第5章 无线传感器网络安全

目前，传感器网络在各个领域得到了广泛使用，经常用来采集一些敏感性数据或在敌对无人值守环境下工作。针对具体应用，在传感网的系统设计初期就应解决它的安全问题。然而传感网的资源有限，如有限的带宽资源、有限的存储能力和计算能力以及有限的能量，给传感器网络的安全带来了不同的挑战，传统的安全技术不能用于解决传感器网络的安全问题。目前针对传感器网络的安全研究主要集中在认证技术、密钥管理、安全路由、安全定位、隐私保护等方面。

5.1 无线传感器网络概述

无线传感器网络（WSN）近年来获得了广泛的关注，微机电系统的发展促进了智能传感器的产生，这些传感器体积小，具有有限处理能力和计算资源。相比传统的传感器，这类传感器不仅价格低廉，而且传感器节点可以感知、测量、收集数据，将经过决策的数据最终传给用户。每个传感器节点由传感器模块、处理器模块、无线通信模块和能量供应模块组成。传感器模块主要负责信息采集、数据转换等；处理器模块负责控制整个传感器节点的操作以及对节点采集和转发的数据进行处理；无线通信模块负责无线通信、交换控制信息和收发采集数据；能量供应模块为传感器节点提供运行所需的能量，电池是目前传感器的主电源。

无线传感器网的部署过程是通过人工、机械、飞机空投等方式完成的。节点随机部署在被监测区域内，以自组织的形式构成网络，因此无线传感器网络通常有很少或根本没有基础设施。根据具体应用不同，传感器节点的数量从几十个到几千个不等，这些传感节点共同工作，对周围环境中的数据进行收集，每一个传感器节点在网络中既充当数据采集者，又要对数据进行转发。和传统网络节点相比，它兼有终端和路由器的双重功能。无线传感器网络主要分为结构化和非结构化两种。非结构化的 WSN 中包含大量分布密集的传感节点，这些节点可以以 Ad Hoc 的方式进行部署。部署成功之后，因为节点数目较多，导致网络维护较困难，传感器节点只能在无人看管的状态下对数据进行监控。在结构化的 WSN 中，所有的或部分的传感器节点是以预先布置方式工作的，节点数目较少，因此网络的维护和管理较容易，如图 5.1 所示。传感器节点监测的数据通过其他节点以多跳中继的方式传送到汇聚节点，最后通过互联网或卫星到达管理节点。用户通过管理节点对无线传感器网络进行配

置和管理、发布监测任务以及收集监测数据。

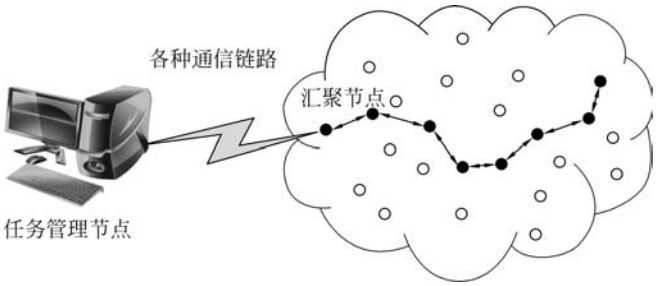

图 5.1 无线传感器网络的体系结构

5.1.1 无线传感器网络的特点

相比传统的计算机网络,无线传感器网络是一种特殊的网络,它的自身特点决定了它无法使用基于传统网络的安全机制。无线传感器网络具有如下特点。

(1) 有限的存储空间。传感器是一个微小的装置,只有少量的内存和存储空间用于存放代码,因此在设计一个有效的安全协议时,必须限制安全性算法的代码大小。例如,一个普通类型的传感器(TelosB)只有一个 8MHz 的 16 位 RISC CPU、10KB 的内存、48KB 程序存储器和 1024KB 的闪存存储空间。基于这样的限制,传感器中内置的软件部分也必须相当小,如 TinyOS 的总编码空间大约为 4KB,核心调度器只占用 178B,因此与安全相关的代码也必须很少。

(2) 有限的电源能量。能量问题是传感器的最大限制,目前传感器节点的能量供应大多还是依靠电池供电的方式,其他的能量供应方式如依靠太阳能、振动、温差等方式还不成熟。在传感器的应用中,必须考虑到单个传感器的能源消耗以及传感网的整体能耗。设计安全协议时,必须考虑该协议对传感器寿命的影响,以及加密、解密、签名等安全操作均会导致传感器节点消耗额外的功率,对一些密钥资料的存储也会带来额外的能量开销。

(3) 有限的计算能力。传感器网络节点是一种微型嵌入式设备,价格低,功耗小,有限的存储空间和电池能量必然导致其计算能力比普通的处理器功能弱得多,这就要求在传感器节点上运行的软件与算法不能过于复杂。

(4) 不可靠的信道。传感器网络中节点之间传输数据无须事先建立连接,但信道误码率较高导致了数据传输的不可靠性。同时由于节点能量的变化以及受高山、建筑物、障碍物等地势地貌和风雨雷电等自然环境的影响,传感器节点间的通信断接频繁,经常导致通信失败。

(5) 使用广播式信道。由于无线传感网采用广播式的链路类型,即使是可靠的信道,节点之间也会产生碰撞,即冲突。冲突的存在会导致信号传输失败,信道利用率降低。在密集型的传感网中,这是个尤为重要的问题。

(6) 延迟的存在。传感网属于多跳无线网络,网络的拥塞和节点对包的处理均会导致网络中的延时,从而使其难以实现传感器节点之间的同步。如果安全机制依赖对关键事件的报告和加密密钥分发,同步问题将成为传感器网络安全中至关重要的问题。

(7) 易受物理袭击。传感器可以部署在任何公开环境下,时常伴有雨、雾、霾等恶劣天

气。在这样的环境中，较放置在安全地点（如机房等地）的台式机而言，更容易遭受物理攻击。

（8）采用远程监控。传感器节点数量大，分布范围广，往往有成千上万的节点部署到某区域进行检测；同时传感器节点可以分布在很广泛的地理区域，这使得网络的维护十分困难，只能采用远程监控方式。但远程监控无法检测到物理篡改等攻击方式。因此传感器节点的软、硬件必须具有高强壮性和容错性。

（9）缺乏第三方的管理。无线传感器是自组织的网络，不需要依赖于任何预设的网络设施，传感器节点能够自动进行配置和管理，自组织形成多跳无线网络。无线传感器网络是一个动态的网络，一个节点可能会因为能量耗尽或其他故障而退出网络，新的节点也会被添加到网络中，网络的拓扑结构随时会发生变化。

（10）应用系统多样化。传感器网络用来感知客观物理世界，获取物理世界的信息量。不同的传感器网络应用关心不同的物理量，因此对传感器网络的应用系统有多种多样的要求，其硬件平台、软件系统和网络协议必然会有很大差别。

5.1.2　无线传感器网络面临的安全威胁

1. 被动攻击和主动攻击

同有线网络类似，传感网面临的安全威胁也主要分成两大类，即被动攻击和主动攻击。在被动攻击中，攻击者不会干扰用户之间的通信，目的是获得网络中传递的数据内容，典型攻击方式有窃听、流量分析、流量监控。在主动攻击中，攻击者会破坏用户之间的通信，对消息进行中断、篡改、伪造、重放以及拒绝服务攻击等。

（1）窃听。窃听是指攻击者通过监控数据的传输进行被动攻击，对数据进行监听。例如，放置在屋外的无线接收器可能监听到屋内传感网所检测到的光照和温度数据，从而推断出主人的一些日常习惯。加密技术可以部分抵抗窃听攻击，但是需要设计一个鲁棒的密钥交换和分发协议。只根据几个捕获到的节点，无法推断出网络内其他节点的密钥信息。由于传感器的计算能力有限，密钥协议必须简单可行。此外，传感器存储空间的有限性导致端到端加密不太可行，因为每个节点可能没有足够空间用于存储大量其他节点的信息，只能存储周围邻居节点的密钥信息。传感网主要支持数据链路层的加密技术。

