析的目的是预测博弈的结果。不言而喻，每一个参与者要选择的策略必须是针对其他参与者选择战略的最优反应，每一个参与者都希望尽可能提高自己的利益所得[16]。因此，博弈论研究强调决策主体行为发生时的直接相互作用。例如，经常遇到的性别战博弈，这是一个两人决策问题，丈夫的决策依赖于妻子的决策；反过来，妻子的决策也依赖于丈夫的决策。

1944 年，John Von Neumann 和 Oskar Morgenstern 的巨著 *Theory of Games and Economic Behavior* 的出版为博弈论在经济学中系统的应用奠定了理论基础。1994 年、1996 年、2001 年、2005 年和 2007 年共 5 次诺贝尔经济学奖被分别授予了经济博弈论方向的学者。对一门学科给予如此高的褒奖，表明了博弈论的强大威力。正是国际经济学界对博弈论的这种肯定，推动了国内外博弈论研究及应用的发展，使得目前的博弈论已发展成一个内容丰富且完善的理论体系。更重要的是，博弈论的应用已逐步扩展到政治学、道德哲学、社会学、生物学和计算机科学等领域。

博弈论的应用需要根据不同的场合选择不同的博弈类型，本书主要利用非合作博弈、演化博弈、联盟博弈研究无线传感器网络安全中的若干关键问题。非合作博弈的核心问题是参与者的策略选择，即在参与人是完全理性的基础上研究参与者在利益相互影响的情况下选择最有利于自己的策略[17]。演化博弈建立在参与人是有限理性的基础上，以参与人种群为研究对象，认为参与人的行为是一个动态调整过程[18]。联盟博弈强调在联盟的内部建立信息的互通，以及具有约束力且可执行的契约。因此，非合作博弈适用于参与人存在竞争且需要探寻只对自身有利策略的场合，演化博弈适用于需要对参与人行为动态演化进行研究的场合，而联盟博弈适用于联盟是否可获得收益，以及获得的净收益如何在联盟内部公平分配的问题。

近些年来，在无线网络领域，包括 Ad Hoc 网络、Mesh 网络、无线传感器网络等，博弈论的应用呈明显上升的趋势。研究涉及的内容包括无线传感器网络媒体接入控制、无线传感器网络安全路由、无线传感器网络 MAC 协议竞争接入控制、认知 MIMO 系统功率分配、毫

微微蜂窝混合接入控制干扰管理、高速移动环境下快速动态无线资源优化、无线自组织网络用户合作激励、认知无线网络动态频谱拍卖、认知无线网络资源分配、智能绿色无线电资源分配、认知无线电动态频谱分配等。

国内外一些著名研究机构和学术团队都在致力于博弈论和无线网络相结合的研究，如中国科学院软件研究所信息安全国家重点实验室、上海交通大学系统控制与信息处理教育部重点实验室、东北大学计算机软件与理论研究所、华东交通大学智能传感器网络中心和网络与信息安全中心、武汉理工大学高性能网络研究中心、四川大学计算机网络与安全研究所、西安电子科技大学智能感知与图像理解实验室、哈尔滨工业大学通信技术研究所、美国佐治亚理工学院宽带无线网络实验室、美国马里兰大学 K. J. Ray Liu 团队、美国加州大学 Mihaela van der Schaar 团队、美国伊利诺大学 Tamer Başar 团队、美国范德堡大学 Myrna Wooders 团队、加拿大曼尼托巴大学 Ekram Hossain 团队、希腊西马其顿大学 Athanasios V. Vasilakos 团队等。与此同时，从近几年的网络通信领域顶级国际会议 SIGCOMM、INFOCOM 和 MobiHoc 上发表的论文可见，每年都有相关文献发表。通信领域国际顶级期刊 *IEEE Journal on Selected Areas in Communications* 在 2011 年的征稿中共有两次主要关注博弈论和无线网络相结合的主题，分别是 Game Theory in Wireless Communications 和 Economics of Communication Networks and Systems。

事实上，博弈论为无线传感器网络安全的研究提供了新颖的思路。自组织、无控制中心、动态拓扑、资源有限是无线传感器网络的主要特点，这些特点决定了每一个节点在通信时会有自己的决策。那么，当节点需要做出决策时，哪一种是最优的？节点也许会表现自私而寻求只对自身有益的决策，甚至会表现恶意而选择破坏网络性能的决策。这些情况利用非合作博弈能找到很好的答案。当然，这里的非合作博弈包括了多种形式，如重复博弈、信号博弈、声明博弈、随机博弈等。另外，还可以选择演化博弈对节点行为的动态演化进行研究。因此，博弈论方法为无线传感器网络安全中多方面关键问题研究提供了可行的新思路和新技术，这是一个重要的充满前景的研究方向。

