第 3 章　无线传感器网络安全

正如第 2 章开头所介绍的，根据 ITU 的物联网报告，无线传感器网络是物联网的第二个关键技术。RFID 的主要功能是对物体的识别；而无线传感器网络的主要功能是感知。无线传感器网络则是大范围多位置的感知。通俗地说，传感器是可以感知外部环境参数的小型计算结点，传感器网络是大量传感器结点构成的网络，用于不同地点、不同种类的参数的感知或数据的采集，无线传感器网络则是利用无线通信技术来传递感知的数据的网络。

其实感知技术还可包括更多的方面，如红外线技术可以感知物体对光线的“遮挡”，广泛应用于节水龙头；摄像头可以感知（采集）物体的图像和动作，广泛应用于视频监控；GPS 设备可以感知物体的位置；声音感应控制电灯的开关。由于无线传感器网络是感知技术中最重要的一种，本章重点介绍无线传感器网络的安全。

3.1　无线传感器安全简介

无线传感器网络（Wireless Sensor Networks，WSN）是集成了传感器技术、微机电系统技术、无线通信技术以及分布式信息处理技术于一体的新型网络。随着科学技术的发展，信息的获取变得更加纷繁复杂。所有保存事物状态、过程和结果的物理量都可以用信息来描述。传感器的发明和应用，极大地提高了人类获取信息的能力。传感器信息获取从单一化到集成化、微型化，进而实现智能化、网络化，成为获取信息的一个重要手段。无线传感器网络在很多场合（如军事感知战场、环境监控、道路交通监控、勘探、医疗等）都承担重要的作用。

3.1.1　无线传感器网络的体系结构

1. 传感器结点的物理结构

在不同的应用场景中，传感器结点的组成不尽相同，但是从结构上来说一般都包含以下 4 个部分：数据采集、数据处理、数据传输和电源。感知信号的形式通常决定了传感器的类型。而现有的传感器结点的处理器通常包括嵌入式 CPU，如 ARM 公司的 ARM 系列、Motorola 的 68HC16 和 Intel 公司的 8086 等。数据传输单元主要由低功耗、短距离的无线模块组成，如 RFM 公司的 TR1000 等。另外运行于传感器网络上的微型化的操作系统主要负责复杂任务的系统调度与管理，比较常见的有 UC Berkeley 开发的 TinyOS 以及 μCOS-Ⅱ嵌入式 Linux。

如图 3.1 所示是一个典型的传感器体系结构图，传感器模块负责数据的感知和产生

及数模转化，信息处理模块负责进行信号处理，最后经由无线通信模块发射出去。

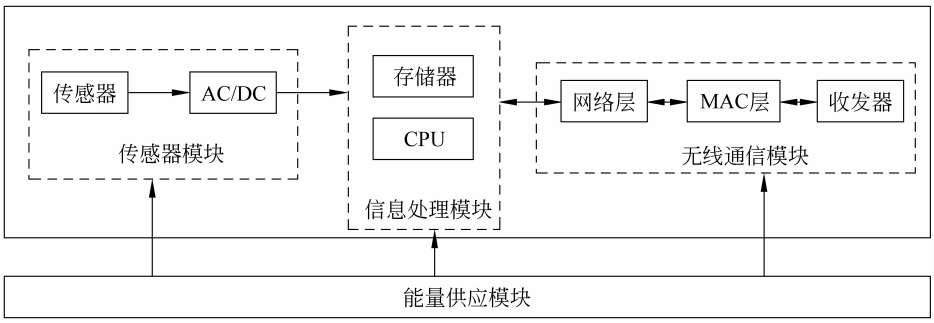

图 3.1　传感器结点体系结构图

传感器网络结点的一些技术参数包括如下几项。

(1) 电池能量。传感器的能量一般由电池提供。一次性电池原则上可工作几年时间。

(2) 传输范围。由于传感器结点能量有限，结点的传输范围只能被限制在一个很小的范围之内(通常是 100 米以内，一般为 1～10 米)，否则会造成传感器的能量枯竭。一些技术(比如数据聚集传输技术)通过先将数据进行聚集，然后传输聚集的结果(而不是每个数据)来减少能量的消耗，帮助减少传感器结点的传输能耗。

