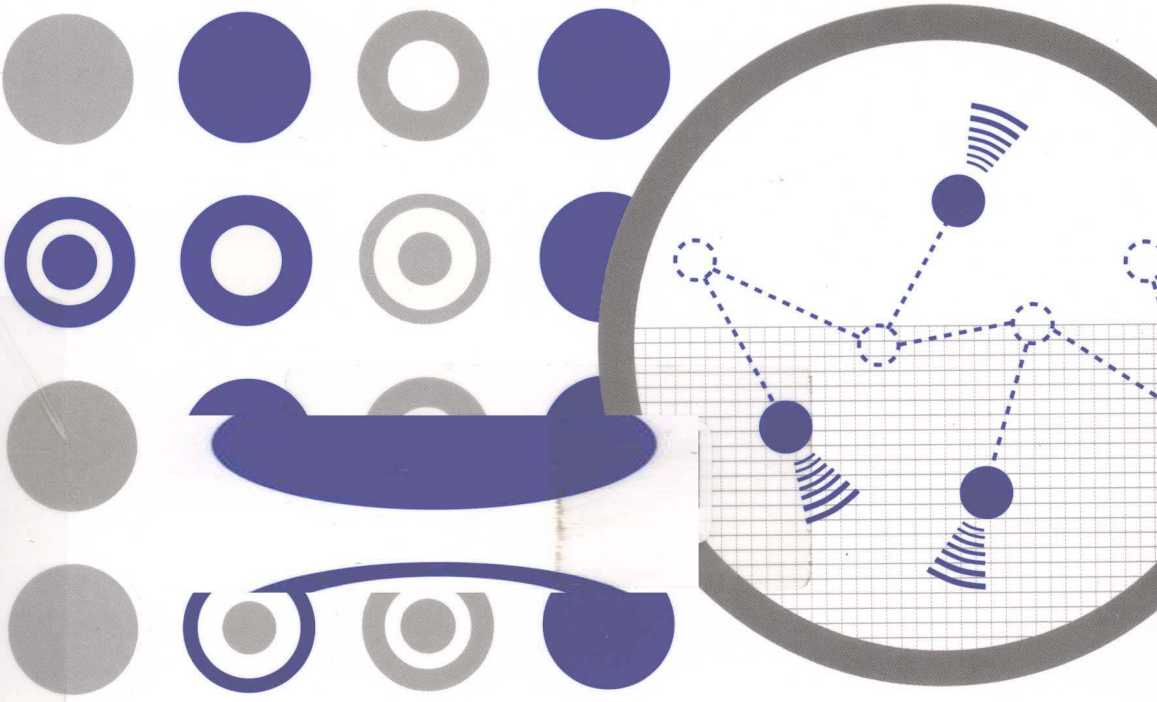
无线传感器网络可生存理论与技术研究

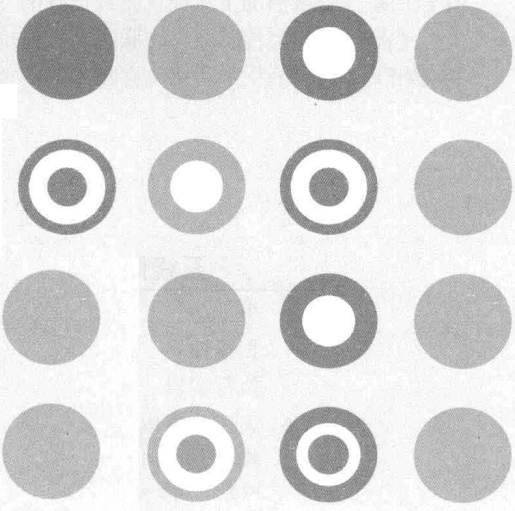
王良民 廖闻剑 著



人民邮电出版社
POSTS & TELECOM PRESS

无线传感器网络
可生存理论与技术研究

■ 王良民 廖闻剑 著



人 民 邮 电 出 版 社
北 京

序

近两年来，物联网研究及其应用引起了一些国家的高度重视，美国、欧盟、日本和我国等纷纷加大经费投入，力图尽快占领科技制高点。物联网由传感器网络、物流系统和网络化嵌入式系统等发展演化而来，有望继 20 世纪 80 年代 PC、90 年代互联网之后，引发 IT 业第三次产业化浪潮。2009 年 1 月，IBM 总裁兼 CEO 彭明盛提出“智慧地球”新理念，美国总统奥巴马积极回应，表示要将其上升为国家发展战略。2009 年 6 月,欧盟提出物联网 14 条行动计划，以确保欧盟在物联网构建中的主导作用。2009 年 8 月，温家宝总理到无锡考察时提出了“感知中国”的战略构想；同年 11 月，他在北京向首都科技界作了题为《让科技引领中国可持续发展》的报告，强调“要着力突破传感网、物联网关键技术”。

无线传感器网络技术是物联网的核心支撑技术之一。对无线传感器网络研究的支持最早见于美国国防部高级研究计划局，他们在 1978 年资助卡内基·梅隆大学进行分布式传感器网络研究，主要研究由若干具有无线通信能力的传感器节点自组织构成的网络。后来，无线传感器网络和互联网、智能计算等技术相结合，逐渐形成了泛在传感器网络。2008 年 ITU-T 发表了《泛在传感器网络》的研究报告，指出传感器网络已经向泛在传感器网络的方向发展，它是由智能传感器节点组成的网络，能以“任何地点、任何时间、任何人、任何物”的形式部署，可以在广泛的领域中推动新的应用和服务，从安全保卫、环境监控到推动生产力、增强国家竞争力。