1.2 本书组织结构

本书总共包含 10 章，分别是“第 1 章 绪论”、“第 2 章 博弈论概述”、“第 3 章 基于信号博弈的无线传感器网络入侵检测最优策略研究”、“第 4 章 基于演化博弈的无线传感器网络节点信任演化动力学研究”、“第 5 章 基于微分博弈的无线传感器网络恶意程序传播机制研究”、“第 6 章 基于随机博弈的受攻击无线传感器网络可生存性评估研究”、“第 7 章 无线传感器网络受攻击协调器节点的防御响应博弈机制研究”、“第 8 章 面向传感云数据外包中心的信任演化机制研究”、“第 9 章 基于随机演化联盟博弈的虚拟传感云服务安全机制研究”、“第 10 章 基于演化博弈的传感器节点保密率自适应调节研究”。

第 1 章由无线传感器网络的研究背景和无线传感器网络安全的需求，说明博弈论与无线传感器网络安全之间的关系。

第 2 章概要介绍了博弈论的基本概念、博弈类型等。通过对完全信息静态博弈、完全且完美信息动态博弈、重复博弈、不完全信息静态博弈、完全但不完美信息动态博弈、不完全信息动态博弈、合作博弈、信号博弈、演化博弈、微分博弈、随机博弈、联盟博弈等博弈类型的说

明和分析，初步了解博弈论，为后续章节博弈论的应用和相关工作的比较提供知识准备。

第3章应用信号博弈描述并分析恶意传感器节点和无线传感器网络入侵检测系统之间的交互过程。在每个独立的阶段，建立“阶段入侵检测博弈”(Stage Intrusion Detection Game)模型，探索该博弈模型纳什均衡存在的条件，并将分别得到纯策略贝叶斯均衡(Pure-strategy Beyasian Equilibrium)和混合策略贝叶斯均衡(Mixed-strategy Beyasian Equilibrium)。随着博弈的进行，通过构建“多阶段动态入侵检测博弈”(Multi-stage Dynamic Intrusion Detection Game)来反映恶意传感器节点和入侵检测代理之间的交互活动。另外，在得到“多阶段动态入侵检测博弈”的完美贝叶斯均衡的基础上，设计入侵检测运行机制和相应的算法。

第4章利用演化博弈研究传感器节点间的信任决策过程，从而揭示无线传感器网络各传感器节点间的信任演化原理。根据各个传感器节点能选择不同策略的实际情况建立“无线传感器网络信任博弈”模型，并且为了研究激励机制对传感器节点选择动作“信任”(即可以合作通信)的影响，在“无线传感器网络信任博弈”模型中整合激励机制参数。为了说明“无线传感器网络信任博弈”模型的稳定性，通过复制动态动力学方程探索“无线传感器网络信任博弈”的演化稳定策略。

第5章扩展经典流行病理论使之适合无线传感器网络恶意程序传播现状，并引入不同的参数来揭示无线传感器网络恶意程序传播过程。然后将恶意程序在无线传感器网络传播时“无线传感器网络系统”和“恶意程序”之间的决策问题看作优化控制问题，并利用微分博弈为“无线传感器网络系统”得到最优控制策略，这种策略将在考虑“恶意程序”最大化破坏无线传感器网络的前提下，最小化“无线传感器网络系统”和“恶意程序”产生的成本。

第6章从可靠度和可用度两方面评估受攻击无线传感器网络的可生存性属性。首先将选择研究的聚簇无线传感器网络看作一个串-并(Serial-parallel)系统，这样就可以应用经典可靠性理论中已有的结论。因为恶意攻击者总是故意发动恶意攻击行为，通过随机博弈给出这些理性恶意攻击者采取恶意攻击的期望概率，再利用连续时间马尔可夫链对受攻击传感器节点生命期的所有状态建立模型，就可得到计算受攻击传感器节点平均无故障时间、可靠度、生存期(Survival Lifetime)和稳态可用度的计算公式，实现受攻击无线传感器网络的可生存性评估。

第7章针对受攻击的ZigBee无线传感器网络，为了最小化从源到目的节点数据包分发的平均跳数并且最大化延长网络生命期，提出了基于博弈论和模糊逻辑的协调器节点选择算法。协调器节点选择算法不仅要考虑数据包分发延迟、网络生命期，而且还要考虑网络攻击防御策略，因此在提出的算法中，首先使用随机博弈对攻击进行动态响应，然后通过模糊逻辑选择服务质量较好的节点作为协调器节点，从而提高网络的服务质量和安全性。