（2）流量分析。流量分析是指对消息进行拦截和检查，目的在于根据消息通信模式推断出消息内容。

（3）拒绝服务攻击/分布式拒绝服务攻击。拒绝服务攻击是指攻击者通过耗尽目标节点的资源，令目标节点无法正常采集或者转发数据。

（4）重放攻击。重放攻击也称为中间人攻击，是指即使攻击者不知道密钥，无法对以前窃听到的消息进行解密，但仍会把以前截获到的消息，重复发送给目标节点。

（5）外部攻击和内部攻击。外部攻击是该攻击者不属于域内节点。内部攻击来源于域内节点，主要是指一些受损节点对网络内部进行主动攻击或者被动攻击。内部攻击和外部攻击相比更严重，因为内部攻击者知道更多的机密信息，具有更多的访问权限。

2. 协议栈攻击

按照 TCP/IP 模型,传感网的安全威胁还可以分为物理层、数据链路层、网络层、传输层和应用层的威胁,表 5.1 列出了每一层的安全威胁。

表 5.1 每层对应的安全威胁

层 次	安全威胁
应用层	抵赖、数据损坏
传输层	会话劫持、洪泛攻击
网络层	虫洞、黑洞、拜占庭、洪水、资源消耗、位置隐私泄露
数据链路层	流量分析、流量监控、MAC 破坏
物理层	干扰、拦截、窃听
多层攻击	DoS、伪造、重放、中间人攻击

(1) 物理层威胁。由于无线网络的广播特性,通信信号在物理空间上是暴露的。任何设备只要调制方法、频率、振幅、相位和发送信号匹配就能获得完整的通信信号,从而成功进行窃听攻击,同时还可以发送假消息进入网络。无线环境是一个开放的环境,所有无线设备共享一个开放空间,所以若有两个节点发射的信号在一个频段上,或者是频点很接近,就会因为彼此的干扰而不能够正常通信。如果攻击者拥有强大的发射器,产生的信号强度足以超过目标的信号,那么正常通信将被扰乱。最常见的干扰信号是随机噪声和脉冲。

(2) 数据链路层威胁。无线网络的广播特性会导致多个用户使用信道时发生冲突,因此每个节点只能工作在半双工的工作模式下。数据链路层的 MAC 协议负责进行信道资源的分配,解决信道竞争,尽力避免冲突。无线传感网中主要采用 CSMA/CA 技术解决多个站点使用信道的情况,MAC 协议假定多个站点能够自动按照 CSMA/CA 标准协调自己的行为,但是一些自私节点或者恶意节点会不按照正常的协议流程去工作。例如,自私节点可能会中断数据的传输;恶意节点可能在转发的数据中恶意改变一些比特位的信息;不断发送高优先级的数据包占据通信信道,使其他节点在通信过程中处于劣势;不断发送信息与其他用户的信号产生碰撞,破坏网络的正常通信;利用链路层的错包重传机制,使受害者不断重复发送上一个数据包,最终耗尽节点的资源。

(3) 网络层威胁。攻击者的目的在于吸收网络流量;让自己加入到源到目的的路径上,从而控制网络流量;让数据包在非最优路径上转发,从而增加延迟;将数据包转发到一条不存在路径上,使其不能到达目的地;产生路由环从而带来网络拥塞。恶意节点在冒充数据转发节点的过程中,可以随机地丢掉其中的一些数据包,即丢弃破坏;也可以将数据包以很高的优先级发送,从而破坏网络的通信秩序;还有可能修改源和目的地址,选择一条错误的路径发送出去,从而导致网络的路由混乱。如果恶意节点将收集到的数据包全部转向网络中的某一固定节点,该节点必然会因为通信阻塞和能量耗尽而失效;如果多个站点联合,会让其他节点误以为通过它们只需要一两跳就可以到达基站,从而把大量的数据信息通过它们进行传输,形成路由黑洞。网络层威胁包括虚假路由协议、选择性转发、槽洞(sinkhole)攻击、女巫(sybil)攻击、虫洞(wormhole)攻击、问候洪泛(hello flood)攻击、伪装应答、关键点攻击等。

(4) 传输层威胁。传感网中采用传输层 TCP 协议建立端到端的可靠连接,类似于有线网络,传感节点容易遭受到 SYN 泛洪攻击、会话劫持攻击。TCP 协议无法确定其原因,如拥塞、校验失败或恶意节点的袭击而造成。TCP 只会不断降低其拥塞窗口,从而使信道吞吐量减小,网络性能下降。会话劫持攻击发生在 TCP 建立连接之后,攻击者采用拒绝服务等方式对受害节点进行攻击,然后冒充受害节点身份(如 IP 地址),同目的节点进行通信。会话劫持攻击在 UDP 中较容易,因为不需要猜测报文的序列号。

(5) 应用层威胁。应用层袭击对攻击者有很大的吸引力,因为攻击者所搜寻的信息最终驻留在应用程序中。应用层威胁主要分为抵赖攻击和恶意代码的攻击,病毒、蠕虫、间谍软件、木马等恶意代码可以攻击操作系统和用户应用程序,并自行传播通过网络,导致整个传感网的速度减慢甚至崩溃。

(6) 多层威胁。多层威胁是指攻击者对网络的攻击发生在多个层次上,如拒绝服务攻击、中间人攻击等。

5.1.3　无线传感器网络的安全目标

为了抵御各种安全攻击和威胁,保证任务执行的机密性、数据产生的可靠性、数据融合的正确性以及数据传输的安全性等,无线传感器网络的安全目标主要包含以下几方面。

(1) 机密性。机密性是网络安全中最基本的特性。机密性主要体现在以下两个阶段:密钥派生阶段,节点的身份信息以及部分密钥材料需要保密传输;派生阶段后,节点通信需要用会话密钥进行加密。

(2) 完整性。机密性防止信息被窃听,但无法保证信息是否被修改,而消息的完整性能够让接收者验证消息内容是否被篡改。

(3) 新鲜性。两个节点间共享一个对称密钥,密钥的更新需要时间,在这段时间内攻击者可能重传以前的数据。为了抵抗重放攻击,必须保证消息的新鲜性,一般通过附加时间戳或者随机数加以实现。

(4) 可用性。与传统的网络安全可用性不同,传感器的资源有限,过多的通信量或计算量均会带来能量的过多消耗,单个传感器的消亡可能引起整个网络的瘫痪。传统的加密算法不适应无线传感器网络,必须设计轻量级的安全协议。

(5) 自治性。无线传感器网络不采用第三方架构进行网络管理,节点之间采用自组织方式进行组网。某个节点失效时,节点会自治愈重新组网,因此无线传感网属于动态网络。几种经典的密钥预分配方案并不适于传感网,节点间必须自组织进行密钥管理和信任关系的建立。

(6) 时钟同步。无线传感器网络的很多应用依赖于节点的时钟同步,因此需要一个可靠的时钟同步机制。如为了节省能量,传感器节点需要定时休眠;有时需要计算出端到端延迟,进行拥塞控制;为了对应用程序进行跟踪,需要组内的传感器节点整体达到时钟同步。

(7) 安全定位。通常情况下,一个传感器网络的有效使用依赖于它能够准确地对网络中的每个传感器进行自动定位。为了查到出错的传感器位置,负责故障定位的传感器网络需要节点的精确位置信息。攻击者通过报告虚假信号强度或者重放攻击等,可以伪造或篡改定位信息。

(8) 认证。为了保证通信双方身份的真实可靠性,节点之间必须进行认证,包括点到点认证和组播/广播认证。在点到点认证过程中,两个节点进行身份确认,会派生出单一会话密钥。组播/广播认证解决的是单一节点和一组节点或者所有节点进行认证的问题,此时需要维护的是组播/广播密钥。

(9) 访问控制。用户通过认证后,访问控制决定了谁能够访问系统、访问系统的何种资源以及如何使用这些资源。访问控制可以防止权限的滥用。

5.2 无线传感器网络安全路由协议

无线传感器网络自身的特点导致其无法直接采用传统的路由协议。另外,在路由的安全性方面,也需要重点关注。无线传感器网络中节点的能量资源、计算能力、通信带宽、存储容量都非常有限,而且无线传感器网络通常由大量密集的传感器节点构成,这就决定了无线传感器网络协议栈各层的设计都必须以能源有效性为首要设计要素。在无线传感器网络中,大多数节点无法直接与网关通信,需要通过中间节点进行多跳路由。因此无线传感器网络中的路由协议作为一项关键技术,在传感网络中占据重要地位。

