无线传感器网络Sybil攻击安全防卫技术

WUXIAN CHUANGANQI WANGLUO
SYBIL GONGJI ANQUAN
FANGWEI JISHU

王伟 编著

国防工业出版社
National Defense Industry Press

无线传感器网络Sybil攻击安全防卫技术

王伟 编著

国防工业出版社

·北京·

图书在版编目（CIP）数据

无线传感器网络 Sybil 攻击安全防卫技术／王伟编著.
—北京：国防工业出版社，2013.4
ISBN 978-7-118-08704-8

Ⅰ.①无… Ⅱ.①王… Ⅲ.①无线电通信-传感器-安全技术 Ⅳ.①TP212

中国版本图书馆 CIP 数据核字(2013)第 068183 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 880×1230　1/32　**印张** 5¼　**字数** 149 千字
2013 年 4 月第 1 版第 1 次印刷　**印数** 1—2000 册　**定价** 30.00 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

前　言

无线传感器网络(Wireless Sensor Network)是当今国内外备受关注的一项新兴技术,它是在聚合了计算机技术、通信技术和传感器技术三大支柱技术之后应运而生的。无线传感器网络具有十分广阔的应用前景,在环境监测、地震监测、医疗监护、城市交通管理、货运管理、军事侦察、仓储管理等诸多领域都有着重要的科研价值和巨大的市场价值。美国的《技术评论》杂志在2003年的一篇文章中论述未来最具有研究价值的新兴十大科学技术的时候,排名第一的就是无线传感器网络。无线传感器网络是由数量众多的传感器节点通过无线通信技术以自组织方式构成网络。但是目前在无线传感器网络的研究中仍有许多问题没有解决,例如:路由协议、定位技术、网络安全等。本书针对无线传感器网络的安全问题,主要围绕着无线传感器网络在Sybil攻击情况下,系统采取的有效检测机制和安全定位方法。

本书共分6章,主要内容安排如下:

第1章无线传感器网络概论。本章对无线传感器网络的定义、基本特点、组成结构、国内外研究现状、应用情况进行了概述和总结,并且对无线传感器网络研究的关键问题,特别是安全问题进行了描述和分析。

第2章无线传感器网络安全技术。本章对网络安全技术的基本问题、研究方法进行了阐述,针对无线传感器网络的典型攻击模型进行了分析,特别是对Sybil攻击进行深入的研究。

第3章无线传感器网络节点定位技术。传感器网络技术主要依赖节点位置建立网络的空间关系,从而报告监测事件,然而由于传感器网络主要应用在无人值守的敌对环境下,网络节点的定位很容易被

敌方攻击，这种脆弱性决定了安全问题在定位过程中的重要性。本章对定位技术的原理和分类进行了介绍。

第4章基于RSSI的Sybil攻击安全定位技术。本章研究在Sybil攻击下的传感器网络节点安全定位机制，分析了传感器网络节点定位系统可能受到的安全攻击和安全需求。基于RSSI解决Sybil攻击的方法不会增加WSN的负担，利用两个接收节点进行分析，比较两个接收节点的RSSI比率，以此来解决RSSI时间不一致性的问题。仿真结果表明，提出的检测方法具有可靠的安全性。

第5章基于Sybil攻击的可信路由技术。在通信网络中路由算法是网络层核心问题，其主要功能是指引分组通过子网到达正确目的节点。从算法思想的总体结构出发，考虑到节点信任度评价及Sybil攻击参数对路由的建立、路径的选择及数据传输的影响。仿真表明改进算法在Sybil攻击下具有良好的安全性。

第6章基于Sybil攻击的容忍入侵技术。入侵容忍系统是第三代的网络安全技术，研究系统在已经遭受到入侵的情况下，如何能有效地屏蔽或遏制入侵所造成的破坏。Sybil攻击容忍算法是利用节点定位系统中存在冗余参照信息的特点，用方差的无偏估计作为安全性检验的依据，利用基于最小安全参照集预测残差，逐个诊断剩余参照数据是否异常，提高定位系统容忍攻击的能力。

