许文丽 王命宇 马 君 著

数字水印技术及应用

Digital watermarking technology and its application

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

数字水印技术及应用

许文丽　王命宇　马　君　著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

数字水印技术的研究涉及信息学、密码学、计算机科学、数字信号处理、图像处理、模式识别等多种学科，具有广阔的应用前景。本书详尽地给出了图像数字水印的各种应用算法及实例，理论基础全面，参考性和可操作性强。

本书可以作为通信与电子系统、信号与信息处理等专业的高年级本科生和研究生的入门教材或参考书，还可以作为信息安全与保密通信、多媒体数字产品保护和电子商务安全等领域的技术人员和管理人员的参考书。

图书在版编目（CIP）数据

数字水印技术及应用 / 许文丽，王命宇，马君著. —北京：电子工业出版社，2013.1
ISBN 978-7-121-18634-9

Ⅰ. ①数… Ⅱ. ①许… ②王… ③马… Ⅲ. ①电子计算机—密码术 Ⅳ. ①TP309.7

中国版本图书馆 CIP 数据核字（2012）第 233000 号

责任编辑：赵 娜 特约编辑：逯春辉
印 刷：三河市双峰印刷装订有限公司
装 订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：720×1 000 1/16 印张：14 字数：314 千字
印 次：2013 年 1 月第 1 次印刷
定 价：42.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着以计算机、网络通信为代表的信息技术的蓬勃发展及其在社会各个领域的广泛应用，人类全部的信息资源以前所未有的程度和方式在全球范围内互连互通。信息、物质、能量是物质世界的三大支柱，是人类社会赖以生存和发展的重要条件，它们共同构成了国民经济发展的决定因素。世界上大多数国家已经将信息化提高到国家发展战略的高度。目前，全球信息产业正面临着新一轮的“U”化战略，即unite（融合）、universal（普及）、user（用户）、unique（独特）、ubiquitous（无处不在）。应时代的发展要求，物联网成为继计算机和互联网之后，世界信息产业的第三次浪潮，成为当今世界相关领域高度关注的综合前沿技术和深入探索研究的热点工程。

物联网的兴起和发展，使得人与物、物与物之间的交互更加紧密，它将越来越广泛地应用于现代社会的政治、经济、文化、教育、科学研究与社会生活的各个领域，包括军事、医疗、交通运输、物流等方面，用以提高社会、经济效益，节约成本，让民众可以随时随地享受科技智慧带来的服务。然而，物联网中万物相关的数据和信息中有些数据会直接关系到国家的机密、人们的隐私等，要保护这些有经济价值和社会价值的数据的安全远比保护互联网上音乐、动漫、影视、游戏等数据重要得多，也困难得多。

物联网的安全基本与一般 IT 系统的安全一样，主要包括信息系统的安全机密性、完整可靠性、真实可信性、通信对象的可信赖性和个人信息的保密等。随着物联网以及泛在网的发展，产权保护、个人隐私的保护以及所创造的数字制品的保护等更加成为数字制品发行业务首要解决的问题。

信息隐藏与数据加密技术都是为保护秘密信息的存储和传输，使之免遭攻击者的攻击和破坏，从而实现信息安全的重要技术，但二者有着显著的区别。信息加密所隐藏的是消息的内容，攻击者虽然知道其存在，但难于提取其中的信息；而信息隐藏则是将需保密的信息“乔装打扮”后藏匿在信息空间中的一个大且复杂的子集中，目的是使攻击者难以搜寻其所在，它所隐藏的是信息的存在形式。虽然信息隐藏与信息加密是互不相同的两类技术，但两者有密切的关系，两者的适当组合运用可以相互弥补不足之处，更好地实现系统的安全。

密码的理论和技术为信息的递送、存储和管理提供了多种可能的解决方案，成为解决信息安全的核心技术之一，它提供了对消息的加密与解密、签字与认证，以及电子商务和电子政务所需的一些特殊要求，如不可否认性、盲签名等技术。密码

