第 5 章　无线传感器网络安全

5.1　无线传感器网络安全概述

随着传感器、计算机、无线通信及微机电等技术的发展和相互融合，产生了无线传感器网络(Wireless Sensor Network，WSN)，目前 WSN 的应用越来越广泛，已涉及国防军事、国家安全等敏感领域，安全问题的解决是这些应用得以实施的基本保证。WSN 一般部署广泛，节点位置不确定，网络的拓扑结构也处于不断变化之中。

另外，WSN 节点在通信能力、计算能力、存储能力、电源能量、物理安全和无线通信等方面存在固有的局限性，WSN 的这些局限性直接导致了许多成熟、有效的安全方案无法顺利应用。正是这种“供”与“求”之间的矛盾使得 WSN 安全研究成为热点。

5.1.1　无线传感器网络安全问题

1. 无线传感器网络与安全相关的特点

WSN 与安全相关的特点主要有以下几个。

(1) 资源受限，通信环境恶劣。

WSN 单个节点能量有限，存储空间和计算能力差，直接导致了许多成熟、有效的安全协议和算法无法顺利应用。另外，节点之间采用无线通信方式，信道不稳定，信号不仅容易被窃听，而且容易被干扰或篡改。

(2) 部署区域的安全无法保证，节点易失效。

传感器节点一般部署在无人值守的恶劣环境或敌对环境中，其工作空间本身就存在不安全因素，节点很容易受到破坏或被俘，一般无法对节点进行维护，节点很容易失效。

(3) 网络无基础框架。

在 WSN 中，各节点以自组织的方式形成网络，以单跳或多跳的方式进行通信，由节点相互配合实现路由功能，没有专门的传输设备，传统的端到端的安全机制无法直接应用。

(4) 部署前地理位置具有不确定性。

在 WSN 中，节点通常随机部署在目标区域，任何节点之间是否存在直接连接在部署前是未知的。

2. 无线传感器网络的条件限制

无线传感器网络安全要求是基于传感器节点和网络自身条件的限制提出的。其中传感器节点的限制是无线传感器网络所特有的，包括电池能量、充电能力、睡眠模式、内存储器、传输范围、干预保护及时间同步。

网络限制与普通的 Ad hoc 网络一样，包括有限的结构预配置、数据传输速率和信息包大小、通道误差率、间歇连通性、反应时间和孤立的子网络。这些限制对于网络的安全路由协议设计、保密性和认证性算法设计、密钥设计、操作平台和操作系统设计以及网络基站设计等方面都有极大的挑战。

3. 无线传感器网络的安全威胁

由于无线传感器网络自身条件的限制，再加上网络的运行多在敌手区域内（主要是军事应用），使得网络很容易受到各种安全威胁，其中一些与一般的 Ad hoc 网络受到的安全威胁相似：

（1）窃听：一个攻击者能够窃听网络节点传送的部分或全部信息。

（2）哄骗：节点能够伪装其真实身份。

（3）模仿：一个节点能够表现出另一节点的身份。

（4）危及传感器节点安全：若一个传感器及其密钥被捕获，存储在该传感器中的信息便会被敌手读出。

（5）注入：攻击者把破坏性数据加入到网络传输的信息中或加入到广播流中。

（6）重放：敌手会使节点误认为加入了一个新的会议，再对旧的信息进行重新发送。重放通常与窃听和模仿混合使用。

（7）拒绝服务（DoS）：通过耗尽传感器节点资源来使节点丧失运行能力。

除了上面这些攻击种类外，无线传感器网络还有其独有的安全威胁种类：

（1）HELLO 扩散法：这是一种 DoS（拒绝服务）攻击，它利用了无线传感器网络路由协议的缺陷，允许攻击者使用强信号和强处理能量让节点误认为网络有一个新的基站。

（2）陷阱区：攻击者能够让周围的节点改变数据传输路线而经过一个被捕获的节点或是一个陷阱。

在物联网中，采用 RFID 标签是对物体静态属性的标识，而传感技术则用来标识物体的动态属性，构成物体感知的前提。从网络层次结构看，现有的传感网组网技术面临的安全问题如表 5.1 所示。

表 5.1　传感器网络组网技术面临的安全问题

层　次	受 到 的 攻 击
物理层	物理破坏、信道阻塞
链路层	制造冲突攻击、反馈伪造攻击、耗尽攻击、链路层阻塞等
网络层	路由攻击、虫洞攻击、女巫攻击、陷洞攻击、Helb 洪泛攻击
应用层	去同步、拒绝服务流等