(3) 网络带宽。传感器网络的带宽通常只有几十千位每秒。如使用蓝牙协议时小于 723Kbps，使用 802.15.4ZigBee 协议时为 250Kbps。

(4) 内存大小。传感器结点的内存大小一般在 6～8Kb，而且一般的空间被传感器网络的操作系统所占据，例如 TinyOS。内存大小通常会影响密钥管理方案的可行性，即密钥管理方案必须能够有效地利用剩余的存储空间，完成密钥的存储，缓存消息等。

(5) 预先部署的内容。通常，传感器网络具有随机性和动态性，因为不可能获取应用环境的所有情况。预先在传感器结点上配置的信息通常是密钥类的信息，例如，通过预先在结点中存储一些秘密共享密钥，使得网络在部署之后能够实现结点间的安全通信。

2. 典型研究对象

加州大学伯克利分校发起的 smart dust 项目开发了多种传感器结点，如 WeC、Mica、Mica2、MicaZ 等。目前普遍采用的是 2004 年开发的 Telos 结点，采用 16 位 4MHz TI 公司的 MSP430 处理器，正常工作状态下功耗 3mW，该处理器芯片具有 5 种低功耗模式，一般睡眠模式下功耗仅为 225μW，深度睡眠模式下功耗仅为 7.8μW。内存 10KB，闪存 48KB。采用的通信芯片是 Chipcon 公司的 CC2420 通信芯片，工作在 2.4GHz 频道上，符合 IEEE 802.15.4 协议规范，数据传输率达到 250Kbps。

3. 无线传感器网络的网络结构

无线传感器网络在不同的应用场景中的网络拓扑结构可能不同。比较典型的应用方式是：无线传感器结点被任意地散落在监测区域，然后结点间以自组织的形式构建网络，对感知参数进行监测并生成感知数据，最后通过短距离无线通信(如 ZigBee)经过多次转发将数据传送到网关(Sink 结点或者汇聚结点)，网关通过远距离无线通信网络(如

GPRS)将数据发到控制中心。也有传感器结点直接将感知的数据发给控制中心的,这便是一种典型的 M2M 通信场景。一般而言,无线传感器网络的结构可以分为分布式网络结构和集中式网络结构两种。

1) 分布式无线传感器网络

分布式无线传感器网络没有固定的网络结构,网络拓扑结构在部署前也无法确定。传感器结点通常随机部署在目标区域中。一旦结点被部署,它们就开始在自己的通信范围内,寻找邻居结点,建立数据传输路径。如图 3.2 所示为分布式网络结构的示意图。

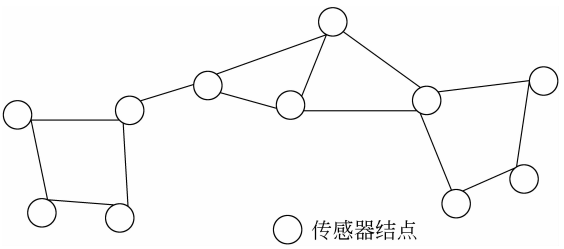

图 3.2 分布式网络结构的示意图

2) 集中式无线传感器网络

在集中式无线传感器网络中,依据结点能力的不同可以分为基站、簇头(Cluster Head)结点和普通结点。基站是一个控制中心,通常认为它具有很高的计算和存储能力,可以实施多种控制命令。基站的功能包括以下几种:典型的网络应用中的网关、具有强大的数据存储/处理能力、用户的访问接口。基站通常被认为是抗攻击、可信赖的,因而基站可成为网络中的密钥分发中心。结点通常部署在与基站一跳或多跳的范围内,多跳结点形成一个簇结构(簇结构即包含一个簇头结点和多个普通结点或孩子结点的树状结构)。基站具有很强的传输能力,通常可以与任意一个网络内的结点通信,而结点的通信能力则取决于结点自身的能量水平和位置。依据通信方式的不同,网络内的数据流可以分为点对点通信、组播通信、基站到结点的广播通信。如图 3.3 所示为集中式网络结构的简图。

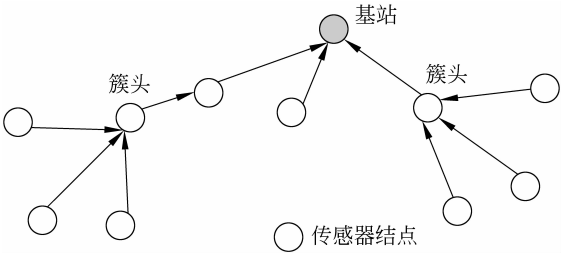

图 3.3 集中式网络结构的简图

无线传感器网络的特点如下,在设计安全方案时需要考虑到这些特点:

(1) 网络结点数量众多,结点密度大(即单位面积内的结点数量较多)。

(2) 网络拓扑结构不稳定,拓扑结构随时会发生变化。

(3) 传感器结点受到应用环境和结点成本的限制,计算和通信能力有限。

(4) 能量受限:无线传感器网络由于部署在特定环境中,通常没有持续的外接电能供应,多以电池作为能量源。

3.1.2　无线传感器网络的安全需求分析

通常无线传感器网络会被部署在不易控制、无人看守、边远或易于遭到恶劣环境破坏或者恶意破坏和攻击的环境当中,因而无线传感器网络的安全问题成为研究的热点。由于传感器结点本身计算能力和能量受限的特点,寻找轻量级(计算量小、能耗低)的适合于无线传感器网络特点的安全手段是研究所面临的主要挑战。

1. 安全需求

(1) 通信与储存数据的机密性。无线传感器网络通信不应当向攻击者泄漏任何敏感的信息。在许多应用中,结点之间传递的是高度敏感的数据或者控制信息。结点保存的感知数据、秘密密钥及其他传感器网络中的机密信息(如传感器的身份标识等),必须只有授权的用户才能访问。同时,因密钥泄漏造成的影响应当尽可能控制在一个小的范围内,从而使得一个密钥的泄漏不至于影响整个网络的安全。解决通信机密性主要依靠使用通信双方共享的会话密钥来加密待传递的消息,解决存储机密性主要依靠加密数据的访问控制。

(2) 消息认证和访问结点认证。结点身份认证在无线传感器网络的许多应用中是非常重要的。例如攻击者极易向网络注入信息,接收者只有通过身份认证才能确信消息是从正确的结点发送过来。数字签名通常不适用于通信能力、计算速度和存储空间都相当有限的传感器结点。传感器网络通常使用基于对称密码学的认证方法,即判断对方是否拥有共享的对称密钥来进行身份的认证。

(3) 通信数据和存储数据的完整性。资源有限的传感器无法支持高计算量的数字签名算法,通常使用对称密钥体制的消息鉴别码来进行数据完整性检验。

(4) 新鲜性。在无线传感器网络中,基站和簇头需要处理很多结点发送过来的采集信息,为防止攻击者进行任何形式的重放攻击(将过去窃听的消息重复发送给接收者,耗费其资源使其不能提供正常服务),必须保证每条消息是新鲜的。由于密钥可能需要进行更新,因而新鲜性还体现在密钥建立过程中,即通信双方所共享的密钥是最新的。

(5) 可扩展性(Scalability)。这是无线传感器网络的特色之一,由于传感器结点数量大、分布范围广,环境条件、恶意攻击或任务的变化可能会影响传感器网络的配置。同时,结点的经常加入、物理破坏或电量耗尽等也会使得网络的拓扑结构不断发生变化。无线传感器网络的可扩展性表现在传感器结点的数量、网络覆盖区域、生命周期、时间延迟等方面的可扩展程度。因此,给定无线传感器网络的可扩展性级别,例如结点的数量级,安全解决方案必须提供支持该可扩展性级别的安全机制和算法,来使传感器网络保持良好的工作状态。

(6) 可用性(Availability)。无线传感器网络的安全解决方案所提供的各种服务能被授权用户使用,并能有效防止非法攻击者企图中断传感器网络服务的恶意攻击。一个合理的安全方案应当具有节能高效的特点,各种安全协议和算法的设计不应当太复杂,并尽可能地避开公钥密码运算(如公钥加密/解密或者数字签名和签名验证),计算开销、存储

容量和通信能力、能量消耗的最小化，最终延长网络的生命周期。

(7) 健壮性(Robustness)。无线传感器网络一般配置在恶劣环境或无人区域，环境条件、现实威胁和当前任务具有很大的不确定性。这要求传感器结点能够灵活地加入或去除、传感器网络之间能够进行合并或拆分，因而安全解决方案应当具有鲁棒性和自适应性，能够随着应用背景的变化而灵活拓展，安全解决方案尽可能满足所有可能的应用环境和条件。此外，当某个或某些结点被攻击者控制后，安全解决方案应当限制其安全影响范围，保证整个网络不会因此而失效。