的不可破译度依赖于密码算法的抗攻击能力和密钥的长度。随着量子计算和 DNA 计算时代的到来，一切建立在计算复杂性理论基础上的密码安全性都面临着严峻的挑战。

数字水印技术是信息隐藏技术的一个重要分支，它在真伪鉴别、隐蔽通信、标识隐含、电子身份认证等方面具有重要的应用价值。应用密码技术加密的内容具有不可观展性，不易进行传播，而且解密之后缺乏有效的手段来保证其不被非法复制、再次传播、非法发行及恶意篡改。

数字水印技术的研究始于 20 世纪 90 年代初期，早期的数字水印技术研究是针对数字图像进行的，如 Tirkel 等人 1993 年在关于该技术的论述中首次提出了“电子水印”（Electronic Watermark）的说法。Schyndel 等人在 1994 年的 ICIP 会议上发表了一篇题为 *A Digital Watermark* 的论文，正式提出了“数字水印”这一术语，同时指出了其可能的应用。该论文被认为是一篇对于数字水印具有历史参考价值的文献，标志着这一研究领域的开始。1996 年，在英国剑桥牛顿研究所召开的第一届信息隐藏学术研讨会（IHW），标志着信息隐藏作为一门新学科的诞生。这次会议将其重要分支——数字水印作为它的主要议题之一，同年 IEEE International Conference on Image Processing 等国际会议也将数字水印列为专题。

随着当代数字技术、各种传输处理技术以及多媒体制作的发展，使得数字产品和网络上传输的信息被保真地非法复制和散布变得更加容易。在开放的互联网、物联网以及泛在网的环境下，如何保护所传输信息的安全性，可靠性，信息来源的可信性、不可抵赖性，如何保护个人隐私（如远程医疗中的电子病历、财务收支、嗜好等），如何保护产权等，都不是容易解决的问题。信息保密和产权（版权）保护都可依赖于数字水印技术。

数字水印技术在图像、视频、音频、文本、数据库等常规载体方面都已经开展了很多研究工作，并取得了较好的研究成果。随着物联网的兴起和发展，研究者开始把在传统网络中广泛使用的数字水印技术引入到物联网的研究中。

为了保护用户的隐私，如身份、地址、路由等不被泄露，在网上的现金支付、投标、拍卖、投票选举等场合，可采用数字水印技术实现匿名支付、匿名通信、匿名签字、匿名选举等。另一方面，为了隐匿版权信息，常在表示数字对象所有权的消息上附上标记（Mark），如数字水印（Digital Watermark）、数字指纹（Digital Fingerprint）、产品序列号（Product Serial Number）等，一旦发现被非法复制，隐藏的标记就可以识别出哪个客户的产品被复制了。

编写本书的目的是向读者介绍数字水印的各项关键技术以及数字水印的各种应用，目的是在新的物联网形势下推出更新更全面的数字水印方面的专著，使读者能够对数字水印技术有一个全面、系统的学习和了解，为今后进一步的研究打下坚实的基础。

本书共 10 章。第 1 章作为引言，简要介绍了数字水印的概念、原理、关键技术及其应用与分类，同时介绍了国内外研究现状。第 2~8 章重点阐述了鲁棒水印的基本框架、特征、设计原理及评估方法，并介绍了多种基于不同应用、不同形式的水印算法，包括数字水印的生成技术、预处理技术、嵌入技术、提取技术和检测技术。第 9 章主要研究了认证水印技术的基本概念和方法，分析水印认证的原理、基本特征和要求，研究了鲁棒数字水印认证的详细算法及应用。第 10 章主要研究了数字水印技术在传感器网络安全中的应用。

本书在研究撰写和出版过程中得到西安财经学院的支持和资助，得到了西安财经学院信息学院的支持和帮助，得到了各级领导、同仁、朋友、亲人的大力支持和帮助，该书的出版更是电子工业出版社编辑部各位领导和编辑辛勤劳作的成果，为了该书能尽快出版，他们付出了很多的辛苦，甚为感动，特此一并致谢！

本书也是陕西省自然科学基础研究项目（编号：2012JQ8023）、国家自然科学基金项目（批准号：61173164，61272436，61103199）和北京市自然科学基金（批准号：4112052）的成果总结。

