山东女子学院优秀学术著作出版基金资助

The Study on Security Problems of Wireless Sensor Networks

无线传感器网络安全问题研究

张玉泉 / 著

山东人民出版社
国家一级出版社 全国百佳图书出版单位

The Study on
Security Problems of Wireless Sensor Networks

无线传感器网络安全问题研究

张玉泉 / 著

山东人民出版社

图书在版编目(CIP)数据

无线传感器网络安全问题研究/张玉泉著. —济南:山东人民出版社,2013.10
ISBN 978-7-209-07862-7

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

中国版本图书馆 CIP 数据核字(2013)第 257105 号

无线传感器网络安全问题研究
张玉泉 著

山东出版集团
山东人民出版社出版发行
社 址:济南市经九路胜利大街 39 号 邮 编:250001
网 址:http://www.sd-book.com.cn
发行部:(0531)82098027 82098028
新华书店经销
山东省东营市新华印刷厂印装

规 格 16 开(169mm×239mm)
印 张 8.25
字 数 130 千字
版 次 2013 年 10 月第 1 版
印 次 2013 年 10 月第 1 次
ISBN 978-7-209-07862-7
定 价 26.00 元

如有质量问题,请与印刷厂调换。(0546)6441693

目 录

第一章 绪论 …… 1

1.1 传感器节点特征 …… 1

1.2 无线传感器网络概念 …… 5

1.3 无线传感器网络体系结构 …… 6

1.3.1 层次型无线传感器网络结构 …… 6

1.3.2 分布式无线传感器网络结构 …… 7

1.4 无线传感器网络特点 …… 8

1.4.1 资源有限 …… 8

1.4.2 大规模的网络 …… 8

1.4.3 自组织的动态自适应网络 …… 9

1.4.4 以数据为中心的网络 …… 9

1.4.5 与应用相关的网络 …… 9

1.5 无线传感器网络发展历史和研究现状 …… 10

1.6 无线传感器网络应用 …… 12

1.6.1 军事应用 …… 13

1.6.2 环境科学 …… 13

1.6.3 医疗健康 …… 14

1.6.4 空间探索 …… 14

1.6.5 其他商业应用 …… 14

1.7 无线传感器网络研究意义 …… 15

1.8 小结 …… 15

1.9 本书研究内容及结构 …… 16
1.9.1 研究内容 …… 16
1.9.2 本书结构 …… 17

第二章 无线传感器网络安全问题 …… 19

2.1 无线传感器网络安全问题提出 …… 19
2.2 无线传感器网络安全需求 …… 20
2.3 无线传感器网络安全算法设计的限制 …… 22
2.3.1 传感器节点本身限制 …… 23
2.3.2 传感器网络本身限制 …… 25
2.4 常见的无线传感器网络攻击方法及其防御技术 …… 28
2.4.1 物理层攻击和防御 …… 28
2.4.2 链路层攻击和防御 …… 30
2.4.3 网络层攻击和防御 …… 32
2.5 小结 …… 37

第三章 分布式无线传感器网络密码管理方案 …… 38

3.1 引言 …… 38
3.2 几种分布式密钥管理方案 …… 40
3.2.1 预共享密钥方案 …… 40
3.2.2 基于随机密钥预分配的密钥管理方案 …… 41
3.3 一种基于 OKS 和网格无线传感器网络对偶密钥预分配方案 …… 44
3.3.1 预备知识 …… 44
3.3.2 预分配密钥方案 …… 46
3.3.3 性能分析 …… 49
3.3.4 安全性分析 …… 50
3.3.5 结束语 …… 50
3.4 一种基于感知区域的分布式密钥管理方案 …… 51
3.4.1 建立基于感知区域的对密钥 …… 51