在此，向本书中出现的所有参考文献作者以及为本书出版付出辛勤劳动的同志表示衷心的感谢！

限于作者的水平，书中难免会有许多缺点和不完善之处，恳请广大专家、同行予以批评指正。

作 者

2012年12月

目　录

第1章　无线传感器网络概论

1.1　无线传感器网络

现代信息技术的三大支柱是传感器技术、通信技术和计算机技术，三种主要技术分别完成了对于被测量对象的信息提取、信息传输以及信息处理，随着信息科学技术的高速迅猛发展，信息的传输与信息处理技术目前已经在研究领域内取得了突破性进展。在当前快速发展微电子技术并且使其逐步走向成熟的大环境下，现代传感器技术也朝着微型化、集成化、智能化和多元化的方向不断发展前行。随着应用领域不断向前地全面发展，无线传感器网络（Wireless Sensor Network）技术也在飞速发展，但是在其信息采集技术上还有很多技术难点，例如：布线困难、采集范围大、采集点众多等诸多问题。如果采用传统的解决方案，网络可以采用总线方式组网，会使传感器技术很难适应当前的应用要求。在这样的大环境背景下，聚合了以上提到的计算机技术、通信技术和传感器技术三大支柱技术，无线传感器网络技术应运而生了。采用无线通信技术由大量传感器节点组成的网络就称为无线传感器网络。无线传感器网络是信息技术发展的一个新领域，集数据的采集、传输以及融合分析于一体，在环境监测、地震监测、医疗监护、城市交通管理、货运管理、军事侦察、仓储管理等诸多领域中都具有非常广阔的应用前景[1]。

在传感器网络的初早期，第一代传感器是指某个网络将传感器运用点对点进行信息的传输以及信息通信的过程。第二代传感器网络是在第一代传感器的基础上，融合了传感器技术和计算机技术，获取外界多种信息信号以及对多种信号的综合处理能力正是这种多技术

的融合让传感器网络所具备的。通过连接传感控制器，传感器网络组成一个具备有综合各种信息和处理信息能力的网络。现场总线技术从20世纪末开始得到应用，被研发者应用于传感器网络，成为组建和构建智能化传感器网络的一项关键技术，网络系统通过使用无线技术被连接起来，在网络中大量运用多功能传感器，从而无线传感器网络就逐渐形成了。

下一代新兴的传感器网络就是无线传感器网络，这个提法在1999年最早出现，是在一篇题为“传感器走向无线时代”的具有代表性的文章中论述的。随后在具有权威性的美国的国际移动计算和网络会议上，研究者也提出了：21世纪人类面临的最具发展机遇的技术之一就是无线传感器网络，由此可见无线传感器网络技术受到的关注程度。美国国内的《技术评论》杂志在2003年的一篇文章中论述未来最具有研究价值的新兴十大科学技术的时侯，排名第一的就是无线传感器网络。美国《商业周刊》在2003年举办的新兴技术的研究专题中，阐述了四大新技术，无线传感器网络同其他三种新技术一样被列在其中。美国《今日防务》杂志主要刊登和报道美国军事领域的讯息，它也前瞻性地认为：随着无线传感器网络在实际应用中的不断发展和全面完善，必将引发一场划时代的技术变革，不论是在军事技术还是在民用技术方面都会起到不可估量的作用。在接下来的一年，《IEEE Spectrum》杂志专门发表了一期被称为“传感器的国度”的专题，在这个专集里，研究者从多个角度论述了无线传感器网络的蓬勃发展和可能产生的广泛深入应用。从以上各个研究刊物所刊登的有关传感器网络的报道和论述，不难想象无线传感器网络对人类社会的方方面面都会带来深远的影响和巨大的变革[2,3]。

无线传感器网络是一种由部署在测量区域内大量的智能的传感器节点通过无线通信的方式，形成一个多跳的自组织网络系统构成的网络应用系统，大量传感器节点密集分布在监控区域内。无线传感器在无线网络覆盖区域中传感器之间协作地互相感知，在任意时刻，节点间连接是通过无线信道，采用对等（Peer to Peer）、多跳（Multi-hop）

等通信方式，自组织网络拓扑结构，传感器节点间协同能力很强，通过对数据局部采集、预处理以及节点间的数据交换从而完成网络检测数据，采集以及处理传感器感知对象的信息，并且把感知到的信息发送给接受信息的观测者。