(8) 自组织性(Self-Organization)。由于无线传感器网络是由一组传感器以自组织的(Ad Hoc)方式构成的无线网络，这就决定了相应的安全解决方案也应当是自组织的，即在无线传感器网络配置之前通常无法假定结点的任何位置信息和网络的拓扑结构，也无法确定某个结点的邻近结点集。

2. 安全方案设计时的考虑因素

由于无线传感器网络本身的特点，其安全目标的实现与一般网络不同，在研究和移植各种安全技术时，必须进一步考虑以下约束：

(1) 能量限制。结点在部署后很难替换和充电，所以低能耗是设计安全算法时首要考虑的因素。能耗特点包括：通信芯片耗能占整个传感器结点能耗的比重最大，如常用的 TelosB 结点上，CPU 在正常状态电流只有 500μA，而通信芯片在发送和接收数据时的电流近 200mA。另外，低功耗的通信芯片在发送状态和接收状态消耗的能量差别不大。因而，安全方案应该尽量减少通信(如协议交互)的次数。

(2) 有限的存储、运行空间和计算能力。目前微处理器一般配有 4～10KB 内存，48～128KB 的闪存。

(3) 结点的物理安全无法保证。在进行安全设计时必须考虑被敌手所控制的结点(也称为被俘结点、妥协结点)的检测、撤除问题，来自内部被俘结点发起的攻击，同时还要将被俘结点导致的安全隐患扩散限制在最小范围内。

(4) 结点布置的随机性。结点往往是被随机地投放到目标区域的，结点之间的位置关系一般在布置前是不可预知的。

(5) 通信的不可靠性。无线通信信道的不稳定、结点并发通信的冲突和多跳路由的较大延迟使得设计安全算法时必须考虑容错问题，合理地协调结点通信，并尽可能减少对时间同步的要求。

另外，无线传感器网络的应用十分广泛，而不同的应用场景对安全的需求往往是不同的，应该根据实际的应用来分析具体的安全需求。

3.2 无线传感器网络的安全攻击与防御

3.2.1 常见网络攻击方法

由于传感器网络采用无线通信，开放的数据链路是不安全的，攻击者可以窃听通信的内容，实施干扰。而且传感器结点通常工作在无人区域，缺乏物理保护，容易损坏，且攻击

者可以获取结点，读取存储内容甚至写入恶意代码。攻击通常与使用的数据链路层协议(如 IEEE 802.15.4)、网络层协议(如路由协议、传输层协议)有关。本节首先对各种攻击简单进行分类，然后按网络体系各层归纳各种攻击方法。

(1) 阻塞(Jamming)攻击：一种针对无线通信的 DoS 攻击。攻击方法是干扰正常结点通信所使用的无线电波频率，达到干扰正常通信的目的。攻击者只需要在结点数为 N 的网络中随机布置 K(K<<N)个攻击结点，使它们的干扰范围覆盖全网，就可以使整个网络瘫痪。

(2) 耗尽(Exhaustion)攻击：恶意结点侦听附近结点的通信，当一帧快发送完时，恶意结点发送干扰信号。传统的 MAC 层协议中的控制算法往往会重传该帧，反复重传造成被干扰结点电源很快被耗尽。自杀式的攻击结点甚至一直对被攻击结点发送请求(Request)信号，使得对方必须回答，这样两个结点都耗尽电源。这一攻击的原理可能与具体 MAC 层协议(如 IEEE 802.15.4 协议)有关。

(3) 非公平竞争攻击。由于无线信道是单一访问的共享信道，采取竞争方式进行信道的分配，该攻击是指在网络中的某些恶意结点总是占用链路信道，采用一些设置，如较短的等待时间进行重传重试、预留较长的信道占用时间等，企图不公平地占用信道。这一攻击的原理与 MAC 层协议有关。

(4) 汇聚结点(Homing)攻击：传感器网络中有些结点执行路由转发功能，Homing 攻击针对这一类结点。攻击者只需要监听网络通信，就可以知道簇头的位置，然后对其发动攻击。簇头瘫痪后，在一段时间内整个簇都不能工作。它也属于 DoS 攻击的一种。

(5) 怠慢和贪婪(Neglect and Greed)攻击：其含义是少转发、不转发或多转发收到的数据包。攻击者处于路由转发路径上，但是随机地对收到的数据包不予转发处理。如果向消息源发送收包确认，但是把数据包丢弃不予转发，该攻击称为怠慢(Neglect)。如果被攻击者改装的结点对自己产生的数据包设定很高的优先级，使得这些恶意信息在网络中被优先转发，该攻击称为贪婪(Greed)。