4. 安全需求

WSN 的安全需求主要有以下几个方面。

1）机密性

机密性要求对 WSN 节点间传输的信息进行加密，让任何人在截获节点间的物理通信信号后不能直接获得其所携带的消息内容。

2）完整性

WSN 的无线通信环境为恶意节点实施破坏提供了方便，完整性要求节点收到的数据在传输过程中未被插入、删除或篡改，即保证接收到的消息与发送的消息是一致的。

3）健壮性

WSN 一般被部署在恶劣环境、无人区域或敌方阵地中，外部环境条件具有不确定性。另外，随着旧节点的失效或新节点的加入，网络的拓扑结构不断发生变化。因此，WSN 必须具有很强的适应性，使得单个节点或者少量节点的变化不会威胁整个网络的安全。

4）真实性

WSN 的真实性主要体现在两个方面：点到点的消息认证和广播认证。点到点的消息认证使得某一节点在收到另一节点发送来的消息时，能够确认这个消息确实是从该节点发送过来的，而不是别人冒充的；广播认证主要解决单个节点向一组节点发送统一通告时的认证安全问题。

5）新鲜性

在 WSN 中，由于网络多路径传输延时的不确定性和恶意节点的重放攻击，使得接收方可能收到延后的相同数据包。新鲜性要求接收方收到的数据包都是最新的、非重放的，即体现消息的时效性。

6）可用性

可用性要求 WSN 能够按预先设定的工作方式向合法的用户提供信息访问服务。然而，攻击者可以通过信号干扰、伪造或者复制等方式使 WSN 处于部分或全部瘫痪状态，从而破坏系统的可用性。

7）访问控制

WSN 不能通过设置防火墙进行访问过滤，由于硬件受限，也不能采用非对称加密体制的数字签名和公钥证书机制。WSN 必须建立一套符合自身特点，综合考虑性能、效率和安全性的访问控制机制。

传感器网络安全目标如表 5.2 所示。

表 5.2　传感器网络安全目标

目　　标	意　　义	主 要 技 术
可用性	确保网络即使在受到攻击（如 DoS 攻击）时也能够完成基本的任务	冗余、入侵检测、容错、容侵、网络自愈和重构
机密性	保证机密信息不会暴露给未授权的实体	信息加密和解密
完整性	保证信息不会被窜改	MAC、散列、签名
不可否认性	信息源发起者不能够否认自己发送的信息	签名、身份认证、访问控制
数据新鲜度	保证用户在指定时间内得到所需要的信息	网络管理、入侵检测、访问控制

5.1.2　无线传感器网络的安全机制

安全是系统可用的前提，需要在保证通信安全的前提下，降低系统开销，研究可行的安全算法。由于无线传感器网络受到的安全威胁和移动 Ad hoc 网络不同，所以现有的网络安

全机制无法应用于本领域，需要开发专门协议。目前主要存在两种思路。

一种思想是从维护路由安全的角度出发，寻找尽可能安全的路由以保证网络的安全。如果路由协议被破坏，导致传送的消息被篡改，那么对于应用层上的数据包来说没有任何的安全性可言。一种方法是“有安全意识的路由”（SAR），其思想是找出真实值和节点之间的关系，然后利用这些真实值生成安全的路由。

该方法解决了两个问题，即如何保证数据在安全路径中传送和路由协议中的信息安全性。这种模型中，当节点的安全等级达不到要求时，就会自动地从路由选择中退出以保证整个网络的路由安全。可以通过多径路由算法改善系统的稳健性（robustness），数据包通过路由选择算法在多径路径中向前传送，在接收端内通过前向纠错技术得到重建。

另一种思想是把着重点放在安全协议方面，在此领域也出现了大量的研究成果。假定传感器网络的任务是为高级政要人员提供安全保护，提供一个安全解决方案将为解决这类安全问题带来一个合适的模型。在具体的技术实现上，先假定基站总是正常工作的，并且总是安全的，满足必要的计算速度和存储器容量，基站功率满足加密和路由的要求；通信模式是点到点，通过端到端的加密保证了数据传输的安全性；射频层总是正常工作。基于以上前提，典型的安全问题可以总结为以下 4 点：