由于作者水平有限，书中难免出现各种疏漏和不当之处，恳请读者批评指正。

作者

2012 年 8 月

目　录

第1章 绪 论

随着计算机网络规模的不断扩大和数字化技术的不断成熟，多媒体信息的交流已达到了前所未有的深度和广度。人们可以通过网络发布自己的作品、重要的信息和进行网络贸易等，从而使网上各种数字化图书、报刊、绘画作品、照片、音乐、动漫及影视作品的数量急剧增加。多媒体数据的数字化为多媒体信息的存取提供了极大的便利，同时也极大地提高了信息服务、表达、传送和获取的效率和准确性。

物联网成为继计算机、互联网之后，世界信息产业的第三次浪潮。物联网作为前沿热点课题，正逐步进入人们的生活，如门禁、平安校园卡、超市购物、图书管理、智能交通、智能电网、远程医疗等，势必将越来越广泛地应用于现代社会的政治、经济、文化、教育、科学研究以及社会生活的各个领域。事实和理论研究表明，物联网的应用不但可以提高经济效益，大大节约成本，而且还可以为全球经济的复苏提供技术动力。当今世界各国，包括美国、欧盟、中国等都在此领域进行了深入探索和研究。

物联网的安全和隐私保护问题是物联网服务能否大规模应用的关键。随着物联网试点工程的实施和应用的拓展，其安全和隐私问题也日益突出，特别是在军事、金融、医疗、交通运输等方面，这些数据直接关系到国家的机密和安危、社会的稳定、人民的隐私和财产安全等。没有安全性和隐私保护作保障的物联网技术是没有应用市场的，更谈不上巨大的商业价值和应用前景。由于物联网融合交叉的多源异构网络特性，使其安全和隐私问题更为复杂，这也将严重制约其技术和应用的发展。因此，物联网的安全和隐私保护成为亟待解决的问题。

本章从互联网、物联网以及未来泛在网的安全问题出发，首先介绍新的网络形势下的安全问题和特征，然后介绍密码学知识及其应用领域，再介绍信息隐藏技术及其分类，最后重点介绍数字水印系统的结构、特点、分类及其应用。

1.1 物联网新形势下的网络安全

1.1.1 因特网环境下的网络安全

随着计算机技术和网络技术的飞速发展，计算机系统功能日渐完善，网络体系也日渐强大，信息网络已经覆盖到社会的各个领域，成为社会发展的重要保证。人们在工作、生活和学习中，将许多信息存储在计算机中，并通过计算机网络来传输，

因而会受到各种人为的攻击（如信息泄露、信息窃取、数据篡改、数据删添、计算机病毒等），这些都会给国家、单位以及个人造成巨大的损失。因此网络安全已经成为一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬等的重要问题，解决网络安全问题刻不容缓。

因特网是一个全球性的网络，在这个庞大的网络里，各种不同类型的计算机通过统一的网络协议和通信协议（TCP/IP）连接在一起，共享信息资源和计算机相关的硬件资源。

Internet 已经成为全球信息基础设施的骨干网，它是一种传统媒介无法比拟的传播手段，具有多媒体的传送功能，同时具有传播速度快、通信量大、覆盖范围广、传播成本较低等特点。人们把 Internet 看成是第二次信息革命的象征，它不仅彻底地改变了信息产业的运行方式，而且将影响世界上大多数行业产业的运行方式，从而导致了一场新的产业革命。由于因特网的全球性、开放性、无缝连通性、共享性、动态性地发展的特性，使得任何人都可以自由地接入 Internet，有善者，也有恶者，恶者会采取各种攻击手段进行破坏活动。

在因特网环境下的网络威胁包括以下方面：

（1）基本的安全威胁

信息泄露，指重要数据在有意或无意中被泄露或透露给某个非授权的人或实体。这种威胁来自诸如电磁泄露、窃听、搭线、建立隐蔽隧道等窃取敏感信息或进行错综复杂的信息探测攻击。

完整性破坏，即数据的一致性通过非授权的增删、修改或重发而受到损坏，以便于取得有益于攻击者的响应，干扰用户的正常使用。

业务拒绝，即对信息或其他资源的合法访问被无条件阻止。攻击者通过不断对网络系统进行干扰、改变网络正常作业流程、发布大量数据包造成网络拥堵甚至瘫痪，或对系统进行非法的、无法成功访问而产生过量的负荷，从而导致系统资源在合法用户看来是不可使用的，使用户无法得到相应的服务。