(6) 方向误导(Misdirection)攻击：这里的方向是指数据包转发的方向。如果被敌人所控制的路由结点将收到的数据包发给错误的目标，则数据源结点受到攻击；如果将所有数据包都转发给同一个正常结点，则该结点很快因接收包而耗尽电源。方向误导攻击的一个变种是 Smurf 攻击。

(7) 黑洞(Black Holes)攻击：又称为排水洞(Sinkholes)攻击。攻击者(用 A 表示)声称自己具有一条高质量的路由到基站，比如广播“我到基站的距离为零”。如果 A 能发送到很远的无线通信距离，则收到该信息的大量结点会向 A 发送数据。大量数据到达 A 的邻居结点，它们都要给 A 发送数据，造成信道的竞争。由于竞争，邻居结点的电源很快被耗尽，这一区域就成了黑洞，通信无法传递过去。对于收到的数据，A 可能不予处理。黑洞攻击破坏性很强，基于距离向量(Distance Vector)的路由算法容易受到黑洞攻击，因为这些路由算法将距离较短的路径作为优先传递数据包的路径。

(8) 虫洞(Wormholes)攻击：通常由两个移动主机攻击者合作进行。一个主机 A 在网络的一边收到一条消息，比如基站的查询请求，通过低延迟链路传给距离很远的另一个主机 B，B 就可以直接广播出去，这样，收到 B 广播的结点就会把传感的数据发给 B，因为

收到 B 广播的结点认为这是一条到达 A 的捷径。

(9) Hello 泛洪(Hello Flood)攻击：在许多协议中，结点通过发送一条 Hello 消息表明自己的身份，而收到该消息的结点认为发送者是自己的邻居(因为数据包可以到达)。但移动主机攻击者可以将 Hello 消息传播得很远，远处的正常结点收到消息之后于是把攻击者当成自己的邻居。这些结点会与“邻居”(移动主机攻击者)通信，导致网络流量的混乱。传感器网络中的几个路由协议，如 LEACH 和 TEEN，易受这类攻击，特别是当 Hello 包中含有路由信息或定位信息。

(10) 女巫(Sybil)攻击：是指一个结点冒充多个结点，它可以声称自己具有多个身份，甚至随意产生多个假身份，利用这些身份非法获取信息并实施攻击。Sybil 攻击能破坏传感器网络的路由算法，还能降低数据汇聚算法的有效性。

(11) 破坏同步(Desynchronization)攻击：在两个结点正常通信时，攻击者监听并向双方发送带有错误序列号的包，使得双方误以为发生了丢失而要求对方重传。攻击者使正常通信双方不停地重传消息，从而耗尽电源。

(12) 泛洪攻击(Flooding)：指攻击者不断地要求与邻居结点建立新的连接，从而耗尽邻居结点用来建立连接的资源，使得其他合法的对邻居结点的请求不得不被忽略。

(13) 应用层攻击：如感知数据的窃听、篡改、重放、伪造等。结点不合作行为。对应用层功能如结点定位、结点数据收集和融合等的攻击，使得这些功能出现错误。

表 3.1 所示给出了无线传感器网络中网络攻击分类的小结。

表 3.1　无线传感器网络中网络攻击的分类

分类标准	分　类	说　明
攻击者身份	结点型攻击	攻击者与传感器结点的计算和通信能力相当
	移动主机型攻击	攻击者与移动电脑同级别，危害范围广
攻击来源	外部攻击	攻击者是敌方放置的，可以是结点或移动电脑
	内部攻击	网络中的结点被攻击者所控制，从网络内部发起攻击
攻击发生的协议层次	物理层攻击	阻塞攻击
	数据链路层攻击	耗尽攻击、非公平竞争攻击
	网络层攻击	汇聚结点攻击、怠慢和贪婪攻击、方向误导攻击、黑洞攻击、虫洞攻击、Hello 泛洪、女巫攻击
	传输层攻击	破坏同步攻击、泛洪攻击
	应用层攻击	如感知数据的窃听、篡改、重放、伪造等，结点不合作