第8章阐述了基于证书认证的信任演化博弈模型及其系统框架。在“证书认证信任演化博弈”交互过程中，通过认证代理补偿一定的信任度来激励传感云用户披露更多的证书，以提高其信任度。传感云用户和认证协调器通过平衡证书泄露和信任补偿之间的关系来决定用户是否能够执行外包数据访问操作，认证代理根据用户披露的证书决定信任度的分配，并使用多轮迭代博弈效用分析法分析了“证书认证信任演化博弈”的稳定性。与传统的基于属性和本体的访问控制系统相比，基于证书认证的信任演化博弈模型及其系统框架提高了安全效用和认证性能。

第 9 章提出了基于随机演化联盟博弈的受攻击虚拟传感云服务系统安全机制。在随机演化联盟博弈的每一阶段，虚拟传感云服务提供者能够观察到服务组合节点的虚拟容量和攻击者的策略，根据这些观察，决定需分配的虚拟容量值来提高虚拟传感云服务组合的服务质量。虚拟传感云服务提供者通过 minimax-Q 和演化联盟形成算法，自适应地变化其防御策略并形成可靠安全的服务组合联盟，从而对攻击者的攻击进行动态防御来提高虚拟传感云服务的安全性和可靠性。与随机博弈和演化联盟博弈相比，随机演化联盟博弈框架在虚拟传感云服务动态组合过程中获得了较好的性能。

第 10 章以最大化网络效用为目标，利用演化博弈论中的复制动力学方程实现传感器节点保密率的自适应调节机制。通过扩展经典保密率计算公式，首先建立了能适应聚簇无线传感器网络环境中簇成员传感器节点和簇头传感器节点之间的保密率计算公式。然后，通过建立一种非合作传感器节点保密率博弈模型，解决了传感器节点最大化各自保密率时影响整个网络通信的问题。最后，利用演化博弈论中的复制动力学方程，给出传感器节点如何动态地选择各自的发射功率来最大化其保密率适应度的演化过程，实现传感器节点保密率自适应调节机制。

第 2 章

博弈论概述

本章给出博弈论的基本概念，介绍适用于不同应用场合的博弈类型，包括完全信息静态博弈、完全且完美信息动态博弈、重复博弈、不完全信息静态博弈、完全但不完美信息动态博弈、不完全信息动态博弈、合作博弈、信号博弈、演化博弈、微分博弈、随机博弈、联盟博弈等，为后续章节博弈论的应用和相关工作的比较提供知识准备。

2.1 博弈论基本概念

博弈论(Game Theory)是现代数学的一个新分支，也是运筹学的重要构成内容之一。博弈论主要研究具有相互依赖行为的参与者的策略选择。现在通常所说的博弈论一般是指非合作博弈理论，认为参与者是理性的，即参与者之间都会在一定的约束条件下最大化自身的利益，同时参与者之间在交互时利益有冲突，行为相互有影响，而且不同参与者掌握的信息常常是不对称的。在这种情况下，博弈论研究参与者的行为、交互时的策略和策略的均衡问题[19, 20]。当然，现代博弈论还包括合作博弈。合作博弈强调的是团体理性、集体的效率、公正和公平[19]。

博弈论作为研究多人谋略和策略问题的理论。首先，一个博弈问题必须至少有两个参与博弈的参与者，在博弈过程中他们都有各自的切身利益。由于各自利益的驱动，他们在做出自己各自的决策时，总想使用最优策略；其次，博弈中的各个参与者之间总不可避免地存在着竞争。竞争贯穿了整个博弈的全过程，同时这种竞争又将博弈的参与者紧紧地联系在一起，相互较量，相互依存；再次，既然参与者之间要进行较量，那么每一个博弈参与者都会尽量掌握对手的特点及其已经采取或可能采取行动的相关知识和信息；最后，就是博弈参与者最为关心的博弈结果[15, 16, 21]。博弈结果随不同参与者采取策略的不同而不同，通常用支付(Payoff)来描述博弈结果。因此，博弈论就是从理论上对博弈参与者之间的行为和交互过程进行研究和分析，为博弈参与者预测出一个理想的结局。这种预测结局的正确性主要体现在博弈参与者都能自愿选择博弈理论为其推导出的策略，并且没有博弈参与者愿意独自偏离其依照博弈理论已选定的策略。所以，每个博弈参与者所选策略是针对其他参与者所选策略的最优反应。

下面介绍博弈论中的一些基本概念。

1) 参与者

参与者(Player)是指一个博弈中独立决策、独立承担后果的决策主体，通常又称为局中