3.4.2 无线传感器网络性能分析 …… 56
3.4.3 结论 …… 57
3.5 小结 …… 58

第四章 层次式无线传感器网络密码管理方案 …… 59

4.1 引言 …… 59
4.2 几种层次式密钥管理方案 …… 59
4.2.1 基于 KDC 的密钥管理方案 …… 60
4.2.2 非 KDC 的密钥管理方案 …… 62
4.3 一种基于三维感知区域的无线传感器网络密钥管理方案 …… 65
4.3.1 方案的网络结构 …… 65
4.3.2 方案的密码建立 …… 67
4.3.3 性能分析和比较 …… 72
4.3.4 结论 …… 75
4.4 小结 …… 76

第五章 基于 LEACH 无线传感器网络路由协议研究 …… 77

5.1 无线传感器网络路由协议的分类 …… 77
5.2 几种无线传感器网络路由协议介绍 …… 79
5.2.1 泛洪协议 …… 79
5.2.2 SPIN(Sensor Protocol for Information via Negotiation) …… 79
5.2.3 定向扩散 …… 80
5.2.4 SAR 协议 …… 81
5.2.5 GEAR 协议 …… 81
5.3 LEACH 协议算法描述及其优缺点 …… 82
5.3.1 LEACH 算法描述 …… 82
5.3.2 LEACH 算法分析 …… 84
5.4 LEACH 协议的改进方案 …… 85
5.5 改进的无线传感器网络 LEACH 协议 …… 86

5.5.1 改进后的新路由协议 …… 87
5.5.2 LEACH 协议和我们新协议的比较 …… 93
5.5.3 结论 …… 94
5.6 小结 …… 94

第六章 异构无线传感器网络密码管理协议 …… 95

6.1 异构无线传感器网络概念 …… 95
6.2 HWSN 的几种异构性表现形式 …… 96
6.3 关于 HWSN 安全的相关工作 …… 98
6.4 一种异构无线传感器网络密码管理方案 …… 99
6.4.1 分布式密码管理方案 …… 99
6.4.2 异构无线传感器网络性能分析 …… 102
6.4.3 结论 …… 106
6.5 小结 …… 106

第七章 总结和展望 …… 107

7.1 本书总结 …… 107
7.2 本书主要创新点 …… 110
7.3 今后工作展望 …… 111

参考文献 …… 112

CHAPTER 1 第一章

绪 论

1.1 传感器节点特征

网络中的传感器节点兼具普通传感器和无线通信节点的功能，和普通传感器一样，能感受规定的被测量并按照一定的规律转换成可用输出信号。它通常有敏感元件和转换元件组成。它包括：（1）敏感元件是指传感器中能直接（或响应）被测量的部分；（2）转换元件指传感器中能将敏感元件感受（或响应）的被测量转换成可用输出信号的部分[1]。

从传感器技术的发展来看，硅微电子技术的成熟使得在单个芯片中实现复杂结构的微电子机械系统成为现实，也给传感器的微型化提供了基础。同时采用了 IC 技术将信号处理和控制电路集成到单个的芯片中，大大提高了传感器的性能并扩展了传感器的功能，即实现所谓的智能化。对于传感器来说，不仅是简单地改变了加工制造的方法，同时对传统的基于传感器测量的控制系统的设计也带来了深刻的影响。并且对传感器本身的设计方法也带来了变革，使得传感器测量控制系统的设计及构成变得简单容易。与传统的系统相比，更加可靠、便宜，并且扩展性更好。很显然，这些特性的实现主要得益于在传感器内部嵌入微处理芯片。与传统的传感器输出模拟原始信号不同，这种传感器可以实现对原始数据的加工处理，并可以

通过标准的接口与外界实现数据交换[2,3]。

在不同的应用中，无线传感器节点结构不尽相同，一般都有数据采集、数据处理、数据传输和电源四大部分组成[4]。如图1.1所示。数据采集模块由传感器及其信号调理电路、AD转换器件组成，负责监测区域内信息的采集和数据转换，被测物理信号的形式决定了传感器的类型；数据处理模块由存储器、微处理器及其应用系统组成，处理器通常选用嵌入式CPU，如Motorola的68HC16，ARM公司ARM7等，控制整个传感器的操作，存储和处理本身采集的数据以及其他节点发送来的数据；数据传输模块由网络通信及射频模块组成，主要采用低功耗、短距离的无线通信模块，比如RFM公司的TR1000等，主要负责与其他节点或基站进行无线通信，交换控制消息和收发采集数据。