国家自然科学基金委员会自 2002 年开始资助无线传感器网络方面的研究项目，并在 2003 年组织了无线传感器网络研讨会。自 2004 年开始，国家自然科学基金委员会信息科学部几个相关科学处陆续资助了几个传感器网络方面的重点项目和一批面上项目，内容涉及传感器网络的各个方面，也包括传感器网络的安全问题。从整个产业的角度看，也许安全及其相关技术的商业份额不足 1%，但这是关键的 1%，它的不足可能导致整个产业的危机。国家自然科学基金委员会从 2005 年开始资助关于无线传感器网络安全问题的研究，其他相关部委也都非常重视无线传感器网络的安全问题，例如 2008 年国家科技重大专项中，就有无线传感器网络安全方面的专题。在当前物联网产业逐步兴起的时候，安全问题的研究与解决显得更为迫切。当然，也许人们可以仿照互联网的发展模式，先从应用系统着手，搭建基础平台，然后不断修补其中的安全漏洞。但是，在病毒、入侵技术

十分发达的今天，新一轮矛与盾的博弈，盾的劣势是非常明显的。而作为物联网基础之一的无线传感器网络，其节点能力弱以及大规模部署的特点，使得这种劣势更加明显。

这个时候，《无线传感器网络可生存理论与技术研究》一书重提 Dobson 博士在 1986 年 IEEE S&P 会议上提出的利用不可靠、不安全的部件（Unreliable Insecure Component）来构建安全可靠系统的理念，利用传感器网络大规模冗余部署的特性，弥补单个节点在安全防范能力上的不足，就具有重要的意义。关于网络系统的可生存性，1993 年 Neumann 等人基于用户需求给出了一个定义，认为可生存性是“在任何不利条件下，基于计算机通信系统的应用所具有的持续满足用户需求的能力”。尽管在产业或者商业模式中，我们难以做到绝对的安全与可靠，但是在具体应用中，用户需求的服务必须得到持续的满足。如果用可生存性来涵盖用户“在任何条件下，都能给我需要的服务”这一需求，那么近年来很多关于无线传感器网络的研究都可以纳入可生存技术的范畴，例如：容错的覆盖控制方法、容侵的拓扑结构、容侵的安全机制、多路径的传输协议等。但是，目前还没有关于无线传感器网络可生存技术的系统著作，王良民博士的这本书恰好弥补了这方面的缺憾。其中关于替代性再生资源以及应用驱动型可生存技术的探索，相当新颖，希望作者能继续在这方面做深入研究。