（1）信息被非法用户截获。

（2）一个节点遭破坏。

（3）识别伪节点。

（4）如何向已有传感器网络添加合法的节点。

以下方案是不采用任何路由机制。在此方案中，每个节点和基站分享一个唯一的 64 位密钥和一个公共的密钥，发送端会对数据进行加密，接收端接收到数据后，根据数据中的地址选择相应的密钥对数据进行解密。

无线传感器网络中的两种专用安全协议是安全网络加密协议（Sensor Network Encryption Protocol，SNEP）和基于时间的高效的容忍丢包的流认证协议 uTESLA。

SNEP 的功能是提供节点到接收机之间数据的鉴权、加密和刷新，uTESLA 的功能是对广播数据的鉴权。因为无线传感器网络可能是布置在敌对环境中的，为了防止供给者向网络注入伪造的信息，需要在无线传感器网络中实现基于源端认证的安全组播。但由于在无线传感器网络中不能使用公钥密码体制，因此源端认证的组播并不容易实现。

传感器网络安全协议 SP INK 中提出了基于源端认证的组播机制 uTESLA，该方案是对 TESLA 协议的改进，使之适用于传感器网络环境。其基本思想是采用 Hash 链的方法在基站生成密钥链，每个节点预先保存密钥链最后一个密钥作为认证信息，整个网络需要保持松散同步，基站按时段依次使用密钥链上的密钥加密消息认证码，并在下一时段公布该密钥。

5.1.3 无线传感器网络的安全分析

由于传感器网络自身的一些特性，使其在各个协议层都容易遭受到各种形式的攻击。下面着重分析对无线传感器网络的攻击形式。

1. 物理层的攻击和防御

物理层中安全的主要问题就是如何建立有效的数据加密机制，由于传感器节点的限制，其有限的计算能力和存储空间使基于公钥的密码体制难以应用于无线传感器网络中。为了节省传感器网络的能量开销和提供整体性能，也尽量要采用轻量级的对称加密算法。

Prasanth Ganesan 等人详细分析了对称加密算法在无线传感器网络中的负载，在多种嵌入式平台构架上分别测试了 RC4、RC5 和 IDEA 等 5 种常用的对称加密算法的计算开销。测试表明，在无线传感器平台上性能最优的对称加密算法是 RC4，而不是目前传感器网络中所使用的 RC5。

由于对称加密算法的局限性，不能方便地进行数字签名和身份认证，给无线传感器网络安全机制的设计带来了极大的困难。因此高效的公钥算法是无线传感器网络安全亟待解决的问题。

2. 链路层的攻击和防御

数据链路层或介质访问控制层为邻居节点提供可靠的通信通道，在 MAC 协议中，节点通过监测邻居节点是否发送数据来确定自身是否能访问通信信道。这种载波监听方式特别容易遭到拒绝服务(DoS)攻击。在某些 MAC 层协议中使用载波监听的方法来与相邻节点协调使用信道。当发生信道冲突时，节点使用二进制值指数倒退算法来确定重新发送数据的时机，攻击者只需要产生一个字节的冲突就可以破坏整个数据包的发送。

因为只要部分数据的冲突就会导致接收者对数据包的校验和不匹配。导致接收者会发送数据冲突的应答控制信息 ACK 使发送节点根据二进制指数倒退算法重新选择发送时机。这样经过反复冲突，使节点不断倒退，从而导致信道阻塞。恶意节点有计划地重复占用信道比长期阻塞信道要花更少的能量，而且相对于节点载波监听的开销，攻击者所消耗的能量非常小，对于能量有限的节点，这种攻击能很快耗尽节点有限的能量。所以，载波冲突是一种有效的 DoS 攻击方法。

虽然纠错码提供了消息容错的机制，但是纠错码只能处理信道偶然错误，而一个恶意节点可以破坏比纠错码所能恢复的错误更多的信息。纠错码本身也导致了额外的处理和通信开销。目前来看，这种利用载波冲突对 DoS 的攻击还没有有效的防范方法。

解决的方法就是对 MAC 的准入控制进行限速，网络自动忽略过多的请求，从而不必对于每个请求都应答，节省了通信的开销。但是采用时分多路算法的 MAC 协议通常系统开销比较大，不利于传感器节点节省能量。