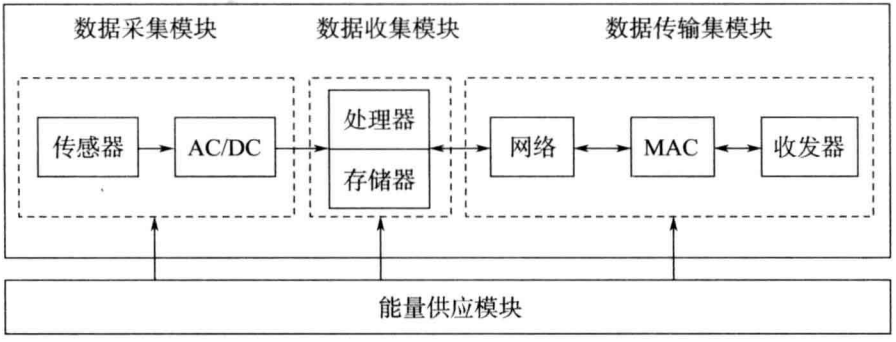

图1.1 传感器节点组成[5]

能量供应模块由电池及电源管理电路等组成，为传感器节点提供运行所必需的能量。

通常情况下节点采用电池供电，一旦电源耗尽，节点就失去了工作能力。为了最大限度地节约电源，在硬件设计方面，要尽量采用低功耗器件，在没有通信任务的时候，切断射频部分电源；在软件设计方面，各层通信协议如果没有特殊的要求都应该以节能为中心，必要时可以牺牲其他的一些网络性能指标，以获得更高的电池效率[5]。

表1.1中列出了一种Berkeley提出的一种名为智能尘埃（SmartDust）节点的特性。

表 1-1　　智能尘埃传感器节点（SmartDust）的特征[5]

CPU	8-bit 4MHz
内存	8KB 指令闪存 512 字节的 RAM 512 字节的 EEPROM
通信	无线 916MHz
带宽	10Kbps
操作系统	TinyOS
操作系统代码空间	3500 字节
有效的代码空间	4500 字节

组成无线传感器网络的节点与 Ad Hoc 等网络有很大不同，并且因为这些差异，造成了无线传感器网络面临很多 Ad Hoc 网络所没有的问题。下面介绍传感器节点的限制因素[6~8]，以期能更好地了解无线传感器网络的特性。

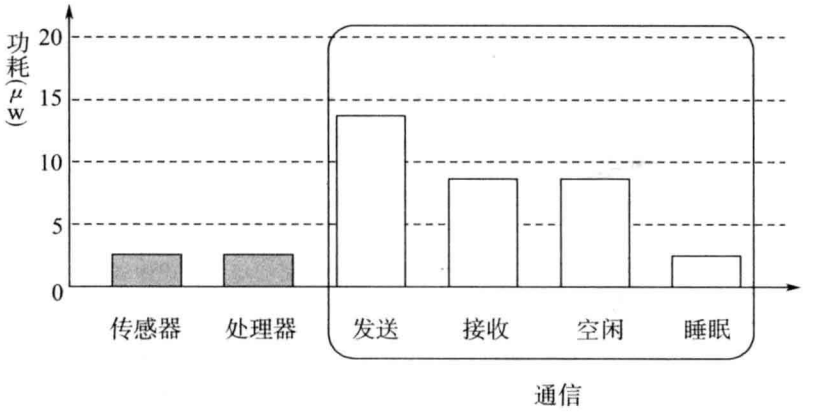

图 1.2　传感器节点各部分消耗能量

（1）电源能量有限。传感器节点消耗能量的模块包括传感器模块、处理器模块和无线通信模块。随着低功耗加工技术的成熟，处理器和传感器模块的能耗可以很低，绝大部分能量损耗在无线通信模块上。Estrin D 在 Mobicom2002 会议上的特邀报告[9]中所描述传感器各个模块消耗能量的情况，如图 1.2[9]所示，传感器节点的大部分能量消耗在无线通信模块。传感