3.2.2　常用防御机制

对于物理层的攻击(如阻塞(Jamming)攻击)使用扩频通信可以有效地防止。另一对策是，攻击结点附近的结点觉察到 Jamming 之后进入睡眠状态，保持低能耗。然后定期检查 Jamming 是否已经消失，如果消失则进入活动状态，向网络通报 Jamming 的发生。

对于传输层的攻击(如 Flooding),一种对策是使用客户谜题(Client Puzzle),即如果客户要和服务器建立一个连接,必须首先证明自己已经为连接分配了一定的资源,然后服务器才为连接分配资源,这样就增大了攻击者发起攻击的代价。这一防御机制对于攻击者同样是传感器结点时很有效,但是合法结点在请求建立连接时也增大了开销。

对于怠慢和贪婪攻击,可用身份认证机制来确认路由结点的合法性;或者使用多路径路由来传输数据包,使得数据包在某条路径被丢弃后,数据包仍可以被传送到目的结点。

抵抗黑洞攻击可采用基于地理位置的路由协议。因为拓扑结构建立在局部信息和通信上,通信通过接收结点的实际位置自然地寻址,所以在别的位置成为黑洞就变得很困难了。

对付女巫攻击有两种探测方法,一种是资源探测法,即检测每个结点是否都具有应该具备的硬件资源。Sybil 结点不具有任何硬件资源,所以容易被检测出来。但是当攻击者的计算和存储能力都比正常传感器结点大得多时,则攻击者可以利用丰富的资源伪装成多个 Sybil 结点。另一种是无线电资源探测法,通过判断某个结点是否有某种无线电发射装置来判断是否为 Sybil 结点,但这种无线电探测非常耗电。

对于更多的攻击,通常采用加密和认证机制提供解决方案。例如对于分簇结点的数据层层聚集,可使用同态加密、秘密共享的方法。对于结点定位安全,可采取门限密码学,以及容错计算的方法等。然而在无线传感器网络中,传感器结点的计算资源非常有限,通常公钥加密和签名算法因计算量太大而不适用,所以对称密钥加密方案研究得较多,而为了应用对称密钥加密方法,首先需要解决加密密钥的管理问题,这将在下一节介绍。表 3.2 给出了对攻击防御方法的小结。

表 3.2　无线传感器网络攻击防御方法

网络层次	攻击方法	防御方法
物理层	阻塞攻击	扩频、优先级消息、区域映射、模式转换
	物理破坏	破坏感知、结点伪装和隐藏
数据链路层	耗尽攻击	设置竞争门限
	非公平竞争	使用短帧策略和非优先级策略
网络层	丢弃和贪婪攻击	冗余路径、探测机制
	汇聚结点攻击	加密和逐跳(hop-to-hop)认证机制
	方向误导攻击	出口过滤、认证、监测机制
	黑洞攻击	认证、监测、冗余机制
传输层	破坏同步攻击	认证
	泛洪攻击	客户端谜题
应用层	感知数据的窃听、篡改、重放、伪造	加密、消息鉴别、认证、安全路由、安全数据聚集、安全数据融合、安全定位、安全时间同步
	结点不合作	信任管理,入侵检测

3.3 无线传感器网络的密钥管理

无线传感器网络安全中有诸多问题，如安全路由，安全定位，安全数据聚集等，篇幅所限这里只能对一个典型问题加以展开介绍。密钥管理问题是无线传感器网络需要首先解决的安全问题，因为密钥的建立与分发是保密通信的前提。同时，由于传感器结点数量庞大、随机布置的(具有随机网络拓扑结构)，且结点具有资源受限(计算、存储和能量有限)，结点可能因断电、被损坏、被捕获而失效或泄漏密钥，于是密钥管理问题变得更加棘手。因而，密钥管理的可扩展性、自组织性、鲁棒性等要求较高，成为无线传感器网络中一个独具特色的研究问题。

3.3.1 密钥管理的分类与评价指标

传感器结点间共享的秘密密钥是消息加密、消息完整性保护和传感器结点认证的主要依据，因此，如何产生、分发、建立、更新、撤销这些密钥是一个首先需要解决的安全问题。

密钥管理协议分为预先配置密钥协议、有仲裁的密钥协议、分组分簇密钥协议等(这些分类之间可能会有重叠)。预先配置密钥协议即在传感器结点在部署的时候预先分配和安装将来要使用的密钥。这种方法简单，但是在动态无线传感器网络中增加或移除结点的时候，就不灵活。在有仲裁的密钥协议中，存在密钥分配中心(Key Distribution Center，KDC)或者可信第三方(Trusted Third Party，TTP)负责建立密钥，KDC 或 TTP 可以是一个结点或者分散在一组可信任的结点中。分组分簇密钥协议中结点被划分成多个簇，每个簇有能力较强(表现在剩余能量上)的一个或者多个簇头，协助密钥分配中心或者基站共同管理整个无线传感器网络。密钥的初始化分发和管理一般由簇头主持，协同簇内结点共同完成。