3. 网络层的攻击和防御

通常，在无线传感器网络中，大量的传感器节点密集地分布在一个区域里，消息可能需要经过若干节点才能到达目的地，而且由于传感器网络的动态性，因此没有固定的基础结构，所以每个节点都需要具有路由的功能。由于每个节点都是潜在的路由节点，因此更易于受到攻击。无线传感器网络的主要攻击种类较多，简单介绍如下。

1) 虚假路由信息

通过欺骗，更改和重发路由信息，攻击者可以创建路由环，吸引或者拒绝网络信息流通量，延长或者缩短路由路径，形成虚假的错误消息，分割网络，增加端到端的时延。

2）选择性的转发

节点收到数据包后，有选择地转发或者根本不转发收到的数据包，导致数据包不能到达目的地。

3）污水池（sinkhole）攻击

攻击者通过声称自己电源充足、性能可靠而且高效，使泄密节点在路由算法上对周围节点具有特别的吸引力，吸引周围的节点选择它作为路由路径中的点。引诱该区域几乎所有的数据流通过该泄密节点。

4）Sybil 攻击

在这种攻击中，单个节点以多个身份出现在网络中的其他节点面前，使之具有更高概率被其他节点选作路由路径中的节点，然后和其他攻击方法结合使用，达到攻击的目的。它降低具有容错功能的路由方案的容错效果，并对地理路由协议产生重大威胁。

5）蠕虫洞（wormholes）攻击

攻击者通过低延时链路将某个网络分区中的消息发往网络的另一分区重放。常见的形式是两个恶意节点相互串通，合谋进行攻击。

6）Hello 洪泛攻击

很多路由协议需要传感器节点定时地发送 Hello 包，以声明自己是其他节点的邻居节点。而收到该 Hello 报文的节点则会假定自身处于发送者正常无线传输范围内。而事实上，该节点离恶意节点的距离较远，以普通的发射功率传输的数据包根本到不了目的地。如果受到攻击，后果非常严重。

7）选择性转发

恶意节点可以概率性地转发或者丢弃特定消息，而使网络陷入混乱状态。如果恶意节点抛弃所有收到的信息，将形成黑洞攻击，但是这种做法会使邻居节点认为该恶意节点已失效，从而不再经由它转发信息包，因此选择性转发更具欺骗性。其有效的解决方法是多径路由，节点也可以通过概率否决投票并由基站或簇头对恶意节点进行撤销。

8）DoS 攻击

DoS 攻击是指任何能够削弱或消除 WSN 正常工作能力的行为或事件，对网络的可用性危害极大，攻击者可以通过拥塞、冲突、资源耗尽、方向误导和去同步等多种方法在 WSN 协议栈的各个层次上进行攻击。可以使用一种基于流量预测的传感器网络 DoS 攻击检测方案，从 DoS 攻击引发的网络流量异常变化入手，根据已有的流量观测值来预测未来流量，如果真实的流量与预测流量存在较大偏差，则判定为一种异常或攻击。在一种简单、高效的流量预测模型的基础上，设计一种基于阈值超越的流量异常判断机制，使路径中的节点在攻击发生后自发地检测异常，最后提出一种报警评估机制以提高检测质量。

传感器网络中的攻击和防御手段可总结为表 5.3。

表 5.3　传感器网络中的攻击和防御手段

网络层次	攻击手段	防御方法
物理层	拥塞攻击	调频、消息优先级、低占空比、区域映射、模式转换
链路层	物理破坏	破坏证明、伪装和隐藏
	冲突攻击	纠错码
	耗尽攻击	设置竞争门限
	非公平竞争	短帧和非优先级策略

续表

网 络 层 次	攻 击 手 段	防 御 方 法
网络层	丢弃和贪婪破坏	冗余路径、探测机制
	汇聚节点攻击	加密和逐跳认证机制
	方向误导攻击	出口过滤、认证监视机制
	黑洞攻击	认证、监视、冗余机制
传输层	泛洪攻击	客户端谜题
	失步攻击	认证

5.2　无线传感器网络的基本安全技术

传感器网络的基本安全技术包括基本安全框架、密钥分配、安全路由和入侵检测以及加密技术等。其中整合多种安全机制于一体，如图 5.1 所示。构成传感器网络的整体安全框架是构建安全传感器网络的重要手段。