5.2.1 安全路由概述

在无线传感器网络中,路由协议主要包括两方面的功能:在保证能量优先的前提下,寻找源节点和目的节点间的优化路径;根据找到的路径将数据分组正确地转发。对于现今的无线传感器网络,各国都提出过很多种路由算法,这些算法将传感器网络有限的能量和计算能力作为首要问题来解决,但对于安全问题的考虑相对较少。如果在网络协议的设计阶段没有给予安全问题足够的重视,而是通过后续的更新来补充安全机制,那么这款协议所消耗的人力物力将是巨大的。

大部分无线传感器网络路由协议在设计时没有考虑安全问题,针对这些路由协议的攻击常见的有以下几种。

(1) 涂改、伪造或重放路由信息。对路由协议最直接的攻击是针对两个节点交换的信息。基于涂改伪造或重放路由信息这种方法,攻击者可能会建立路由环线,攻击或击退网络流量,扩展或缩小源路由,产生虚假错误信息,造成网络分割,增加端到端延迟。

(2) 选择性转发。多跳网络通常假设参加的节点会诚实地转发接收到的消息。在一个选择性转发的攻击中,恶意节点会拒绝转发某些消息而仅仅是删掉它们,确定它们没有被传播得更远。在这种攻击中,恶意节点就像一个黑洞,拒绝转发它看到的一切包。但是这种攻击的冒险之处就是邻居节点会断定它失败了继而去寻找另一个路由。这种攻击通常在攻击者已经明确被包括在一个数据流的路径之内时是最有效的。我们相信,攻击者发射一个选择性转发袭击很可能会沿着阻力最小的路径并且试图把自己包括进真实的数据流之中。

(3) 天坑攻击。在无线传感器网络中,有些路由方案是依据链路质量和传输延迟来选路的。在这种情况下,某些恶意节点会利用诸如笔记本电脑这种拥有很强通信能力的终端混入正常的通信网络中,将自身伪装成一个通信质量很高的节点,以此欺骗环境中的其他节点,将大部分的通信流量吸引过来,对接收到的数据进行处理之后再选择性转发。

(4) sybil 攻击。在 sybil 攻击中，一个节点对于网络中其他节点呈现多种身份。sybil 攻击可以明显减少容错方案的有效性，如分布式存储、分散和多路径路由、拓扑维护等。副本、存储分区或者路由都是能够用一个攻击者呈现多个身份的相交节点。sybil 攻击也对地理路由协议造成了重大攻击威胁。

(5) wormhole 攻击。虫洞攻击是指两个以上的恶意节点共同发动攻击，两个处于不同位置的恶意节点会互相把收到的绕路信息经由私有路径传给另一个恶意节点，使这两个节点之间仿佛只有一步之隔。如图 5.2 所示，图中恶意节点之间存在一条高质量、低延迟的通信链路，左侧的恶意节点临近基站，这样较远处的恶意节点可以使周围节点相信自己有一条到达基站的高效路由，通过此方法就能将周围的通信流量吸引过来。

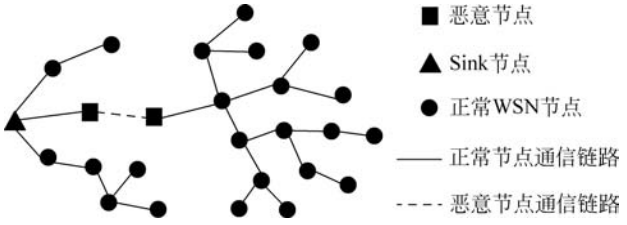

图 5.2　wormhole 攻击

(6) hello flood 攻击。hello flood 攻击是针对传感网的新型攻击，许多协议需要节点广播 hello 包向它们的邻居告知自己。接收这样 hello 包的节点也许会认为它是在发射频率范围内的正常发送方。一个笔记本电脑级别的攻击者用足够大的发射能量广播路由或者 hello 数据包，会使网络中的每个节点信服攻击者就是它的邻居。通常用洪水来表示消息像疫情一样通过每一个节点迅速传播，因此起名为 hello flood 攻击。

(7) 确认欺骗攻击。确认欺骗攻击的前提是该协议运用了链路层确认模式。无线传感器网络中的通信方式都是广播通信，恶意节点可以利用这个特征伪造一个确认包，并将其发送给消息源节点，从而使正常的消息发送节点错将一条低质量链路或者一个失效节点当成一条可成功送达的目的地，并向其不断传输数据，这样恶意节点就可以利用此漏洞发动攻击了。

5.2.2　典型路由协议及安全性分析

通过对无线传感器网络路由协议的研究，本文选取了一些相对比较重要和有代表性的路由协议，对其核心路由机制、特点和优缺点进行了介绍，重点分析了这些路由协议的安全特性和抗攻击能力。

1. Directed Diffusion 协议

Directed Diffusion 是一个典型的以数据为中心、查询驱动的路由协议，路由机制包含兴趣扩散、初始梯度建立以及路径加强三个阶段，如图 5.3 所示。

在兴趣扩散阶段，由汇聚节点周期性地广播兴趣消息到其邻居节点上，兴趣消息包含对象类型、目标区域、数据发送时间间隔、持续时间等四个部分。当节点收到邻居节点的兴趣消息时，如果该消息的参数类型不存在于节点的兴趣列表中，那么就建立一个新表项存储该

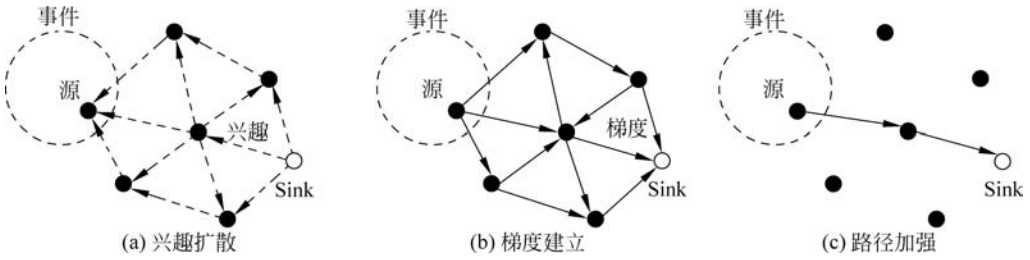

图 5.3 Directed Diffusion 协议的三个阶段

消息；如果节点中存在与该消息的某些参数相同的表项，则对该表项中的数据进行更新；如果该消息和刚刚转发的某条消息一样，则直接丢弃。初始梯度建立和兴趣扩散同时进行。在兴趣扩散过程中，节点在创建兴趣列表时，记录中已经包含了邻居节点指定的数据发送率即梯度。当节点具有与兴趣消息相匹配的数据项时，就把兴趣消息发送到梯度上的邻居节点，并以梯度上的数据传输速率为参照标准对传感器模块采集数据的速率进行设定。鉴于自身有多个邻居节点在网络环境中进行广播兴趣消息，汇聚节点有可能在这个阶段通过不同的路径接收到相同的数据。汇聚节点通过多个节点从源节点收到数据之后，将这条路径建立为加强路径，以保证接下来的数据能通过这条加强路径以较高的速率进行传输。大多数路径加强是以类似于链路质量、传输延迟等数据为标准进行选择的，这里我们以传输延迟为例进行概述。汇聚节点会最先选定最近发来数据的邻居节点作为这条加强路径的下一跳，并向该邻居节点发送相应的路径加强信息，以确保其及时对自身的兴趣列表进行更新；接下来该邻居节点会重复上面的步骤来确定自己的下一跳，这样的步骤会持续进行，直至路径加强信息传至源节点。