非法使用，即某一资源被某个非授权的人或以某一非授权的方式使用。

（2）主要的可实现的威胁

在安全威胁中，主要的可实现的威胁是十分重要的，因为任何这类威胁的某一实现都会直接导致任何基本威胁的某一实现。因而，这些威胁使基本的威胁成为可能，主要的可实现威胁包括渗入威胁和植入威胁。

主要的渗入威胁有：

假冒　即某个实体假装成另外一个不同的实体，是侵入某个安全防线的最为通用的方法。某个非授权的实体提示某一防线的守卫者，使其相信它是一个合法的实体，此后便能够使用此合法用户的权利和特权。黑客大多数采用假冒攻击。

旁路控制　即为了获得非授权的权利或特权，某些攻击者会研究发觉系统的缺

陷或安全性上的薄弱之处。例如，攻击者通过各种手段发现原本应保密但却又暴露出来的一些系统“特征”，再利用这些“特征”就可以绕过防线守卫者侵入到系统内部。

授权侵犯 即被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权的目的，也称为“内部攻击”。

主要的植入威胁有：

特洛伊木马 即软件中含有一个察觉不出的或者无害的程序段，当它一旦被执行，就会破坏用户的安全性。例如，一个外表上具有合法目的的软件应用程序组，它还具有一个暗藏的目的，就是将用户的文件复制到一个隐藏的秘密文件中，这种应用程序就被称为特洛伊木马。此后，植入特洛伊木马的那个攻击者就可以阅读到该用户的文件。

陷阱门 即某个系统或其部件中设置“机关”，使得当提供特定的输入数据时，允许违反安全策略。

（3）潜在威胁

如果在某个给定环境中对任何一种基本威胁或主要的可实现的威胁进行分析，我们就能够发现某些特定的潜在威胁，而任意一种潜在威胁都可能导致一些更基本的威胁发生。例如，考虑信息泄露这样一种基本威胁，我们可能找出以下几种潜在威胁：窃听、业务流分析、操作人员的不慎重导致的信息泄露、媒体废弃所导致的信息泄露。

网络通信中，主要的安全防护措施被称为安全业务。使用的有下列五种：

认证业务 即提供某个实体（人或系统）的身份的保证；

访问控制业务 即保护资源以防止对它的非法使用和操纵；

保密业务 即保护信息不被泄露或暴露给非授权的实体；

数据完整性业务 即保护数据以防止未经授权的增删、修改或替代；

不可否认业务 即防止参与某次通信交换的一方事后否认本次交换曾经发生过。

由于网络攻击的破坏性强，影响范围大，断定难度大，因此对网络服务质量和安全造成了严重的威胁。又由于 TCP/IP 协议的不完善、UDP 协议的不可靠以及计算机程序的错误，造成了网络上的许多漏洞。但这并不是说，我们面对这些问题束手无策，借助完善严密的管理制度、科学有效的技术方法，可以尽可能降低危险，做到防患于未然。

网络安全管理中最重要的是建立健全网络安全使用规则、安全策略、应急对应方案，确定网络安全工作的目标和对象，控制用户的访问权限，制定网络安全责任书，专机专用，对疏于防范和有泄密嫌疑的用户，应依据相关条款给予相应的处理。虽然现在用于网络安全防护的产品很多，但是黑客仍无孔不入，对社会造成了严重的危害。因此，掌握、利用网络技术给人们带来方便的同时，又能使信息安全得到

保证，这将是新一代网络管理人员的目标。

计算机网络的安全管理不仅要看所采用的防范措施，而且还要看它所采取的管理措施和执行计算机安全保护法律、法规的力度。只有将两者紧密结合，才能使计算机网络安全得到真正的保障。加强对计算机用户的安全教育、建立相应的安全管理机构，不断完善和加强计算机的管理功能、计算机及网络的立法和执法力度，提高计算机用户的安全意识等，对防止计算机犯罪、抵制黑客攻击和防止计算机病毒干扰，都是十分重要的措施。