我和王良民博士的相识源于自然科学基金的通信评审工作，后来得知他从 2004 年攻读博士学位时开始研究无线传感器网络的生存理论与技术，博士毕业当年就获得了青年科学基金的资助。7 年来他一直从事相关研究，此书是他和研究组科研成果的系统表述。令我感到欣喜的不仅是这样一部专著，还有这本书的背后，我看到一大批年轻有为的博士们留在了高校或研究所，继续从事他们喜欢的科研工作，逐步形成了自己的研究特色，成为对某个领域有系统看法的年轻学者。我希望王良民博士和廖闻剑高级工程师的这本著作能给该领域的科研工作者和研究生提供有价值的参考，对推动无线传感器网络生存技术的研究起到积极作用。

2011 年 2 月 22 日于北京

前　言

无线传感器网络源于美国国防高级研究计划局，他们资助卡耐基梅隆大学进行分布式传感器网络的研究项目。传感器网络的出身决定了它从一开始就和军事应用、安全问题、恶劣甚至敌对的环境紧密相关。无线传感器网络有两个特点，一个是单个节点能力弱，另一个是节点廉价适合大规模部署，因此，利用节点及网络结构的冗余性来弥补单个节点能力的不足，成为构建其安全性、稳定性及可靠性的常见思路。当前与无线传感器网络相关的容错技术、可靠性技术多数是基于这个思路实现的。

目前，学术界关于网络的可生存性尚没有统一的定义，但是在描述上可以达成共识，这就是“在任何不利条件下，系统能提供用户需求的关键服务的能力”，即不管是否遭受入侵、故障，是否部署在恶劣的环境中，不管采用什么手段和技术——是加固系统、入侵响应还是优雅降级，可生存技术的最终目标是面向用户需求，提供关键服务。容错、容侵是最常见的可生存技术；自愈、自再生、自生成技术则是近年来受到越来越多关注的新一代可生存技术。本书首先从多重覆盖、多联通拓扑、多路径传输三个方面介绍了容错的无线传感器网络可生存技术；接着考虑到入侵与故障的不同，区分了容错和容侵这两个概念。在此基础上，讨论了无线传感器网络的安全结构、入侵检测及生存性定量评估技术。随后，以移动节点的定向补位和播撒节点作为更新性补偿资源，研究了无线传感器网络自再生的可生存技术。最后，从应用出发，定义系统的关键服务，根据关键服务的需求，设计新的 MAC 协议，并认为这种面向应用设计的保障关键服务的实现技术，应该也是可生存技术中重要的一类，希望引起研究人员和技术人员的兴趣。

这本书是我在博士、博士后及访问学者 7 年工作时间内科研工作的系统表述，包含了本人和合作者们共同完成的相关研究，有理论方面的探索，技术上的创新，也有系统应用过程中具体问题的解决。2004 年初，我到西安电子科技大学攻读博士学位时，导师马建峰教授就让我从事无线传感器网络安全技术的研究；2007 年初，我博士答辩结束时，马老师鼓励我继续从事无线传感器网络尤其是与容侵技术相结合的可生存问题的研究。随后我到江苏大学申请了国家自然科学基金项目“容忍入侵的无线传感器网络拓扑控制理论与方法研究”，当年就获得了资助。作为密码学的博士生，为进一步了解网络架构及相关知识，我向东南大学计算机科学与技术流动站申请从事博士后工作，我的合作导师顾冠群院士在面试时和我就

容侵的网络结构及网络生存性问题展开了讨论，并招收了我这个据说是他一生唯一的一个博士后。在站期间，我申请了博士后科学基金和江苏省博士后科学基金，均获得了支持，而“容忍入侵的无线传感器网络协同防御体系与方法”在 2008 年获得了第一批国家博士后科学基金特别资助，我的一篇关于无线传感器网络容侵拓扑自再生方面的论文也被中国计算机大会录用并选为优秀论文。2009 年我应邀成为 ACM 组织的传感器网络应用国际会议 SNA2010 的 TPC member；随后获得了国家留学基金的支持，赴新加坡师从国际电子电器工程学会会士 Alex KOT 从事访问学者工作。他创新地提出让我研究以移动节点作为“钦差大臣”——哪里需要到哪里去这样一个混合网络模式。总体来说，这段时间，我的研究工作一直集中在无线传感器网络的安全性、容侵、自再生等方面，研究问题涉及覆盖、拓扑和路由层面的容错、容侵两类可生存关键技术，还包括了安全结构和入侵检测、生存性评估等生存性研究相关的经典内容。最近我们研究了移动节点修复覆盖洞、播撒节点形成第二代网络的资源替代问题，还研究了在这两类补偿性资源基础上的网络自再生问题。所有这些工作在本书中都得到了系统表述。