Directed Diffusion 具有一些新特点：以数据为中心的传输，基于强化适应性的经验最优路径，以及网络内数据汇聚和高速缓存。由于缺乏必要的安全防护，即使拥有这些优越的特性以及很好的健壮性，Directed Diffusion 仍然承受不了攻击者的攻击。基于 Directed Diffusion 的特点，攻击者可以对其造成如下的威胁：①攻击者将自己伪装成一个基站，广播兴趣消息。当节点接收到此信息并转发时，攻击者可以对目标数据进行监听；②攻击者可以利用不真实的加强或减弱路径以及假冒的匹配数据，以达到影响数据传输的目的；③攻击者通过向上游节点发送欺骗性的低延迟、高速率的数据来发动 sinkhole 或 wormhole 攻击；④攻击者通过对 sink 节点发动 sybil 攻击，可以阻止 sink 节点获取任何有效信息。

2. LEACH 协议

LEACH(low energy adaptive clustering hierarchy)是一种低能耗、自适应的基于聚类的协议，它利用随机旋转的本地簇基站来均分网络中传感器的能量负荷。LEACH 使用本地化的协作来启用动态网络的可扩展性和鲁棒性，并采用数据融合的路由协议来减少必须发送到基站的数据量。LEACH 的主要特点包括三方面：①对于簇设置和操作的本地化协调与控制。②簇基站或簇头以及相应簇的随机旋转。③用于减少全局通信量的本地压缩。

接下来简述 LEACH 筛选簇头节点的过程：一个节点自身随机生成一个 0 和 1 之间的数字，一旦这个随机生成数小于阈值 $T(n)$，则广播自身成为簇头节点的消息；之后在每一次循环中，簇头节点都会将自身阈值重置为 0，以保证自身不会再次成为簇头节点；随着循环的不断进行，其余未当选过簇头节点的节点成为簇头时的阈值也渐渐增大。阈值 $T(n)$ 的计算公式为

$$T(n)=\begin{cases}\dfrac{p}{1-p[r \bmod (1/p)]}, & n \in G\\ 0, & \text{其他}\end{cases}$$

其中 p 是所需的簇头百分比(如 $p=0.05$)；r 是当前轮次；G 是这一轮中没有成为过簇头节点的集合。

当簇头被选出以后，它开始向整个网络广播信息，网络中的非簇头节点根据接收到的广播信号的强弱来判读自身属于哪个簇，并向自己所属的那个簇的簇头节点发出相应的反馈信息。当整个网络正常工作以后，节点将自身收集到的数据发送给簇头节点，再由簇头节点将这些数据进行融合，进一步发送给汇聚节点。

利用大多数节点发射距离小的优点，我们设计了能够发送数据到基站的簇模式，只需要少数节点向基站发送长距离。LEACH 优于经典的聚类算法，利用自适应簇和旋转簇头，使系统的能源需求分布到所有的传感器。此外，LEACH 能够在每个簇中执行本地计算，以减少必须发送到基站的数据量，大幅度地减少了能量消耗。

鉴于网络中各个非簇头节点选择自己属于哪个簇是通过信号强弱来判定的，这就给了攻击者机会，使那些恶意节点可以通过增大自身信号强度来吸引那些非簇头节点，让节点们误以为它就是簇头节点，导致遭受选择性转发或天坑攻击。由于 LEACH 在设计过程中令所有节点都能与 BS 通信，这就保证自身对于虚假路由和 sybil 攻击有一定的抵御能力。

3. GPSR 协议

GPSR 是一种对于无线数据报网络的新型路由协议，协议设计每个节点可以利用贪心算法依据邻居与自身位置信息转发数据。算法的大致流程是当节点接收到数据以后，便开始以该数据为标准对本身存储的邻居节点列表进行处理。一旦自身到基站的距离大于列表中的邻居节点，那么节点就会将这个数据转发给它的邻居节点。

但是在实际的网络环境中，转发过程经常会出现“空洞”现象。如图 5.4 所示，在这个拓扑结构中，X 到基站 BS 的距离要小于 W 和 Y。根据贪心算法的转发机制，X 不会将 W 和 Y 作为自身转发列表中的下一跳。面对空洞问题时，我们可以利用右手法则来解决。当节点接收到通过右手法则转发过来的数据时，节点本身开始进行比较。只有自己到基站的距离大于邻居节点到基站的距离，才启用贪心算法对数据进行转发。

另外，GPSR 也有可能遭受到位置攻击，如图 5.5 所示。攻击者通过虚假信息将节点 B 的错误位置信息告知节点 C，让 C 误以为节点 B 在(2,1)，于是将数据转发给 B。而真实的节点 B 又会根据贪心算法将数据再发还给节点 C，如此下去就会导致整个网络因死循环而陷入瘫痪。

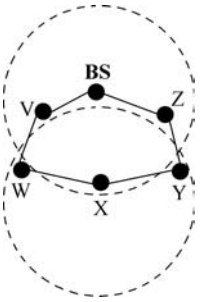

图 5.4 GPSR 中的空洞问题

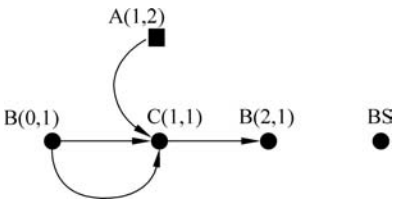

图 5.5 利用位置信息的攻击

5.3 无线传感器网络密钥管理

由于无线传感器网络的特点,很多成熟的有线或无线网络的密钥管理方案不能直接应用于无线传感器网络。对于无线传感器网络安全解决方案,加密技术是基础的安全技术,用于满足无线传感器网络的身份验证、保密性、不可抵赖性、完整性通过加密的安全性要求。对于加密技术,密钥管理是一个关键问题。通信安全性有四种类型的键:关键节点和基站之间的通信、该节点的节点密钥、基站和通信密钥中所有节点的组密钥在无线传感器网络之间的通信过程、更多的邻居节点。下面具体分析无线传感器网络及相关密钥管理方案。

5.3.1 密钥管理的评估指标

对于一个传统的网络,通过对密钥管理方案的分析就可以评估其优缺点,但这在无线传感器网络中是不够的。由于无线传感器资源约束的特点,无线传感器网络比传统的网络安全问题面临更多的挑战。因此,无线传感器网络的安全标准和传统网络不同。由于无线传感器网络自身的特点和局限性,无线传感器网络密钥管理方案的考核指标有以下几点:

(1) 安全性。不论是传统网络还是无线传感器网络,密钥管理的安全性都是至关重要的,它是所有解决方案的前提因素,包括保密性、完整性、可用性等。

(2) 对攻击的抵抗性。无线传感器网络中的传感器节点体积小,结构脆弱,很容易遭受物理攻击,导致网络信息被泄露。对攻击的抵抗性指的就是当网络中的某些节点被恶意俘获后对剩余网络部分中节点间正常安全通信造成的影响程度。理想状况下,当一个网络拓扑失去部分节点后,其他节点仍然可以正常地安全地通信。

(3) 负载。无线传感器网络中一共包含三种负载:通信负载、计算负载和内存负载。对于传感器网络中的节点来说,密钥管理方案必须要低耗能。而且节点之间广播通信时所消耗的能量远大于其自身的计算耗能,所以密钥管理的通信负载要尽可能小。由于节点有限的计算能力,传统网络中所采用的复杂的加密算法不适用于传感器网络,因此密钥管理方案要尽可能设计得简单些。由于节点的存储空间有限,不会保存过多密钥信息,因此合适的密钥管理方案要使每个节点预分配的信息尽可能减少。

(4) 可认证性。认证在无线传感器网络安全问题上是一个至关重要的步骤,网络中的节点可以通过认证机制抵御如节点冒充这样的攻击方式。因此,节点间的认证机制是否完

善也成为密钥管理方案评估的一项重要指标。

(5) 扩展性。在现实的传感器网络环境中,会部署成千上万的传感器节点,这就要求一个好的密钥管理方案要能支持大规模的网络拓扑。另外,它也要兼顾传感器网络的动态变化,如节点的加入和离开。当有的节点因遭受外界攻击或自身能源耗尽而不能正常工作时,密钥管理方案应该能够保证网络的后向安全性;当网络拓扑需要增加新的节点时,密钥管理方案应该能够保证网络的前向安全性。