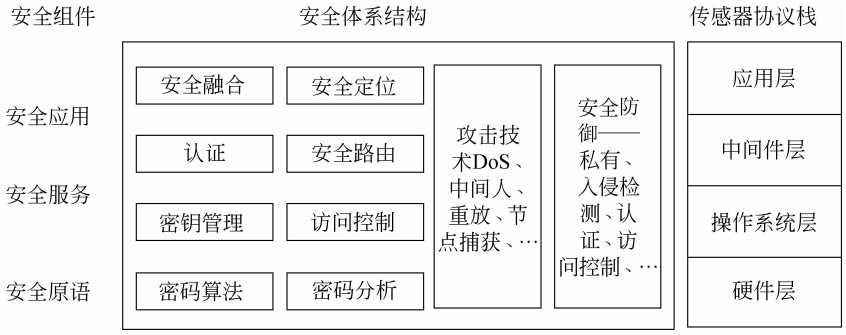

图 5.1　传感器网络安全体系结构

5.2.1　安全框架与密钥分配

1. 安全框架

现有的安全框架有 SPIN(包含 SNEP 和 uTESLA 两个安全协议)、Tiny Sec、参数化跳频、LisP 和 LEAP 协议等。

2. 密钥分配

传感器网络的密钥分配主要倾向于采用随机预分配模型的密钥分配方案，其主要思想是在网络构建之前，每个节点从一个较大的密钥池中随机选择少量密钥构成密钥环，使得任意两个节点之间能以一个较大的概率共享密钥。

5.2.2 安全路由

由于传感器网络中许多路由协议相对简单，更易受到攻击，所以常常采用安全路由来增加网络的安全性，常用的方法有：

(1) 路由中加入容侵策略，可提高物联网的安全性。

(2) 用多径路由选择方法抵御选择性转发攻击。采用多径路由选择，允许节点动态地选择一个分组的下一跳节点，能更进一步地减少入侵者控制数据流的计划，从而提供保护。

(3) 在路由设计中加入广播半径限制抵御洪泛攻击。采用广播半径限制，每个节点都限制一个数据发送半径，使它只能对落在这个半径区域内的节点发送数据，而不能对整个网络广播，这样就把节点的广播范围限制在一定的地理区域。具体可以对节点设置最大广播半径 Rmax 参数。

(4) 在路由设计中加入安全等级策略抵御虫洞攻击和陷洞攻击。

5.2.3 入侵检测技术

由于在物联网中完全依靠密码体制不能抵御所有攻击，故常采用入侵检测技术作为信息安全的第二道防线。入侵检测技术是一种检测网络中违反安全策略行为的技术，能及时发现并报告系统中未授权或异常的现象。

按照参与检测的节点是否主动发送消息，可将入侵检测技术分为被动监听检测和主动检测。被动监听检测主要是通过监听网络流量的方法展开，而主动检测是指检测节点通过发送探测包来反馈或者接收其他节点发来的消息，然后通过对这些消息进行一定的分析来检测。

根据检测节点的分布，被动检测可分为密集检测和稀疏检测两类。密集检测通过在所有节点上部署检测算法来最大限度发现攻击，检测通常部署在网络层。

网络层上的攻击检测方法主要有看门狗检测方法、基于 Agent 的方法、针对特别攻击的方法以及基于活动的监听方法等。链路层上主要通过检测到达 RTS 请求的速率来发现攻击。

在物理层上主要检测阻塞攻击，现存的有效方法有：通过检测单个节点发送和接收成功率来判断是否遭受攻击；通过分析信号强度随时间的分布来发现阻塞攻击特有的模式；以及通过周期性检查节点的历史载波侦听时间来检测攻击。

稀疏检测则通过选择合适的关键节点进行检测，在满足检测需求的条件下尽量降低检测的花费。

主动检测主要有 4 种方法：

(1) 路径诊断的方法。

其诊断过程是源节点向故障路径上选定的探测节点发送探测包，每个收到探测包的节点都向源节点发送回复，若某节点没有返回包，说明其与前一个节点间的子路径出现故障，需要在其间插入新的探测节点展开新一轮检测。

(2) 邻居检测的方法。

单个节点通过向各个邻居节点从对应的不同物理信道发送信号获得反馈来发现不合法

的节点 ID;也可以在链路层 CTS 包中加入一些预置要求,如发送延迟等,如果接收方没有采取所要求的行为则被认定为非法节点。还有针对特定攻击的检测,基站向周围节点发送随机性的组播,然后通过消息反馈的情况检测针对组播协议的攻击 DOM。