在研究无线传感器网络容侵理论与技术的同时，江苏大学计算机科学与通信工程学院帮助我组建了无线传感器网络研究小组，这是一个包含 6 位教师的稳定团队，我们开始了较为全面的无线传感器网络研发工作。我们依托电子制造企业，设计了多个版本的高可生存性的节点，从硬件层增加了冗余性，可满足恶劣环境中信息的传输、存储；我们研发了恶劣环境中的应用 MAC 技术、路由技术、零丢包数据传输技术等。我们将自研发的节点和 XBOW 公司的系列节点一起，组建了混合网络，分别基于 Jenic 无线单片机的研发系统、TinyOS 开放源码系统和 XBOW 的 Moteworks 平台做了实现工作，而理论研究工作分别在 TOSSIM 及 NS2 仿真器进行模拟实验，有条件地在实际平台测试。实际上，我们的团队也和企业进行横向合作，研制的恶劣环境下的高可靠性节点，设计并开发的特种环境下可靠传输的网络系统，都在相关企业开始产品化和商业化。事实上，特种应用环境中无线传感器网络系统的关键服务仅仅体现在危急时刻，为此需要采取一些措施保证此时优先级高的关键服务，如应用驱动的 EDA-MAC，我们把这种“应用事件”驱动型的“应急”的技术手段放在本书的最后一章，称之为应用型可生存技术。我们希望这方面的“技巧型”研究也能受到广大对可生存技术感兴趣的研究者和技术人员的重视。

因此，本书内容作为此段时间内我们研究团队所有工作的自然集成及系统化表述，都涵括在无线传感器网络可生存的理论与技术这一个主题之下。本书试图系统地介绍无线传感器网络的可生存技术，但是并不是面面俱到，而是重点介绍我们近几年来的研究工作。本书的主要读者还是大学及研究所里从事科研工作的人员，包含大学高年级学生、研究生以及从事无线传感器网络应用工作的技术人

员。如果这本书在系统介绍我们自己工作的同时，能够把我们几年来对可生存技术的兴趣与体会表达出来，能够吸引更多的读者关注这个领域，那么将是对本书作者及其他推动这本书问世的朋友们的最大肯定。

我想把前言的最后一部分留给所有为本书研究成果有过贡献和帮助的老师、朋友与学生，没有他们的指导和支持，就没有本书的出版。

本书的研究内容除作者之外，还包含了多名合作者的心血，有指导我从事相关研究的4位导师：博士导师长江学者马建峰教授，博士后合作导师中国工程院院士顾冠群教授和罗军舟教授，访问学者合作导师、国际电子电气工程学会会士Alex KOT教授；还有我在江苏大学无线网络结构、安全及应用研究团队的领导和同事们，他们是詹永照教授、张建明教授、熊书明博士、王新胜博士和陈向益博士；以及为本书作出了最直接贡献的学生们，这些在我们研究小组工作和学习过的研究生们有顾丽芳、余群、张沛、周玲玲、蒋丽萍、江长勇、蒋中秋、徐广华、饶静宜、李菲、姜涛、秦颖、茅冬梅等。本书的很多研究成果与他们的聪明才智和勤奋认真是分不开的。

在这些合作者之外，我还要感谢国家杰出青年基金获得者江苏大学校长袁寿其教授，2年前他建议我著一部书系统地表述自己的科研工作，是我筹划本书的思想源头。我还需要特别感谢应我请求欣然为本书作序的刘克教授，我能在博士毕业后继续从事本书所述的研究，得益于国家基金的及时支持；而我了解并敢于申请基金则得益于他2005年在西安电子科技大学关于基金的宣讲报告，他讲述的国家基金资助原则和申请的方法与技巧，至今我依然经常引用以指导比我更年轻的同事。最后，向我的好朋友阎星娥女士和肇丽女士表示衷心的感谢，前者促成了我和廖老师合著这本书，后者推动了本书的出版。