(6) 密钥连接性。密钥连接性指节点之间直接建立通信密钥的概率。要想使无线传感器网络正常工作,就必须保持一个足够高的密钥连接概率。由于传感器网络中的节点很难与较远的节点相互直连通信,所以这一种情况是可以忽略的,不用考虑。密钥连接性只需确保邻居节点间建立通信密钥的概率足够高。

综上所述,在无线传感器网络中,要设计出一个适用于整个网络中可能出现的所有状况的密钥管理方案是很困难的,所以无线传感器网络安全问题的核心就是建立一个完备的安全密钥管理方案。

5.3.2　密钥管理分类

通常情况下,传感器节点的能耗、密钥管理方案所能支持的最大网络规模、整个网络可建立安全通信的连通概率、整个网络的抗攻击能力都是设计无线传感器网络密钥管理方案的必要要求,方案必须满足这些要求。下面我们依据这些方案和协议的特点对密钥管理方案进行适当的分类。

1. 对称密钥管理与非对称密钥管理

基于使用的密码机制,无线传感器网络密钥管理可以分为对称密钥管理和非对称密钥管理两类。在对称密钥管理之中,节点间通信使用相同的密钥和加密算法来对传输的数据进行加密解密。对称密钥管理具有相对较短的密钥长度、相对较小的计算通信和存储开销,这也是无线传感器网络密钥管理的主要研究方向。对于非对称密钥管理,节点使用不同的加密解密密钥。鉴于非对称密钥管理使用了多种加密算法,所以它对于传感器节点的计算存储通信能力要求较高。如果不加修改,难以运用到无线传感器网络中。一些研究认为优化之后的非对称密钥管理也适用于无线传感器网络,但是从安全级别的方向考虑,非对称密钥管理机制的安全性要远高于对称密钥管理机制。

2. 分布式密钥管理和层次式密钥管理

根据网络拓扑结构的不同,无线传感器网络密钥管理可以分为分布式密钥管理和层次式密钥管理两类。在分布式密钥管理中,传感器节点具有相同的通信与计算能力,节点自身密钥的协商、更新通过使用其预分配的密钥以及与周边节点的相互协作来完成。而在层次式密钥管理中,传感器节点被分配到不同的簇中,每个簇的簇头节点负责处理普通节点的密钥分配、协商与更新等。分布式密钥管理的优点是邻居节点间协同作用强,分布特性很好;层次式密钥管理的优点是大部分计算集中在簇头节点,降低了对普通节点计算和存储能力的需求。

3. 静态密钥管理与动态密钥管理

依据传感器网络中节点在部署完毕后密钥是否再次更新,可将无线传感器网络分为静态密钥管理和动态密钥管理两类。在静态密钥管理中,传感器节点在部署到特定区域之前会对其预分配一定的密钥,部署后通过数据交流来生成新的通信密钥。该通信密钥的生存周期为整个网络运行时期,其间不会发生改变。在动态密钥管理中,网络中的密钥需要周期性地进行分配、更新、撤回等操作。静态密钥管理具有通信密钥无须多次更新的特点,保证了计算和通信的开销不会过高。可一旦某些节点受损,该网络就会面临安全威胁。而动态密钥管理则会周期性地更新通信密钥,使攻击者不会轻易地通过捕获节点来盗取通信密钥,确保了网络运行的安全性。但是这种周期性的更新操作会产生大量的计算和通信开销,大幅度增加了整个网络系统的能源消耗。

4. 随机密钥管理与确定密钥管理

由传感器节点密钥分配方案的不同,可以将无线传感器网络密钥管理分为随机密钥管理和确定密钥管理两类。在随机密钥管理中,传感器节点获取密钥的方式犹如从一个或多个巨大的密钥数据库中随机抽取一定数量的密钥,节点间的密钥连通率介于 0 和 1 之间。而在确定密钥管理中,节点是通过位置信息、对称多项式等固定的方法获取密钥的,节点间的密钥连通率一直为 1。随机密钥管理具有分配方式简单、节点部署自由等优点,缺点是分配方案具有一定的盲目性,容易导致节点存贮空间的浪费。而确定密钥管理对于节点的密钥分配具有很强的针对性,能够高效地利用节点的存储空间,方便地在节点间建立连接,但是部署方式的局限性以及节点间通信和计算的高耗能也成为了这种方案的弊端。

5. 组密钥管理

1) 组密钥管理概述

还有一种与以上分类都不同的管理方案,即组密钥管理方案。组密钥是所有组成员都知道的密钥,用来对组播报文进行加密/解密、认证等操作,以满足保密、组成员认证、完整性等需求。相比对单播的密钥管理,前向私密性、后向私密性和同谋破解是组密钥管理特有的问题。

前向私密性主要是针对网络中出现节点退出现象后的反映。这种现象发生后,前向私密性就会禁止退出的节点(包括主动退出的节点或被强制退出的节点)再次参与组通信,而剔除这些节点之后新生成的组密钥同样能够实现向前加密。后向私密性则要求网络中新加入的节点不能完成对其加入前组播报文的破解。

组密钥管理是一个负责的管理机制,既要预防单个节点的攻击,也要兼顾多个节点的联合攻击。一旦多个节点掌握了足够的信息联合起来对整个系统进行破解,那么无论密钥更新得多频繁,攻击者也会实时掌握最新的密钥,进而导致组密钥管理机制的失败,前向私密性和后向私密性都无法实现,使整个系统被完全破解,这就达到了同谋破解的目的。因此在设计组密钥管理机制的时候要避免同谋破解。

2) 组密钥管理的影响因素

除了上述这三个问题以外,组密钥管理还会受到下面这些因素的影响:

(1) 差异性。组密钥管理涵盖很多通信节点,这些节点之间存在着各种各样的差异,如安全级别、功能、通信带宽、计算能力、服务类型等。为了适应这些差异,在设计组密钥管理方案时要统筹兼顾。

(2) 可扩展性。传感器网络的拓扑并不是固定不变的。随着规模的不断扩大,密钥的数量也会不断增多,所需的计算量、传输带宽、更新时间也会大幅增加。

(3) 健壮性。点对点通信时,一方失效整个通信则会终止。但是对于大规模的组通信来说,即使部分节点失效也不应该给整个网络的会话造成严重影响。

(4) 可靠性。可靠性是确保组密钥管理机制能够有效工作的重要性能。组播传输通常是不可靠的,乱序、丢包、重复信息等情况经常发生。如果设计的组密钥管理没有足够好的可靠性,将无法保证组成员在网络中的正常通信。

3) 设计组密钥管理时应考虑的因素

综上所述,设计一个完善的组密钥管理方案需要考虑的因素如下所示。

(1) 前向私密性:组内节点退出后将无法再次参与到组播通信中。

(2) 后向私密性:新加入的节点无法破译其加入之前的组播报文。

(3) 抗同谋破解性:防止多个攻击者节点联合起来破解组密钥。

(4) 生成密钥的计算量:由于能源有限,要考虑更新密钥时的计算量给节点带来的负担。

(5) 发布密钥占用带宽:不能让发布密钥过多占用有限的传输带宽。

(6) 发布密钥的延迟:降低延迟以确保组内节点及时获取最新密钥。

(7) 健壮性:即使一些节点失效也不会影响整个网络的正常通信。

(8) 可靠性:确保密钥的发布和更新操作能顺利进行。

5.3.3　密钥管理典型案例

1. LEAP 密钥管理方案

LEAP(localized encryption and authentication protocol)是一个密钥管理的安全框架协议。为了确保网络的安全,总共需要 4 种密钥:①独占密钥:每个传感器节点与基站的共享密钥;②对密钥:每个节点与其他传感器节点通信的共享密钥;③簇密钥:同一通信群组内的节点所共用的加密密钥;④群组密钥:整个网络中所有节点共享的密钥。

1) 独占密钥

独占密钥用于保证单个传感器节点与基站的安全通信,传感器节点可使用这个密钥计算出感知信息的消息论证码(MAC)以供基站验证消息来源的可靠性,也可以用这个密钥来举报它周围存在的恶意节点或者它所发现的邻居节点的不正常行为给基站。基站可使用这个密钥给传感器节点发布指令。