(3) 通过向多个路径发送 ping 包的方式以发现路径上的关键节点,从而部署攻击检测算法。

(4) 基于主动提供信息的检测。网络中部分节点向其他节点定期广播邻居节点信息,其他节点通过分析累积一定时间后的信息发现重复节点。

以上这些检测技术在网络中实现,不可避免的问题是:由于物联网节点资源受限,且是高密度冗余撒布,不可能在每个节点上运行一个全功能的入侵检测系统(IDS),因此,如何在传感网中合理地分布 IDS 的问题有待于进一步研究。

5.3　无线传感器网络安全研究重点

无线传感器网络技术是一项新兴的前沿技术,国外比国内研究得更早、更深入。纵观国外近几年对无线传感器网络安全领域的研究,可将其分为几大类,如表 5.4 所示。

表 5.4　无线传感器网络安全项目分类

类	子　类	类	子　类
密码技术	加密技术	路由安全	安全路由行程
	完整性检测技术		攻击
	身份认证技术		路由算法
	数字签名	位置意识安全	攻击
密钥管理	预先配置密钥		安全路由协议
	仲裁密钥		位置确认
	自动加强的自治密钥	数据融合安全	集合
	使用配置理论的密钥管理		认证

5.3.1　无线传感器网络安全技术

无线传感器网络也是无线通信网络的一种,有着基本相同的密码技术。密码技术是无线传感器网络安全的基础,也是所有网络安全实现的前提。涉及无线传感器网络的安全技术有如下几种。

1. 加密技术

加密是一种基本的安全机制,它把传感器节点间的通信消息转换为密文,形成加密密钥,这些密文只有知道解密密钥的人才能识别。

加密密钥和解密密钥相同的密码算法称为对称密钥密码算法;而加密密钥和解密密钥

不同的密码算法称为非对称密钥密码算法。对称密钥密码系统要求保密通信双方必须事先共享一个密钥，因而也叫单钥（私钥）密码系统。这种算法又分为分流密码算法和分组密码算法两种。而非对称密钥密码系统中，每个用户拥有两种密钥，即公开密钥和秘密密钥。公开密钥对所有人公开，而只有用户自己知道秘密密钥。

2. 完整性检测技术

完整性检测技术用来进行消息的认证，是为了检测因恶意攻击者窜改而引起的信息错误。为了抵御恶意攻击，完整性检测技术加入了秘密信息，不知道秘密信息的攻击者将不能产生有效的消息完整性码。

消息认证码是一种典型的完整性检测技术。

（1）将消息通过一个带密钥的杂凑函数来产生一个消息完整性码，并将它附着在消息后一起传送给接收方。

（2）接收方在收到消息后可以重新计算消息完整性码，并将其与接收到的消息完整性码进行比较：如果相等，接收方可以认为消息没有被窜改；如果不相等，接收方就知道消息在传输过程中被窜改了。该技术实现简单，易于在无线传感器网络中实现。

3. 身份认证技术

身份认证技术通过检测通信双方拥有什么或者知道什么来确定通信双方的身份是否合法。这种技术是通信双方中的一方通过密码技术验证另一方是否知道他们之间共享的秘密密钥或者其中一方自有的私有密钥。这是建立在运算简单的对称密钥密码算法和杂凑函数基础上的，适合所有无线网络通信。

4. 数字签名

数字签名是用于提供服务不可否认性的安全机制。数字签名大多基于非对称密钥密码算法，用户利用其秘密密钥将一个消息进行签名，然后将消息和签名一起传给验证方，验证方利用签名者公开的密钥来认证签名的真伪。

5.3.2 密钥确立和管理

密码技术是网络安全构架十分重要的部分，而密钥是密码技术的核心内容。密钥的确立需要在参与实体和密钥计算之间建立信任关系，信任建立可以通过公开密钥或者秘密密钥技术来实现。无线传感器网络的通信不能依靠一个固定的基础组织或者一个中心管理员来实现，而要用分散的密钥管理技术。

密钥管理协议分为预先配置密钥协议、仲裁密钥协议和自动加强的自治密钥协议。预先配置密钥协议在传感器节点中预先配置密钥。这种方法不灵活，特别是在动态无线传感器网络中增加或移除节点的时候。在仲裁密钥协议中，密钥分配中心（KDC）用来建立和保持网络的密钥，它完全被集中于一个节点或者分散在一组信任节点中。自动加强的自治密钥协议把建立的密钥散布在节点组中。