器节点传输信息时要比执行计算时消耗更多的能量，传输 1 比特信息 100m 距离需要的能量大约可以计算 3000 条指令。

无线通信模块存在发送、接收、空闲和休眠四种状态。无线通信模块在空闲状态一直监听无线信道的存在情况，检查是否有数据发送给自己，而在睡眠状态则关闭通信模块，从图 1.2 中可以看出，无线通信模块在发送状态时的能量消耗最大，在休眠状态时最小。

（2）计算和存储能力有限。传感器节点是一种微型嵌入式设备，要求它价格低功耗小，这些限制必然导致其携带的处理器能力比较弱，存储器容量比较小。为了完成各种任务，传感器节点需要完成检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。

随着低功耗电路和系统设计技术的提高，目前已经开发出很多超低功耗处理器。除了降低处理器的绝对功耗以外，现代处理器还支持模块化供电和动态频率调节功能。利用这些处理器的特性，传感器节点的操作系统设计了动态能量管理和动态电压调节模块，可以更有效地利用节点的各种资源。动态能量管理是当前节点周围没有感兴趣的事件发生时，部分模块处于空闲状态，把这些组件关掉或调到更低能耗的休眠状态。动态电压调节是当微处理器负载较低时，通过降低微处理器的工作电压和频率来降低处理能力，从而节约微处理器的能耗[10]。

（3）通信能力有限。无线通信的能量消耗与通信距离的关系为：

$$E = kd^n \qquad (1-1)$$

其中，参数 n 满足关系 $2 < n < 4$。n 的取值与很多因素有关，例如传感器节点部署贴近地面时，障碍物多干扰大，n 的取值就大；天线质量对信号发射质量的影响也很大。考虑诸多因素，通常取 n 为 3[11]。随着通信距离的增加，能耗将急剧增加，因而在满足通信连通度的前提下应尽量减少单跳通信距离。一般而言，传感器节点的无线通信半径在 100m 以内比较适合[12]。

因为传感器节点的能量限制以及网络覆盖区域较大，网络适合于采用多跳传输的路由机制。传感器节点的无线通信带宽有限，通常最多只有几百 kbps 的通信速率。由于节点能量的变化，受高山、建筑物、障碍物等地势地貌以及风雨雷电等自然环境的影响，无线通信性能可能经常变化，频

繁出现通信中断。在这样的通信环境和节点有限通信能力的情况下，设计网络通信机制时要特别考虑满足无线传感器网络的通信需求[13]。

1.2 无线传感器网络概念

无线传感器网络[11,14~19]是由部署在监测区域内的大量低成本、低功耗、具备感知、数据处理、存储和无线通信能力的传感器节点通过自组织方式形成的网络，其目的是协作地采集、处理和传输网络覆盖区域中被感知对象的信息。

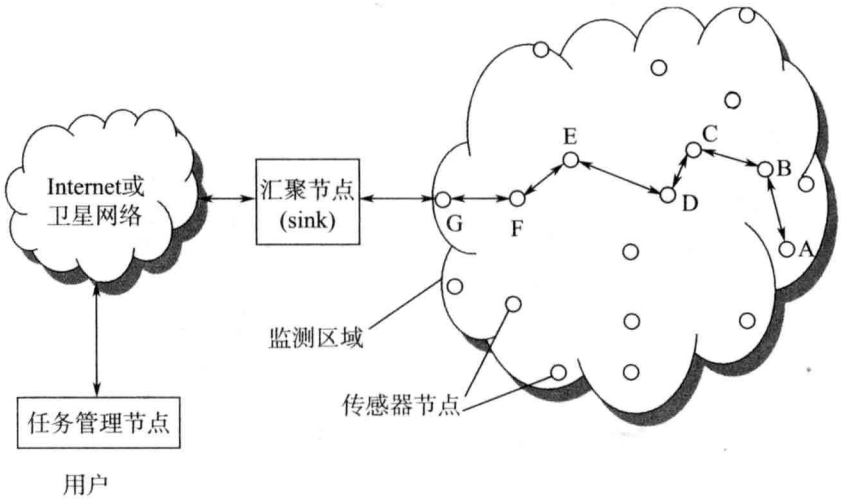

图 1.3 典型无线传感器网络的体系结构示意图[20]