这个密钥是在节点布置之前预置到节点中的。节点 u 的独占密钥 K_{um} 可用一个伪随机函数 f 来生成 $K_{um}=f_{K_m}(u)$,K_m 是密钥生成者用于生成独占密钥的主密钥。密钥生成者只需要存储 K_m,在需要与节点 u 通信的时候再用伪随机函数计算出它们之间的通信密钥。

2) 对密钥

对密钥是指每个节点与它的一跳邻居节点的共享密钥,用于加密需要保密的通信信息或者用于源认证,既可以在节点布置之前预置,也可以在节点布置以后通过相互通信进行协商。协议假设整个网络的初始化时间 $T_{\min}$ 内攻击者不会对节点造成威胁,并且在 T_{est} 时间内新加入网络的节点可以与邻居节点协商好共同密钥($T_{\min} > T_{\text{est}}$),新入网的节点 u 与其邻居节点建立起对密钥的过程如下:

(1) 初始状态时,密钥生成者给节点 u 初始化密钥 K_1,每个节点计算出自己的独占密钥 $K_u = f_{K_1}(u)$。

(2) 节点 u 被散布到目标区域后,广播自己的身份信息 u 给它的邻居节点 v;收到广播信息的节点回复自己的身份 v 给节点 u,并且附加一个对自己身份证明的 $\text{MAC}(K_v, u|v)$ 信息。节点 u 可对 v 回送的身份信息进行验证,并用 K_1 以及伪随机函数 f 计算出 v 的主密钥 K_v,$K_v = f_{K_1}(u)$。

(3) u 通过伪随机函数 f 计算得到与 v 的对密钥 $K_{uv} = f_{K_v}(u)$,节点 v 可采用相同的计算方式得到与 u 的对密钥。

3) 簇密钥

簇密钥是一个节点与它通信范围内的邻居节点所共享的密钥,用于加密本地广播通信,可用于网络内部的数据聚合或者新节点的加入,在对密钥建立以后协商建立。簇密钥的生成过程为:由节点 u 生成一个随机密钥 K_{uc},用 $v_1, v_2, v_3, \cdots, v_m$ 与邻居的对密钥 K_{uv} 加密 K_{uc} 广播给所有邻居节点,邻居节点 v 在收到节点 u 的簇密钥后,回送自己的簇密钥给节点 u。如果节点 u 的一个邻居节点被撤销了,节点 u 可以生成新的簇密钥并且广播给它的合法邻居节点 v。

4) 群组密钥

群组密钥指基站与所有传感器节点共用的密钥,用于基站广播加密信息给整个网络中的节点。生成群组密钥最简单的方式是在节点散布到目标区域之前给所有的节点置入一个相同的、与基站通信的密钥。由于全网使用相同的群组密钥,当有节点被撤销时必须更新这个密钥,以防被撤销节点还能监听基站与每个节点的广播通信,可采用 uTESLA 协议更新网络的群组密钥。

2. Eschenauer 随机密钥预分配方案

Eschenauer 和 Gligor 在 WSN 中最先提出随机密钥预分配方案(简称 E-G 方案)。该方案由 3 个阶段组成:第 1 阶段为密钥预分配阶段。部署前,部署服务器首先生成一个密钥总数为 P 的大密钥池及密钥标识,每一节点从密钥池里随机选取 k($k \ll P$)个不同密钥。这种随机预分配方式使得任意两个节点都能够以一定的概率拥有共享密钥。第 2 阶段为共享密钥发现阶段。随机部署后,两个相邻节点若存在共享密钥,就随机选取其中一个作为双方的配对密钥,否则进入到第 3 阶段。第 3 阶段为密钥路径建立阶段。节点通过与其他存在共享密钥的邻居节点经过若干跳后建立双方的一条密钥路径。

根据经典的随机图理论,节点的度 d 与网络节点总数 n 存在以下关系:

$$d = \left(\frac{n-1}{n}\right)[\ln n - \ln(-\ln P_c)]$$

其中，P_c 为全网连通概率。

若节点的期望邻居节点数为 n'（$n' \ll n$），则两个相邻节点共享一个密钥的概率 $P' = d/(n'-1)$。在给定 P' 的情况下，P 和 k 之间的关系可以表示如下：

$$P = 1 - [(P-k)!\,]2/[(P-2k)!\;P!\,]$$

E-G 方案在以下 3 方面满足和符合 WSN 的特点：一是节点仅存储少量密钥就可以使网络获得较高的安全连通概率。例如，要保证节点数为 10 000 的 WSN 保持连通，每个节点仅需从密钥总数为 100 000 的密钥池随机选取 250 个密钥即可满足要求。二是密钥预分配时不需要节点的任何先验信息，如节点的位置信息、连通关系等。三是部署后节点间的密钥协商无须 Sink 的参与，使得密钥管理具有良好的分布特性。

3. 基于组合论的密钥预分配方案

Camtepe 用组合设计理论(combinatorial design theory)来设计 WSN 的密钥预分配方案。假设网络的节点总数为 N，用 n 阶有限射影空间(finite projective plane)(n 为满足 $n^2+n+1 \geqslant N$ 的素数)生成一个参数为($n^2+n+1, n+1, 1$)的对称 BIBD(balanced incomplete block design，平衡不完全区组设计)，支持的网络节点数为 n^2+n+1，密钥池的大小为 n^2+n+1，能够生成 n^2+n+1 个大小为 $n+1$ 的密钥环，任意两个密钥环至少存在一个公共密钥，并且每一密钥出现在 $n+1$ 个密钥环里。可见，任意两个节点的密钥连通概率为 1。但素数 n 不能支持任意的网络规模。例如，当 $N > n^2+n+1$ 时，n 必须是下一个新的素数，而过大的素数则会导致密钥环急剧增大，突破节点的存储空间，导致不适用于 WSN。使用广义四边形(generalized quadrilateral，GQ)可以更好地支持大规模网络，如 GQ(n，n)，GQ(n，n^2)和 GQ(n^2，n^3)分别支持的网络规模达到 $O(n^3)$、$O(n^5)$和 $O(n^8)$，但也存在着素数 n 不容易生成的问题。

为此，Camtepe 提出了对称 BIBD 与 GQ 相结合的混合密钥预分配方案：使用对称 BIBD 或 GQ 生成 b 个(b 值大小由 BIBD 或 GQ 决定，$b < N$)密钥环；然后使用对称 BIBD 或 GQ 的补集设计随机生成 $N-b$ 个密钥环，与前面生成的 b 个密钥环一起组成 N 个密钥环。这种混合的密钥预分配方案提高了网络的可扩展性和抗毁性，但不保证节点的密钥连通概率为 1。无论是对称 BIBD、GQ 还是混合方案，都比 E-G 方案的密钥连通概率更高，平均密钥路径长度也更短。

5.4 无线传感器网络认证机制

认证技术是信息安全理论与技术的一个重要方面。认证主要包括实体认证和信息认证两方面。实体认证用于鉴别用户身份，给网络的接入提供安全准入机制，是无线传感器网络安全的第一道屏障；信息认证用于保证信息源的合法性和信息的完整性，防止非法节点发送、伪造和篡改信息。

5.4.1 实体认证机制

为了让具有合法身份的用户加入到网络中并有效地阻止非法用户的加入，确保无线传

感器网络的外部安全,在实际应用的无线传感器网络中,必须要采取实体认证机制来保障网络的安全可靠。

由于无线传感器网络中通常需要大规模、密集配置传感器节点,为了降低成本,传感器节点一般都是资源严格受限的系统。一个典型的传感器节点通常只有几兆赫至几十兆赫的主频、几十千字节的存储空间以及极其有限的通信带宽,因此传统的认证协议不能直接在无线传感器网络中加以应用,需要研究、设计出计算量小、对存储空间要求不高且高效的适合于无线传感器网络的认证机制。目前的实体认证协议主要是在公钥算法和共享密钥算法的基础上提出的。