1. 预先配置密钥

(1) 网络预分配密钥方法。无线传感器网络整个网络共享一个秘密密钥，所有结点在配置前都要装载同样的密匙。这种方法简单，但是若某个结点的密钥被敌人知道，则整个网络中使用的密钥就暴露了，从而整个网络的通信都失去了保密性。

(2) 结点间预分配密钥方法。在这种方法中，网络中的每个结点需要知道与其通信的所有其他结点的 ID 号，在每两个结点间共享一个独立的秘密密钥。如果每个结点都可能与网络中的其他结点通信，并建立一个共享的秘密密钥，假定结点总量为 n 个，则每个结点要存储 n－1 个密钥，整个网络需要的密钥总量为 n(n－1)/2 个。当结点数量达到几千个时，密钥的数量就比较大了。

2. 有仲裁的密钥协议

仲裁协议假设存在建立密钥的可信第三方(TTP)。根据密钥建立的类型，可分为对称密钥分发协议和公钥分发协议。对称密钥分发通常有密钥分发中心(KDC)。对公钥的分发通常比较容易。

密钥建立协议支持组结点的密钥建立，即建议一组结点之间通信需要使用的密钥。

还有一种分等级的密钥确立协议叫做分层逻辑密钥，在具有相同层次的结点之间的建立密钥关系。

除了上述的分类方法以外还有其他一些分类的方法。表 3.3 给出了其他分类及其描述。

表 3.3　密钥管理名称描述

密钥管理方案名称	描　　述
基于主密钥的管理方案	网络中只有单一的密钥，进行加密、解密操作
对(Pairwise)密钥方案	把网络内的通信转化为结点间的通信模式，通过结点对之间的安全实现网络的安全
基于公钥的密钥管理方案	基于公钥技术的密钥管理方案，例如椭圆曲线公钥密码技术 TingECC 在传感器网络中的实现
预共享的密钥管理方案	这是目前研究比较成熟的模型，其中的方案主要有预分配机制、q-composite 机制、多路增强机制、随机预分配方案，以及基于位置信息的密钥管理方案等
动态密钥管理方案	提高了网络的适应能力，更好地支持网络规模的变化
集中式密钥管理方案	主要包括 LEAP 协议[6]、异构传感器网络密钥管理方案等

3. 密钥管理方案的评价指标

评价一种密钥管理技术的好坏，不能仅从能否保障传输数据安全来进行评价，还必须满足如下准则：

(1) 抗攻击性(Resistance)。主要指抗结点妥协的能力。在无线传感器网络中，敌人可能捕获部分结点并复制这些结点来发起新的攻击。针对这种情况，无线传感器网络必须能够抵抗一定数量的结点被捕获而发起的新的攻击。

(2) 密钥可回收性(Revocation)。如果一个结点被敌人控制，对网络产生破坏行为时，密钥管理机制应能采取有效的方式从网络中撤销(Revoke)该结点。撤销机制必须是轻量级的，即不会消耗太多的网络通信资源和结点能量。

(3) 容侵性(Resilience)。如果结点被捕获，密钥管理机制应能够保证其他结点的密钥信息不会被泄漏。即可以容忍网络中被捕获的结点数小于一定的阈值。同时，新结点能够方便地加入网络，参与安全通信。

3.3.2　确定密钥分配方案 Blundo

1. 结点间共享密钥

该模型保证了每个结点之间存在一对共享密钥，结点间会话密钥的建立可以利用该密钥生成。优点是由于要求每个结点必须存储所有其他结点的共享密钥，因而任意两个结点间总可以建立共同的密钥。任何两个结点间的密钥对是独享的，其他结点不知道其密钥信息，任何一个结点被捕获不会泄漏非直接连接的结点的密钥信息。模型简单，实现容易。缺点是扩展性不好，新结点的加入需要更新整个网络中所有的结点所存储的密钥