图 1.3 是一个典型无线传感器网络的体系结构。无线传感器网络通常包括传感器节点（sensor node），汇聚节点（sin k node）以及任务管理节点。数量众多的传感器节点通过随机部署或确定部署的方式分布在监测区域内，通过自组织方式形成多跳无线通信网络。传感器节点响应汇聚节点转发的用户对兴趣事件的查询或者按照指令实时收集目标的动态信息，沿某条或多条多跳路径将数据传输给汇聚节点，最后再由汇聚节点通过 Internet 或者卫星网络将数据传送给任务管理节点[20]。

1.3 无线传感器网络体系结构[21~23]

1.3.1 层次型无线传感器网络结构

层次型传感器网络结构如图1.4所示，构成网络的节点种类不同，网络系统通常包括一个或几个功能强大的基站（Base Station）、一些汇聚节点（Sink Nodes）和数目众多的传感器节点（Sensor Nodes），这些不同种类的节点构成一个多层次的网络拓扑。某些特殊情况下，传感器网络还会和卫星通信网及因特网连接，接受任务管理用户的控制[8]。

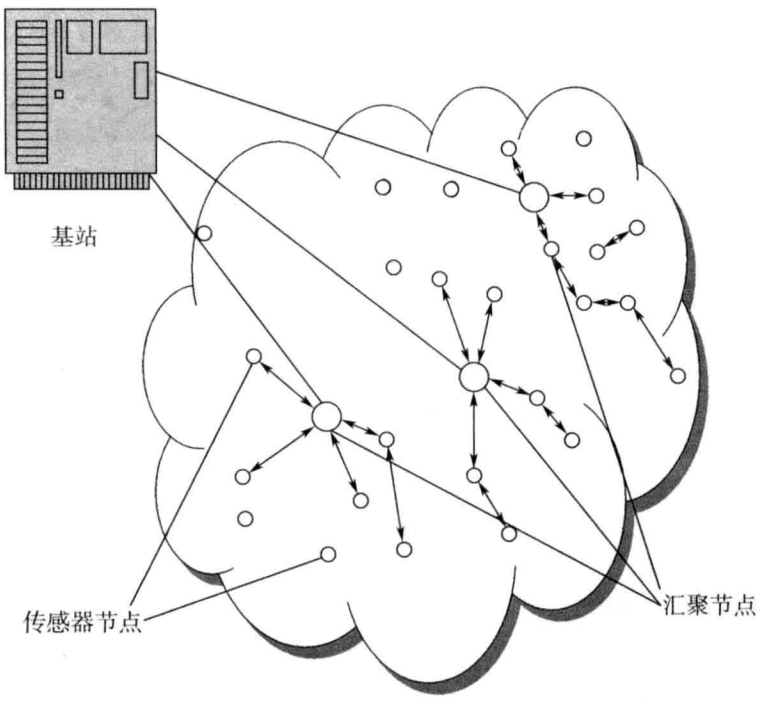

图1.4 层次型传感器网络体系结构[24]

基站是网络中最强大的节点，其物理性能远远超过汇聚节点和传感器节点，基站负责控制网络和收集数据，并在大多数情况下负责安全密钥的产生和分发；镶嵌在网络中的一些中心节点称为汇聚节点，在大多数情况下汇聚节点比普通传感器节点有更强的计算处理能力和更多的内存和储备能量，汇聚节点主要是收集附近节点的数据，处理数据并将主要结果输送到基站；传感器节点是网络中的基本节点，大量的基本节点随机部署在监测区域内通过自组织方式构成通信网络，感知的数据在节点间通过多跳方式由各个基本节点汇流到汇聚节点，经过计算处理最后集中到基站[24]。