经过国内外学者的不断研究,无线传感器网络安全方面已经取得了很大进展,并且在认证方面也提出了许多方法,但是大多数学者都认为计算复杂、步骤繁复的公钥认证模式仍不适用于资源有限的传感器网络。不过,随着研究的深入,国内外一些学者也提出了一些基于公钥算法的认证协议在无线传感器网络中进行应用。

下面分别介绍基于 RSA 和 ECC(elliptic curves cryptography,椭圆曲线密码)两种公钥算法的实体认证协议在无线传感器网络中的应用。

1. 基于 RSA 公钥算法的 TinyPK 实体认证方案

对于公钥算法来说,虽然使用私钥进行解密和签名操作所需的计算量及消耗的能量比较大,但使用公钥进行加密和验证操作所需的计算量及消耗的能量却相对要小很多,同时速度也比较快。考虑到计算量和能量消耗的不对称性,我们可以让传感器节点只负责执行公钥算法中的加密和验证操作,把计算量大、能量消耗多的解密和签名操作交给基站或者与无线传感器网络建立安全通信的外部组织来完成。正是基于这种思想,R. Watro 等提出了基于低指数级 RSA 算法的 TinyPK 实体认证方案。TinyPK 是首次提出采用 RSA 公钥算法建立起来的 WSN 实体认证机制,通过合理分配加解密与签名验证任务,这种公钥算法可以方便地在 WSN 中进行实体认证。

与传统的公钥算法的实现相似,TinyPK 也需要一定的公钥基础设施(public key infrastructure,PKI)来完成认证工作。首先需要一个拥有公私密钥对的可信的认证中心(CA),显然,在无线传感器网络中这一角色可由基站来扮演(通常认为基站是绝对安全的,它不会被攻击者俘获利用)。任何想要与传感器节点建立联系的外部组织也必须拥有自己的公私密钥对,同时,它的公钥需要经过认证中心的私钥签名,并以此作为它的数字证书来确定其合法身份。最后,每个节点都需要预存有认证中心的公钥。

TinyPK 认证协议使用的是请求-应答机制,即该协议首先由外部组织给无线传感器网络中的某个节点发送一条请求信息。请求信息中包含两个部分:一个是自己的数字证书(即经过认证中心私钥签名的外部组织的公钥),另一个是经过自己的私钥签名的时间标签和外部组织公钥信息的校验值(或者称散列值)。请求信息中的第一部分可以让接收到此消息的传感器节点对信息源进行身份认证,而第二部分则可以抵抗重放攻击(时间标签的作用)和保证发送的公钥信息的完整性(散列值的作用)。传感器节点接收到消息后,先用预置的认证中心的公钥来验证外部组织身份的合法性,进而获取外部组织的公钥;然后用外部组织的公钥对第二部分进行认证,进而获取时间标签和外部组织公钥的散列值。如果时间标签有效并且实际计算得到的外部组织的公钥的散列值与第二部分之中包含的散列值完全

相同，则该外部组织可以获得合法的身份。随后，传感器节点将会话密钥用外部组织的公钥进行加密，然后传送给外部组织，从而建立起二者之间安全的数据通信。外部组织与传感器节点整个通信过程如图 5.6 所示。

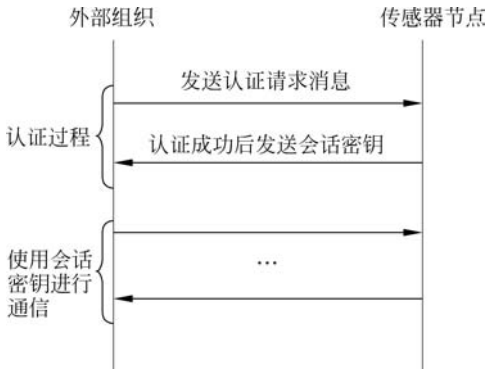

图 5.6　TinyPK 认证协议中外部组织与传感器节点的通信过程

传感器节点在认证过程中的工作流程如图 5.7 所示。

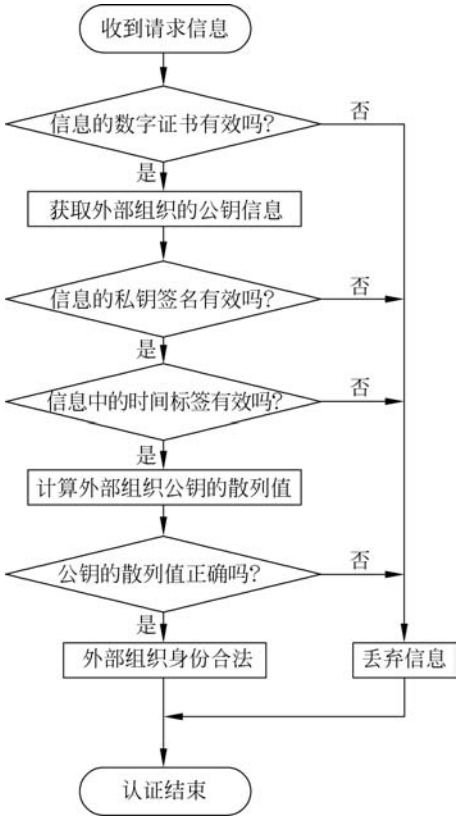

图 5.7　TinyPK 认证协议中节点的工作流程

2. 基于 ECC 公钥算法的强用户认证协议

上面介绍的基于 RSA 公钥算法的 TinyPK 实体认证方案虽然能够实现公钥算法在

WSN 中的应用,但它仍然有自己的缺点,比如,如果网络中某个认证节点被捕获(考虑到无线传感器网络的实际应用环境,网络中的某个或者某一些认证节点被捕获的可能性是比较大的),那么整个网络的安全性都会受到威胁,因为攻击者可以通过这个被捕获的节点获得与之相关的会话的密钥并以合法身份存在于网络之中。

针对这个问题,Z. Benenson 等提出了基于 ECC 公钥算法的强用户认证协议。与 TinyPK 相比,该协议有两点重要改进:

(1) 公钥算法使用 ECC 而不是 RSA。首先,和 RSA 一样,采用 ECC 公钥算法也能够完成加解密、签名与验证工作,从而可以在无线传感器网络中建立公钥基础设施来顺利实现认证工作和密钥的管理。并且,在达到相同的安全强度的条件下,与 RSA 相比,ECC 需要的密钥长度更短,对用于保存密钥的存储空间的需求也相应减小。

(2) 采用 n 认证取代了 TinyPK 协议中使用的单一认证。这一点非常重要,它不但可以应付网络中的节点失效问题,同时还解决了 TinyPK 实体认证协议中单个认证节点被捕获就可能导致网络受到安全威胁的问题。

基于 ECC 公钥算法的强用户认证过程如下:

(1) 外部组织向其通信范围内的 n 个传感器节点广播一个请求数据包(U, cert_u),其中 U 是外部组织的身份信息; cert_u 是合法的外部组织从认证中心获得的数字证书,即由认证中心私钥签名的外部组织的公钥。

(2) 某个传感器节点 S_i 在收到请求数据包后保存下来并同时给请求方返回一个应答数据包(S_i, nonce_i),其中 S_i 是该传感器节点自己的身份信息,nonce_i 是一个一次性随机数。每个接收到外部组织请求信息的传感器节点都执行同样的操作。

(3) 外部组织收到 S_i 返回的数据包后,用散列函数计算出一个散列值 $h(U, S_i, \text{nonce}_i)$,并用私钥签名后重新发送给 S_i。

每一个传感器节点 S_i 先验证 cert_u 以获得外部组织的公钥,然后用外部组织的公钥去验证第三个步骤中收到的散列值 $h(U, S_i, \text{nonce}_i)$并与实际执行 $h(U, S_i, \text{nonce}_i)$函数所得到的散列值进行对比。如果相同,则该节点通过外部组织的认证。

(4) 每一个对请求方 P 认证成功的节点 S_i 使用共享密钥计算出消息认证码并返回给 P。如果 P 得到了 $n-t$ 个消息认证码,则它在无线传感器网络中拥有合法的身份。