当然，我必须感谢我的家人和朋友，特别是我的妻子，5年来，我们聚少离多，是她承担了家务和照顾孩子的工作，让我有更多的时间和精力从事本书的工作。谨以此书献给我3岁的孩子，他无邪的言行举止给了我工作之余最大的快乐。

由于科研水平有限，加之著书经验不足，本书一定有不少缺点和错误，希望得到广大读者的指正。无线传感器网络随着物联网产业的发展，必然会继续飞速发展；而其可生存技术将会受到越来越多的关注与重视。我们将在吸取大家意见和建议的基础上，不断修改和完善书中内容，为推动无线传感器网络可生存理论与技术的进步尽绵薄之力。

王良民

2010年12月26日

目　录

第1章 概 述

首先简要地描述了无线传感器网络概念的由来、网络的组成和网络的功能；然后介绍可生存性的概念以及可生存技术的特点，辨析生存性与安全性的相关与不同；针对不同的可生存系统重点介绍并比较两类可生存技术，认为容错、容侵和自再生是3类可生存关键技术；最后给出了本书的章节安排。

1.1 无线传感器网络

无线传感器网络（WSN,Wireless Sensor）的概念最早由美国军方提出，起源于1978年美国国防高级研究计划局（DARPA, Defense Advanced Research Projects Agency）开始资助卡耐基梅隆大学（CMU, Carnegie Mellon University）进行分布式传感器网络的研究项目，主要研究由若干具有无线通信能力的传感器节点自组织构成的网络。随着无线通信技术和多种网络接入方式的发展，无线传感器网络和互联网技术、智能计算技术的结合，逐渐形成了泛在无线传感器网络（USN, Ubiquitous Sensor Network）。2008年，ITU-T发表了《泛在传感器网络》的研究报告，指出传感器网络已经向泛在传感器网络的方向发展，它是由智能传感器节点组成的网络，可以以“任何地点、任何时间、任何人、任何物”的形式部署，可以在广泛的领域中推动新的应用和服务。

无线传感器网络结构如图 1-1 所示，传感器网络系统通常包括传感器节点（Sensor）、汇聚节点（Sink）和基站及管理节点。大量的无线传感器节点随机部署在监测区域内，实现了短距离、低功耗、低速率的数据传输。传感器节点之间通过无线传输的方式进行连接与转发，形成大范围的覆盖容纳。传感器节点之间能够自组织组网，可以根据不同的需要智能地采用不同的网络拓扑结构。数据通常以多跳的方式，经过路由到其他中间节点进行数据融合和转发，最后到达基站节点，或通过网关和多种传输方式进入互联网，到达用户可以操作的管理节点。

无线传感器网络节点通常是一个微型的嵌入式系统，它的计算能力、存储能力很弱，而且通信带宽窄，由自身携带的电池供电，能量也非常有限。节点不仅要收集本地信息进行数据处理，还要对其他节点转发过来的数据进行存储、管理、融合和转发。网关和基站的存储能力、计算能力、通信能力以及供电能

力通常都比较强，连接传感器网络与外部网络。如果网关由一个具有增强功能的传感器节点充当，通常也称为汇聚节点。在具体研究中，如果不考虑汇聚节点与外部网络的连接，抽象地认为由用户直接控制汇聚节点，则此时汇聚节点也称为基站。