在系统目标内部所存在的数量众多的位置处以毗邻或处于待监测状态的传感器节点组成了无线传感器网络。在无线传感器网络中，传感器节点的功能就是其组成部分采集数据、处理信号以及传输信号等。对于某些应用，由于具体位置无需精确部署，传感器节点可以采用火炮发射、飞机播撒等方式放置，并且传感器节点经常处于无人值守的状态。由于传感器节点可能被部署在环境恶劣的区域或地区，因此，无线传感器网络必须具有良好的抗袭击或抗毁的能力，而且抗袭击或抗毁能力不仅是对单一的传感器节点而言，其含义还包括如果网络中的一些节点损坏，可以利用其他节点完成信息采集、处理和传输，也就是传感器节点的高冗余度带来传感器网络的高抗毁能力。自组织网络协议和算法使传感器网络可以顺利地完成上述工作。此外，由于无线传感器网络的节点数量巨大，所以传感器节点的成本必须尽可能的低。同时无线传感器网络的工作环境和工作方式也决定了传感器节点必须功耗低、体积小、工作时间长。

1.2 无线传感器网络组成结构

在无线传感器网络中，节点是网络的基本组成元素，它具有传感器功能、信号处理功能以及无线通信功能，在网络中的数据传输过程中，节点既是系统信息包的发送者，同时也是系统信息包的转发者。节点通过网络进行自组织和路由的传输，把数据向网络中的网关发送。然后网关可以通过多种通信方式与外部的网络联系，例如：卫星、移动通信网络、互联网等，如果是对于大规模的实际应用，那么在网络中将会有多个网关进行通信工作。

无线传感器网络典型的体系结构见图 1 - 1。

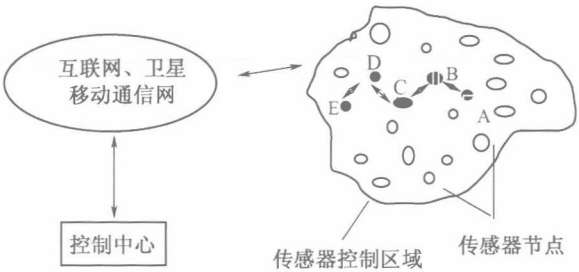

图 1-1　一个典型的传感器网络体系结构

无线传感器网络的最基本组成就是传感器节点。目前，国内外已经出现了许多种无线传感器网络节点的设计，例如美国 Crossbow 公司和 Dust 公司等，其中 Crossbow 公司已经推出了 Mica 系列传感器网络产品，目前已经有了 Mica、Mica2、Mica2Dot 等产品，图 1-2 所示是 Mica2 传感器节点。

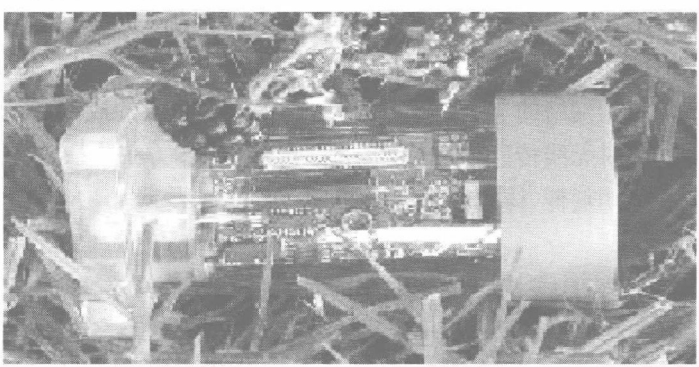

图 1-2　Mica2 传感器节点

Dust 公司已经设计了最终能够悬浮在空气中的传感器，称为“智能微尘”(SmartDust)，现已设计出的全功能“智能微尘”的直径只有 5mm 左右，该公司计划设计出直径小于 1mm 的传感器产品。图 1-3 所示就是 SmartDust“智能微尘”传感器节点。