1.3.2 分布式无线传感器网络结构

同层次型传感器网络相比，分布式传感器网络没有中心节点（如图1.5所示），只是数目庞大的传感器节点按照一定的部署规则部署后通过自组织方式构成的协同式对等（p2p）网络。

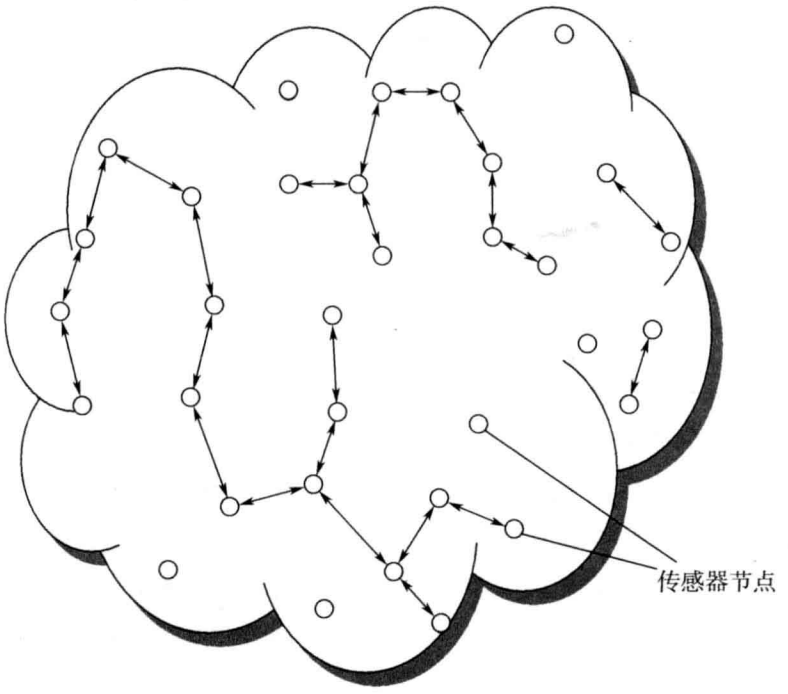

图 1.5 分布式传感器网络体系结构[24]

分布式传感器网络中的主体是传感器节点，传感器节点通常是一个微型的嵌入式系统，它的处理能力、存储能力和通信能力相对较弱，提供能源的是能量有限的电池。从网络功能来看，传感器节点兼顾传统网络的终端和路由器双重功能，即除了信息采集和处理外，还要对其他节点转发来的数据进行存储、计算、融合及转发，同其他节点协作完成整个任务[24]。

1.4 无线传感器网络特点[25~26]

1.4.1 资源有限

传感器节点的资源极其有限，详见表1-2。

表1-2 传感器节点资源有限的表现[27]

受限方面	具体表现
能量有限	不可回收，纽扣电池供电且不可更换，必须高效使用能量。
感应能力	单个节点只有部分感应能力，如加速度、电磁场、声音、光强度等其中的某几个特征，必须充分利用感应数据。
计算能力	存储器一般小于100KB、主频小于1000MHz，但也有128K的，比如Atmega128。
通信能力	节点无线电波的覆盖范围小于100米，一般只有几十kbps的通信带宽，还会有不确定的变化。

1.4.2 大规模的网络

为了提高网络获取更精确的信息，在监测区域通常会部署大量的传感器节点，它们通过无线通信设备连接起来形成网络。大规模体现在两个方面：传感器网络所覆盖的区域较大，传感器节点所部署的密度较大。这样传感器网络可以获得更加真实全面的信息；大量节点采集信息可以提高信息的精度，同时又降低了对单个节点感应数据的精度要求；大规模多节点分布式的部署，冗余节点的存在可以使无线传感器网络具有较强的容错性。