计算机网络的安全管理防范措施中，防范措施和管理措施非常重要，但技术措施是最直接、最常用和最有效的屏障。技术保障策略主要有如下几种：

（1）物理防御措施。如保护网络关键设备，建立科学先进的机房内环境，注意防火、防雷、防辐射、防潮和保证持续供电等。

（2）防火墙技术。防火墙是指一个由软件和硬件设备组合而成，处于企业或网络群体计算机与外界通道之间，限制外界用户对内部网络访问及管理内部用户访问外界网络的权限。防火墙能在内部网络与外部网络之间构造起“保护层”，配置防火墙是实现网络安全最基本、最经济、最有效的安全措施之一。当一个网络接上 Internet 之后，系统的安全除了考虑计算机病毒、系统的健壮性之外，更主要的是防止非法用户的入侵，而目前这种防止的措施主要是靠防火墙技术完成。防火墙能极大地提高一个内部网络的安全性，并通过过滤不安全因素的服务而降低风险。通过以防火墙为中心的安全方案配置，能将所有安全软件配置在防火墙上。目前，技术最为复杂而且安全级别最高的防火墙是隐蔽智能网关，它将网关隐蔽在公共系统之后使其免遭直接攻击。隐蔽智能网关提供了对互联网服务进行几乎透明的访问，同时阻止了外部未授权访问对专用网络的非法访问。

（3）计算机病毒防治。随着计算机技术的发展，计算机病毒也越来越多，尤其在连接互联网的状态下，计算机更容易被病毒入侵。虽然大部分用户都安装了杀毒软件，但杀毒过程本身是被动的，因为只有发现病毒后，利用杀毒软件对其剖析、选取特征串，才能找到该“已知”病毒的解决办法，一旦发现新病毒或变种病毒时，要再次对其进行剖析、选取特征串，才能找到新的解决办法。杀毒软件不能检测和消除研制者未曾见过的“未知”病毒，甚至对已知病毒的特征串稍作改动，它就可能无法检测这种病毒或在杀毒时出错。有些用户的计算机上虽然安装了杀毒软件，但仍经常被病毒攻击，其原因一方面是发现病毒时，该病毒可能已经流行起来或已经造成破坏；另一方面，就是管理上的问题，许多人并不是警钟常鸣，也不可能随时随地去执行杀毒软件，只有发现病毒问题时，才用工具检查，这就难免因一时疏忽而使计算机被病毒攻击。因此，首先，必须为计算机安装杀毒软件，并且更新病毒库的速度要尽量跟上病毒变异的速度；其次，使用者要注意在连网的情况下，不要随便打开来历不明的网站地址和邮件；最后，对重要数据做好备份。

（4）虚拟专用网（VPN）技术。VPN是目前解决信息安全问题的一个较新较成功的技术课题之一，所谓虚拟专用网（VPN），技术就是在公共网络上建立专用网络，使数据通过安全的加密管道在公共网络中传播，即以公用开放的网络作为基本传输媒体，通过加密和验证网络流量来保护在公共网络上传输的私人信息不会被窃取和篡改，从而向最终用户提供类似于私人网络（Private Network）性能的网络服务技术。在公共通信网络上构建VPN有两种主流的机制，这两种机制分别为路由过滤技术和隧道技术。目前VPN主要采用了如下四项技术来保障安全：隧道技术（Tunneling）、加解密技术（Encryption & Decryption）、密钥管理技术（Key Management）和使用者与设备身份认证技术（Authentication）。其中几种流行的隧道技术分别为PPTP、L2TP和Ipsec。VPN隧道技术能提供不同层次的安全服务，这些安全服务包括不同强度的源鉴别、数据加密和数据完整性等。在网络层可以通过在路由器上配置MPLS VPN协议实现，在接入层可以通过在用户终端增加VPN设备或在计算机上建立VPN连接来实现。VPN也有几种分类方法，如按接入方式分为专线VPN和拨号VPN，按隧道协议可分为第二层的和第三层的，按发起方式可分为客户发起的和服务器发起的。