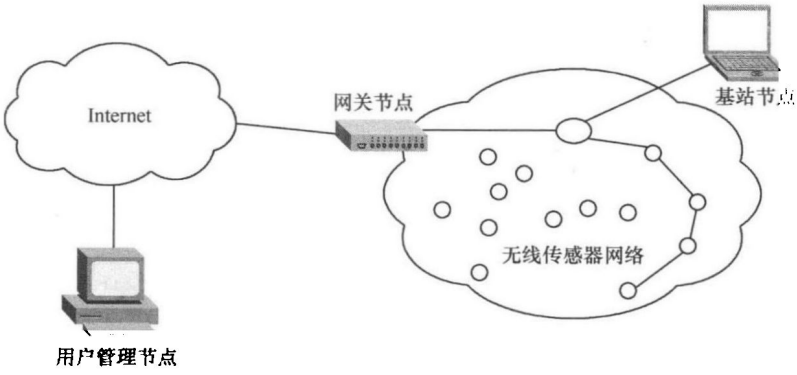


图 1-1　无线传感器网络体系结构

无线传感器网络通常布部署在无人照料（Unattended）的恶劣环境中，为此需要网络具有自维护的特征，即使部分节点因为故障、入侵以及电池耗竭而失效或者死亡时，也不影响网络监控和数据传输两大关键服务。无线传感器网络通常以播撒的方式部署在敌方能接触到的恶劣环境中，节点自身能力弱、防范能力差，使得包含其可靠性、安全性和可用性的网络生存性问题成为很难解决却又必须考虑的困难问题，而因为节点廉价而大规模冗余部署，也给增强其生存性的容错、容侵及再生等关键技术提供了用武之地。

1.2　可生存性的定义及特点

Neumann 等人[1]于 1993 年定义了网络系统可生存性：在任何不利条件下，基于计算机通信系统的应用所具有的持续满足用户需求的能力。其中，用户需求包括安全性、可靠性、响应和正确性等需求。与之相似，1997 年 Ellison 等人[2]定义了网络系统的可生存性：网络系统在遭受攻击和意外事故的情况下及时完成任务的能力。2000 年 Knight 和 Sullivan[3]提出了一种网络系统可生存需求的四元组表示。我国的杨超等[4]给出了系统可生存性的形式化模型，王超等[5]给出了系统可生存性的综述。

网络系统可生存性的实现有赖于其所处的计算环境，而这种计算环境的发展趋势是从有界网络向无限极大网络发展。与有界网络相比，无限极大网络有以下

特点：

- 有多个管理域但每个管理域都不具有全局管理控制权限；
- 网络中的每个节点对整个网络的节点数量和特性都不完全了解，缺少全局可见性；
- 节点间的互操作性由节点间的协议决定；
- 合法用户和攻击者在环境中的地位是相同的，不可能用管理策略加以区分。

对比 1.1 节对无线传感器网络的介绍与以上无限极大网络的特点，不难看出，无线传感器网络正好满足其所有特性，因此无线传感器网络的可生存性研究具有重要的意义。

无限极大网络系统容易成为攻击者的目标，缺少全局管理，难以人力修复。要实现具有无限极大网络特点网络的可生存性，网络系统必须具备以下 4 个特性。

（1）抵御

抵御非法入侵是安全性研究的主要内容，也是生存性研究的一部分。传统的安全技术如认证、加密，可靠性技术如多样性、容错、容侵等，仍然是生存性的最常用方法。

（2）识别

随着规模和复杂性的不断增长，网络系统不可避免地会遭受攻击破坏和发生故障，网络系统的可生存性也主要体现在对攻击和系统损坏程度的识别和恢复上。

（3）恢复

对于生存性而言，无论是否出现攻击和故障，系统及其重要服务都要得到保护。对于攻击和故障等，可生存性研究认为重要的是对其影响的评估和系统的恢复，而不是对起因的及时响应。判定网络系统生存性是否失败的标准，不是是否被入侵，而是网络系统能否提供用户需求的关键服务。