1.4.3 自组织的动态自适应网络

由于无线传感器网络大部分情况下是被随机的部署（比如通过飞机撒布、或由动物携带）到所要观察的对象环境中，这就要求传感器网络节点具有自组织的能力，能够自动进行配置和管理，通过拓扑控制机制和网络协议自动形成信息传输与协作网络。

此外，无线传感器网络的现有的拓扑结构可能会由于外界干扰（环境因素、人为破坏）或电能耗尽造成的传感器节点失效；环境条件或自身条件造成无线链路的带宽发生改变；传感器节点、所观察的对象和观察者都可能改变位置；控制中心动态的人工干预（比如军事上为了防止某些传感器节点落入敌军）；为了有效利用能量延长节点寿命，使节点动态的加入或退出。这都要求无线传感器网络具有动态的自适应能力[28]。

1.4.4 以数据为中心的网络

一般的网络，网络设备以及其他资源都是靠网络中唯一的 IP 地址来定位的方式不同，传感器网络是事件、任务型的网络，脱离传感器网络谈单个节点是没有意义的。无线传感器网络中的节点编号是否唯一，取决于具体的网络通信协议的设计。无线传感器网络的上层应用只是告诉网络它所关心所监测的区域是否有某个事件发生，或者由网络主动地将某个事件的发生通知上层应用，用户不会将某个查询任务给某个节点。这样通过数据信息来进行查询或交流的方式决定了无线传感器网络是一个以数据为中心的网络。

1.4.5 与应用相关的网络

传感器网络是通过节点的感应模块来感知某些物理量，根据这些物理量的特征来判断某种事件的发生或某些现象的变化。但是，由于现实中物理量很多，每个传感器网络的要求不可能都是相同的，而是需要根据特定应用的具体特征来决定使用更好的机制与手段构筑系统。

1.5 无线传感器网络发展历史和研究现状

无线传感器网络[8,29~30]集成了传感器技术、微机电系统（Micro-Electro-Mechanism System，MEMS）技术、无线通信技术和分布式信息处理技术。从上个世纪90年代开始出现到现在，传感器网络从最初的节点研制，到网络协议设计，到智能群体的研究，已成为国际上一个新的IT热点技术，吸引了大量的学者对其展开了各方面的研究，并取得了一些进展（包括众多的节点平台和大量的通信协议），但还没有形成一套完整的理论和技术体系来支撑这一领域的发展，还有众多的科学和技术问题尚待突破，是信息领域具有挑战性的课题。对无线传感器网络的基础理论和应用系统进行研究，开发具有自主产权的系统具有重要的学术意义和实际应用价值。

根据研究侧重点的不同，把无线传感器网络从20世纪90年代开始到现在的发展历程分为三个阶段。第一阶段主要致力于小型化、功耗低、低成本的传感器节点的开发和研制，出现了众多的传感器节点；第二阶段则是把无线传感器网络作为通信网络研究其特性，主要是数据链路层的MAC协议和网络层的路由协议；第三阶段侧重于无线传感器网络群体智能行为的研究。目前的研究正处于第二、第三阶段。

第一阶段的研究主要来自美国军方和自然基金委资助的一些项目，开发了许多传感器节点和研究平台，代表性的节点有UCLA和Rockwell自动化中心研制的WINS节点，MIT研制的μAMPS节点，UC Berkeley的Smart Dust节点和Motes节点。在这些平台中，Motes硬件平台及其配套的TinyOS操作系统最为广泛，为全球400多家研究机构所采用。第一阶段也对无线传感器的通信协议进行了一些研究和设计，主要是将Ad-hoc网络中的相关协议（比如802.11等）进行改进，增加对能耗有效性的支持。

1987年美国国防部高级研究计划署（the Defense Advanced Research Projects Agency，DARPA）在宾夕法尼亚匹兹堡的卡内基-梅隆大学（Carnegie-Mellon University in Pittsburgh，Pennsylvania）主办分布式传感器网络研讨会[31]。由于军事防御系统的需要，提出对传感器网络的通信与计算之间的