（5）密码技术。包括加密与解密技术。加密是网络与信息安全保密的重要基础。它是将原文用某种既定方式规则重排、修改，使其变为其他程序读不懂的密文。解密则是将密文根据原加密的方法还原。密码技术是信息安全核心技术，密码手段为信息安全提供了可靠保证。密码的数字签名和身份认证，是当前保证信息完整性的主流方法之一。密码技术主要包括古典密码体制、单钥匙密码体制、数字签名以及密钥管理。目前，已成熟的加密方法有很多，如替换加密、移位加密、一次性密码本加密、序列密码加密等。

（6）数字签名。对于网络上传输的电子文档，可使用数字签名的方法来实现内容的确认。签名有两个关键问题，一是签名不能被仿照，二是签名必须与相应的信息捆绑在一起，保证该信息就是签名欲确认的对象，以解决伪造、抵赖、冒充和篡改等安全问题。数字签名采用一种数据交换协议，使得收发数据的双方都能够满足两个条件：接受方能够鉴别发送方的身份；发送方不能否认他发送过数据这一事实。数据签名一般采用不对称加密技术。发送方对整个明文进行加密变换，得到一个值，将其作为签名。接收者使用发送者的公开密钥对签名进行解密运算，如其结果为明文，则签名有效，也证明对方的身份是真实的。

（7）鉴别。鉴别的目的是验明用户或信息的“正身”。对实体声称的身份进行唯一识别，以便验证其访问请求，或保证信息来源以验证消息的完整性，进而有效地对抗非法访问、冒充、重演等威胁。按照鉴别对象的不同，鉴别技术可以分为消息鉴别和通信双方相互鉴别；按照鉴别内容不同，鉴别技术可以分为用户身份鉴别和消息内容鉴别。

（8）网络访问控制策略。访问控制是网络安全防范和保护的主要策略，其任务是保证网络资源不被非法使用和访问。一般采用基于资源的集中式控制、基于资源和目的地址的过滤管理以及网络签证等技术来实现。访问控制策略包括入网访问控制、操作权限控制、目录安全控制、属性安全控制、网络服务器安全控制、网络监测、锁定控制和防火墙控制策略七个方面的内容。

（9）扫描器。扫描器是一种能自动检测远程或本地主机安全性弱点（漏洞）的程序，它能查询 TCP/IP 各种服务的端口，并记录目标主机的响应，收集关于某些特定项目的有用信息。这项技术的具体实现就是安全扫描程序。扫描程序可以在很短的时间内查出现存的安全薄弱点，开发利用可得到的攻击方法，并把它们集成到整个扫描中。扫描以统计的格式输出，便于参考和分析。一个好的扫描器相当于一千个口令的价值。对于管理员来说，扫描器是一种网络安全性评估软件。安全扫描技术与防火墙、安全监控系统互相配合便能够提供高安全性的网络。

目前流行的扫描器有：NSS 网络安全扫描器；stroke 超级优化 TCP 端口检测程序(可记录指定机器的所有开放端口)；SATAN 安全管理员的网络分析工具；JAKAL；XSCAN。

1.1.2 无线传感器网络安全

1. 无线传感器网络的特点及问题

无线传感器网络作为一种新型的无线网络，在组成及应用场景与传统网络有较大的不同，它集合传感器技术、计算机技术、信息处理技术和通信技术于一体。主要特点有：

（1）以数据为中心。无线传感器网络中节点数量巨大，并且由于网络拓扑的动态特性和节点放置的随机性，节点并不需要也不可能以全局唯一的 IP 地址来标识，只需使用局部可以区分的标号标识。用户对所需数据的收集，是以数据为中心进行，并不依靠节点的标号。同时，在应用过程中不可更换电池，因此能量也相当受限。

（2）传感器节点的微型化，资源受限。无线传感器网络中，节点只具有有限的硬件资源，其计算能力和对数据的存储、处理能力相当受限，使其不能进行复杂的计算。传统 Internet 网络上成熟的协议和算法对无线传感器网络而言“开销”太大，难以使用。此外，节点只能携带有限的电池能量，并且由于物理限制难以给节点更换电池，所以传感器节点的电池能量限制是整个无线传感器网络设计过程中最关键的约束之一，它直接决定了网络的工作寿命。

（3）部署方式。无线传感器网络通常工作在人类难以接近或危险的区域内，为了对一个区域执行监测任务，往往有成千上万的传感器节点部署到该区域，因此无