在不同应用中，传感器网络节点组成不尽相同，但其组成的基本原理是相同的，基本的无线传感器网络节点一般是由 4 个部分组成：

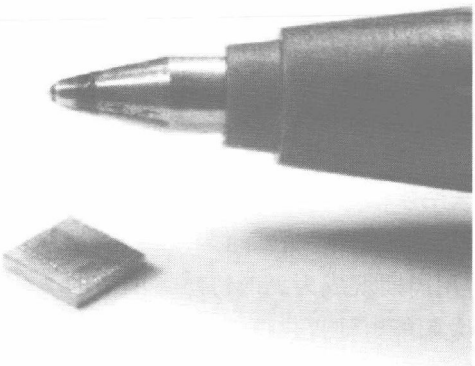

图 1-3　SmartDust 传感器节点

第一部分是传感器模块，第二部分是处理器模块，第三部分是无线通信模块，第四部分是能量供应模块，如图 1-4 所示。

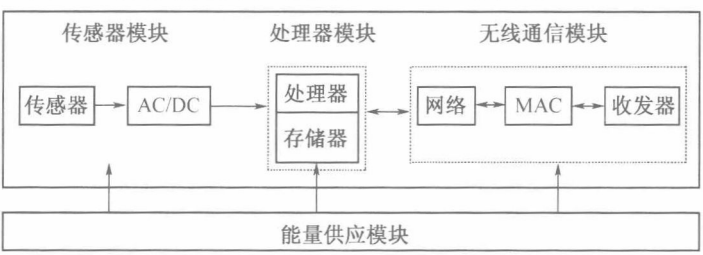

图 1-4　传感器节点体系结构

在整个系统结构中，传感器模块的主要功能是，对周围自身环境以及目标对象进行数据采集和转换。模块还会根据实际应用需求的不同附加一些相关组件，例如：位置发现系统、能量发生器和协调单元等。传感单元主要由传感器和模拟数字转换器两个子单元组成。传感器首先采集信息，然后将模拟信号传送给模拟数字转换器，转换为数字信号，然后再传送给处理单元。

处理器模块的主要功能是，对整个无线传感器网络节点的控制和管理，对传感器采集到的数据信息和由其他节点发送过来的数据进行处理和分析操作，其中还包含高层网络协议的运行过程。其结构一般

是由嵌入式系统构成，包括 CPU 处理器、存储器等。

无线通信模块的主要功能是，负责与其他传感器节点进行通信，使网络信息互联。根据数据传送距离的不同，采用的通信模块的协议和电路也有不同的种类。

能量供应模块的主要功能是，为无线传感器节点提供其所需要的能量，通常采用体积较小、工作时间长的微型电池。但是对于某些应用的传感器节点的能源一般是不能更换的，所以设计有效的方法来延长网络的应用周期就成为无线传感器网络的一个核心问题。从理论上讲，运用太阳能电池提供能量就能持久地补给能源，但在工程实践中生产这种微型化的太阳能电池还有很大的难度，所以节能是传感器节点中非常重要的部分。

正是有着与一般的无线网络不同的特点，所以传统的无线网络协议不能盲目地照搬，其并不适用于无线传感器网络。那么目前研究无线传感器网络的主要问题有：物理层通信、路由协议、跟踪技术、节点定位、能量消耗、时间同步、网络拓扑结构、安全防护等。首先简单地介绍无线传感器网络各层的研究问题。

如图 1 - 5 所示，整个协议主要由物理层（Physical Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）和应用层（Application Layer）组成，其中还包括任务管理平台（Task Management Plane）、移动管理平台（Mobility Management Plane）和能量管理平台（Power Management Plane）。

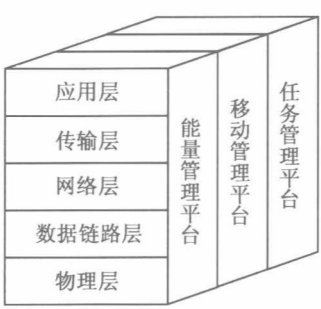

图 1 - 5　传感器网络协议

（1）物理层。由于传感器节点之间通过无线媒介通信，那么在无线通信信道中就会产生路径衰落、多径、散射和障碍物吸收等问题，这样通信信号就会受到影响，而且还会增加节点的能量消耗，那么物理层研究的主要方向就是怎样对传输信道进行建模。在物理层中的调制机制也非常重要，它的可靠性将会影响整个无线传感网络能否正常通信，在文献[4,5]中对此项技术进行了深入的研究。

（2）数据链路层。传感器节点在无线传感器网络中是以广播形式进行通信的，但是由于传感器节点的通信距离是有限的，所以其广播的范围也是有限的，因此就要考虑到访问的公平性和可靠性，那么在数据链路层中减少数据冲突，从而使无线信道正常工作是考虑的主要问题之一。目前对数据链路层的研究主要集中在有以下几个方面：如何解决隐藏终端和暴露终端的问题[6]，采用多信道的方法来解决终端暴露以及数据传输冲突的问题，在退避时钟和竞争窗口等参数进行调整的情况下，怎样使其性能获得提升，如针对节点的能耗问题，提出高性能、低功耗的算法。

（3）网络层。在网络层中，其主要的功能就是实现路由机制。无线传感器网络的主要功能就是在监测区域内收集所需要的信息，并且对信息进行传输、处理，作出相关的决策，那么能否把这些采集到的数据安全、高效地传送到基站就是一个关键技术。由于数据广播模式的不同，通信方式主要为单播、广播和多播协议，即存在简单的单条路由以及复杂的多条路由，所以在数据的传输过程中以及数据聚集的功能设计中要节省其能量消耗。