（4）进化

适应与进化以及减少可能再次发生相同或相似的攻击。

为此本书研究无线传感器网络抵御故障及攻击影响的生存技术，包含信息安全的抵御措施、入侵的识别和基于冗余与再生的恢复、进化能力。

1.3　可生存与信息安全技术

信息安全技术发展至今，大致经历了 3 个发展阶段：以防范入侵为主的信息保护阶段、以入侵检测技术为特色的信息保障阶段和以容忍入侵为核心的信息可生存阶段。

1.3.1 以防范入侵为特色的信息保护阶段

当设计和研究信息安全措施时，人们最先想到的是保护。它假设能够划分明确的网络边界并能够在边界上阻止非法入侵，其基本技术原理是保护和隔离，通过保护和隔离达到真实、保密、完整和不可否认等安全目的。比如，通过口令阻止非法用户的访问；通过存取控制和权限管理让某些人看不到敏感信息；通过加密使别人无法读懂信息的内容；通过等级划分使保密性得到完善的保证等。但是，并不是在所有情况下都能够清楚地划分并控制边界，从而导致保护措施也并不是在所有情况下都有效。随着 Internet 的逐步扩展，人们发现在许多情况下保护技术无法起作用，比如，在正常的数据中夹杂着可能使接收系统崩溃的参数、在合法的升级程序中夹杂着致命的病毒、黑客冒充合法用户进行信息偷窃、利用系统漏洞进行攻击等。随着信息空间的增长，这种在系统存取控制的基础上，采取各种类型的防火墙来堵住原来系统中的缺口的方法，已经难以满足实际需要了。实际情况往往比设计者和评估者想象的要复杂得多，许多著名的安全协议和系统都被发现存在漏洞。仅仅依靠保护技术已经没有办法挡住所有敌人的侵入，于是，入侵检测技术就应运而生了。

1.3.2 以入侵检测为代表的信息保障阶段

已有的关于信息保障技术的研究是以入侵检测技术为主要代表的第二代信息安全技术。“信息保障技术”的基本假设是，如果挡不住入侵，但至少能发现入侵和入侵造成的破坏。比如，能够发现系统死机、网络扫描、流量异常等。

其实，从完全意义上来说，信息保障本身有比“信息安全”更宽的含义。信息保障是包括保护、检测、响应并提供信息系统的恢复能力，保护和捍卫信息系统的可用性、完整性、真实性、机密性以及不可否认性的全部信息操作行为，即信息保障技术融合了保护、检测、响应、恢复四大技术，是针对完整生命周期的一种安全技术。在信息保障技术中，所有的响应都依赖于检测结论，检测系统的性能就成了信息保障技术中最为关键的部分。因此，检测技术是信息保障技术的核心，检测系统能否检测全部的攻击成为检测技术面临的最大挑战。

然而，早在 1987 年，Cohen 博士就发表了关于区分病毒代码和正确程序代码的定义，认为通过分析代码是不可能区分它们的。系统漏洞千差万别，攻击手法层出不穷，检测技术要发现全部攻击是不可能的，准确区分正确数据和攻击数据是不可能的，准确区分正常系统和有木马的系统是不可能的，准确区分有漏洞的系统和没有漏洞的系统也是不可能的。为此，必须用新的技术来保护关键系统。

1.3.3 以容忍入侵为核心的生存技术阶段

生存技术是系统在入侵和故障已发生的情况下，在限定的时间内完成使命的

能力。对于信息安全领域而言，生存技术的核心技术是容忍入侵，即在入侵不可避免甚至不可检测的情况下，来保护关键系统和关键服务的技术。早在 20 世纪 80 年代中期，Dobson 和 Randell 就提出了利用不安全并且不可靠的部件来构建安全可靠的系统的方法[6]，这实际上是容忍入侵的思想雏形。Fraga 和 Powell 更是在其论文中正式提出了容忍入侵（Intrusion Tolerance）的术语，且该术语被一直延用至今[7]。Deswarte Y, Blain L 和 Fabre J C 等人提出了基于分割 + 分散（fragmentation-scattering technique）的方法实现容忍入侵的思路[8, 9]。然而在此之后，容忍入侵的思想一直没有得到业内人士的太多关注。

近几年来，随着分布式密码学的研究，特别是秘密共享和门限密码学方面的研究逐渐成熟与完善，再加上分布式网络应用系统的大量应用，容忍入侵的理论、方法与应用又开始进入人们的视野，并且逐渐成为信息安全业内人士关注的一个焦点。国际上，比较有影响的有 ITUA 的先进冗余技术[10]、ITTC 的门槛密码学[11]、SRI 的可靠系统结构[12]和 UMBC 的容忍入侵数据库[13]等。国内，国防科技大学[14]、武汉大学[15, 16]、中科院软件所[17]、西安电子科技大学[18, 19]等也分别在不同的领域做了大量工作。

对现有无线传感器网络容忍入侵技术的研究并不多见，主要是构建冗余的路由[20]、基于多路径的可靠数据传输[21, 22]、多目标的基站[21]等，通过建立多路径、多基站等，使得当网络中个别节点、基站被入侵时，发挥其他路径、节点和基站的作用，保证数据采集传输等关键服务的通畅。Yang[23]提出了一种将节点身份与其位置捆定的方法，是利用邻近区域内的多个节点的协作提高系统的容侵能力。总体来说，文献[20～22]是利用节点（基站）的冗余性来容忍入侵，而文献[23]则是利用区域内节点密度的冗余性来提供系统面临入侵时的生存性。然而这些工作不曾考虑到网络在物理层和链路层是否具有需求的冗余性，即网络拓扑是否提供了多路径存在的可能性？网络中是否有足够的节点来提供需求的多通信链路或节点密度？为此，本项目研究容忍入侵的无线传感器网络拓扑控制方法，研究如何布置网络才能使系统在物理层具有足够的节点密度，研究如何生成并维持一个存在冗余多路径的网络拓扑。国内关于无线传感器网络容忍入侵的文献，可查的仅有关于拓扑控制方面的。文献[24]从理论上探讨了基于拓扑的容错和容侵的区别，而文献[25]则提出了一种自再生的拓扑生成方法。

1.4　可生存技术的分类

可生存系统通常具有 1.2 节介绍的 4 个方面特征，但在本质上来说，可生存系统应能够在面对随时出现的故障与攻击的情况下仍然连续地为预期的用户提供

及时服务。它必须面对系统用攻击避免和预防手段无法阻止的破坏行为带来的影响，必须对它们采取一些必要的措施保证关键应用的功能连续正确。这些措施体现在无线传感器网络中就是冗余节点部署、多重覆盖、多联通拓扑、多路径路由、容侵的安全结构以及对入侵结果的检测、评估和恢复等可生存技术与应对策略。

可生存系统按照可生存技术植入系统的时间可以分为两类：第一类是先应式的错误遮蔽系统，意思是攻击发生了以后，整个系统好像没什么感觉；另一种是反应式的攻击响应系统，这也是比较容易想到的解决方案，通过改进检测系统，加快反应时间，从而使原有的信息保障和错误遮蔽技术上升到一种在攻击发生的情况下能够继续工作的系统。

1.4.1 先应式可生存技术

采用先应式可生存技术的系统从一开始就重新设计整个系统，以保证攻击发生后对系统没有太大的影响。该方法的基本原理和以往的容错技术类似，在设计时就制造足够的冗余，以保证当部分系统被攻击时，整个系统仍能够正常工作。Byzantine 容错主要针对随机错误，当错误发生时，只要满足一定的条件，整个系统仍旧能够得出正确的结果。门限密码学的思想是：“n 个个体中的 t 个个体参与合作就能够完成密码运算，而少于 t 个个体即使合作也无法完成这种网络运算”，放在无线传感器网络中一样可以应用。这就是说，只要少于 t 个节点被攻击者控制了，只要还拥有多于 t 个的个体，节点依然能完成管理者发布的任务。

此外，由于冗余是有限的，随着时间的积累，攻击者可能会攻陷越来越多的节点，从而超出了系统所能容忍的 t，为此，先应式可生存技术通常还需要周期性地增加网络节点，以防止其冗余部分产生错误而未觉察到，从而导致整个系统失败。

1.4.2 反应式可生存技术

采用反应式可生存技术的系统不需要重新设计系统结构，系统的操作和连接界面也可以与原有的一样。这样的容侵系统包括两个基本组成部分：入侵检测与判决系统、包含在线的修复管理程序和隔离机制的系统资源控制系统。当入侵检测系统检测到入侵时，就调用资源重新分配以减缓这种入侵现象，或采用隔离机制隔离数据和操作，从而阻止错误发生；同时，入侵判决系统作出正确的判决以后，修复管理程序再将攻击操作所导致的错误结果进行修补。当判决系统认为确实是攻击时，就将被隔离的操作删除掉；当判定不是攻击时，就将这些隔离的结果融合到正确的系统中去。

可以看出，反应式可生存系统非常依赖于入侵检测判决系统，这样的系统也被称作生存技术的触发器。因此关于无线传感器网络的入侵检测技术也是本书介绍的重要内容之一。