（4）传输层。传输层的作用是维护应用层中传感器网络应用要求的数据流。传输层利用网络层提供的服务，通过传输层地址提供给高层用户传输数据的通信端口，使系统间高层资源的共享不必考虑数据通信方面和不可靠的数据传输方面的问题。它的主要功能是：对一个进行的对话或连接提供可靠的传输服务，在通向网络的单一物理连接上实现该连接的复用，在单一连接上提供端到端的序号与流量控制、差错控制及恢复等服务。

（5）应用层。在应用层中，针对特定的应用服务，进行信息采集、数据处理以及查询等功能。不同的应用场合和要求，对实际系统中的传感器采集模块和数据处理模块的要求也不尽相同。

1.3 无线传感器网络的关键问题

对于无线传感器网络的应用，其性能和可用性至关重要。下列几条是评价无线传感器网络性能的标准，目前还没有达到实用阶段，还需要进一步地模型量化。

（1）能源有效性。无线传感器网络的能源有效性是指，该网络在有限的能源条件下能够处理的数据量。能源有效性是无线传感器网络在无人值守、严酷条件下应用的一项重要性能指标。

（2）生命周期。无线传感器网络的生命周期是指，从无线传感器网络启动到不能提供需要的信息为止所持续的时间，也就是无线传感器网络的应用寿命。

（3）时间延迟。无线传感器网络的延迟时间是指，当主机发出请求到接收到采集信息所需要的时间。

（4）感知精度。无线传感器网络的感知精度是指，观察者接收到的采集信息的精度，包括位置精度、信息精度等。传感器的精度、信息处理算法、网络通信协议等都会对精度产生影响。感知精度、时间延迟和能量消耗之间具有很大的相关性。

（5）可扩展性。无线传感器网络的可扩展性主要表现在传感器数量扩展、网络覆盖区域扩展、生命周期延长、时间延迟缩短、感知精度提高等方面的可扩展极限。对于可扩展性级别，无线传感器网络必须提供出支持该可扩展性级别的机制和方法。

（6）容错性。由于无线传感器网络的应用环境或其他原因，物理维护或者替换已经失效的传感器节点常常是十分困难的。这样无线传感器网络的软件、硬件应该具有很强的容错性，从而保证系统具有很好的运行稳定度。

根据前面的介绍，了解了无线传感器网络中最基本的问题。根据无线传感器网络的特点、应用要求、实际问题，目前主要的研究方向如下。

（1）能量问题。能量是无线传感器网络中最为稀缺的资源，因此节能问题贯穿网络的各个层次。节点的能量十分有限，所以要求算法应该尽可能地节能。因为传感器节点传输数据时所消耗的能量大大高于将数据在本地进行计算所消耗的能量，如果传感器节点将 1Kb 的数据传输 1m，消耗的能量足够节点在本地进行 3000 次命令运算。由此可见，如果能够尽量减少节点对数据的传输，就能够减少节点在通信上能量的消耗。目前降低数据传输路由长度，是设计无线传感器网络相关算法的重要思路之一。当然在无线传感器网络中减少电路能耗、减少相关运算量、启动空闲待机机制等也都是提高能量利用率的方法。

（2）定位问题。定位是大部分应用的基础。如果节点需要进行自身定位，最直接的方法就是运用 GPS（Global Positioning System）技术，GPS 可以通过卫星对节点进行快速、准确的定位，正是由于 GPS 系统需要卫星的技术支持，从而造成了其结构比较复杂，而且成本较高，那么就限制了大规模无线节点的应用。所以在无线传感器网络的定位算法当中，常常对节点进行联合定位。文献[7]对节点定位算法进行了综述，而且进行了详细的性能比较。

（3）网络拓扑问题。无线传感器网络的拓扑技术主要分为两个方面：拓扑发现和拓扑控制。其中拓扑发现包括传感器节点地理信息的路由和传感器节点空洞的发现；而拓扑控制包括无线网络覆盖拓扑和无线网络连接拓扑，主要考虑在静态网络、动态网络和混合型网络的情况下，网络的覆盖和连通状态，而能量控制和管理机制主要通过网络的连接拓扑来分析[8]。

（4）时钟同步问题。目前在所有的分布式系统中，时钟同步都是一个非常重要的问题。研究时钟同步对于无线传感器网络尤为重要。首先，无线传感器网络的任务非常复杂，往往是由网络内的