整个认证过程如图 5.8 所示。

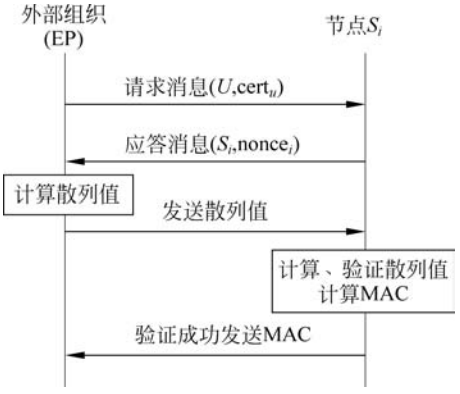

图 5.8 基于 ECC 公钥算法的强用户认证过程

每个传感器节点收到认证请求数据包后的认证流程如图 5.9 所示。

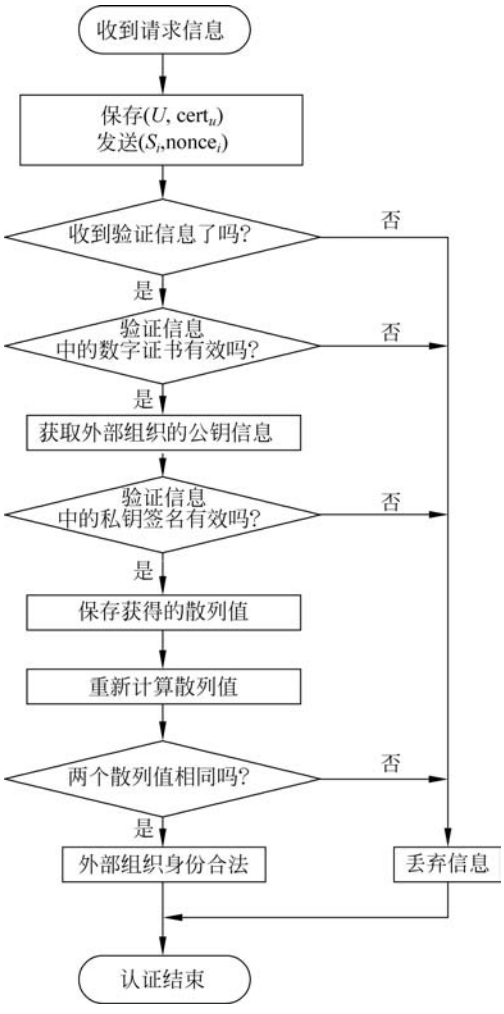

图 5.9　基于 ECC 公钥算法的节点认证过程

这种认证协议的安全强度相对比较高，但节点能量消耗也比较大。另外，对于拒绝服务攻击(DoS)，它没有很好的防御措施，需要另外添加入侵检测机制来处理。

5.4.2　信息认证机制

为了防止处于危险环境中的无线传感器网络遭受恶意节点的攻击，无线传感器网络需要采用消息认证机制来确保数据包的完整性以及信息源的合法性。在无线传感器网络的通信模式中，既包含小规模网络中节点与基站、节点与节点间的单跳传输，也有大型网络中的多跳传输。面对这样的情况，无线传感器网络所采用的消息认证机制也有所不同。

1. 无线传感器网络单跳通信模式下的信息认证

在小规模的无线传感器网络中，由于所有的节点都在基站的通信范围以内，所以基站可

以方便地向网络中所有节点广播信息,而网络中的每个节点也可以以单跳的通信方式向基站反馈数据。为了确保单跳通信模式传感器网络的合法性,在此需要引入单播源认证和广播源认证。

1) 单播源认证

节点与基站之间的单播通信认证是比较容易实现的,只需让基站与节点共享一对密钥对即可。在发送信息之前,发送方根据共享密钥对和发送信息计算出一个 MAC 值随消息一起发出;接收方接收到这个消息后利用共享密钥和接收到的消息计算出一个 MAC 值,然后进行对比;如果一致则确信这条消息源自一个合法的数据源。

2) 广播源认证

A. Perrig 等研究人员在 TESLA(timed efficient stream loss-tolerant authentication)协议的基础上提出了基于广播源认证机制的协议,使其能较好地适用于无线传感器网络。该协议的主要思想是利用哈希链在基站生成密钥链,传感器网络中的每个节点预先保存该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,基站按照时间顺序使用密钥链上的密钥加密消息认证码,并随着时间段的推移逐渐公布该密钥。传感器节点利用认证信息来认证基站公布的密钥,并对其进行消息认证码的验证。该协议采用对称加密,很好地适应了传感器网络资源受限的特点,但是由于认证信息是预先储存的,导致该协议的扩展性较差。

2. 无线传感器网络多条通信模式下的消息认证

在大规模的无线传感器网络中,传感器节点需要将收集到的信息传送给目的节点。如果两者之间的距离相对较远,通信的方式则会采用多条路由的方式。传统网络的消息认证方式通常是通信双方共享一个密钥,或者采取公钥加密解密的认证方式,但无线传感器网络节点的存储空间和资源有限,不可能完成这样一种方案,所以多跳通信模式下认证机制的设计就显得较为困难。现在存在一种多条通信模式下的认证方法——逐跳认证方式,就是在每一条一对一的通信链路上都共享一个密钥,这样就可以通过每一跳的认证来确保真正通信双方的信息认证。这种方案的弊端是一旦链路上的某几个节点被俘获了,整个网络的通信安全就会受到严重影响,因此这种认证方案具有很强的局限性。

而多路径认证方式则可以在一定程度上解决这个问题。该方法的基本思想是信息源通过多条不相交的路径将信息传送给目的节点,目的节点会根据收到的不同版本的数量选择占大多数的那个作为合法信息,并将发送其他本版信息的路径定位为不可信路径。这样就使得即使网络中某几个节点被恶意俘获也不会影响通信双方的安全通信。但是该方式的不足之处就是耗能过高,多跳不相交路径上的节点都需要为这次通信服务,极有可能导致因信息泛洪而使网络部分瘫痪。

H. Vogt 提出的另一种虚拟多路径认证方案可以较好地解决上一方案出现的问题。它的主要流程是网络中的每个节点先与跟自己距离为一跳和两跳的节点分别共享一个密钥,然后节点 s 针对下一跳和下两跳的节点计算出两个 MAC 值,随消息传输出去;同时转发自身上一跳节点 s' 对自身下一跳节点 s'' 的 MAC 值;下一跳节点 s'' 验证收到的两个 MAC,如果都是合法的,则重复节点 s 的上一步操作,保证消息在传输的过程中完成双重认证。该方案融合了上述两种认证机制的优点,很好地提高了信息传输过程中的信息认证强度。

5.5　无线传感器网络的位置隐私保护

无线传感器网络中的隐私可以分为两大类：数据隐私和上下文隐私，具体分类详见图 5.10。数据隐私通常是为了保护传感器节点发送或接收的数据包内容不被攻击；而上下文隐私则侧重于对得到关注的周围上下文信息内容的保护，其中位置隐私是一种典型的上下文隐私。

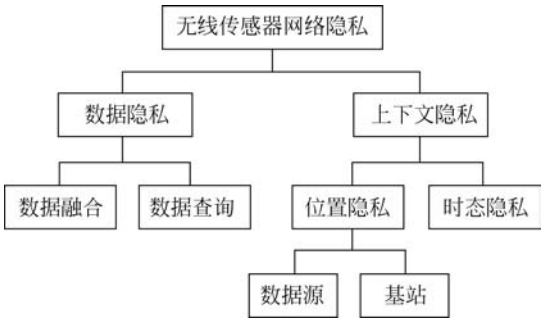

图 5.10　无线传感器网络的隐私分类

数据隐私保护是指对网络收集到的数据和向某个网络查询的数据信息的保护，主要有两类攻击者：外部攻击者和内部攻击者。外部攻击者只是窃听网络通信，通过简单的加密就可以防御这类的攻击者；而内部攻击者可以捕获一个或多个节点，最简单的防御方法就是实现节点和基站之间端到端的加密，然而这样就不能达到数据融合的目的。因此，面临的挑战是既要实现隐私保护，又要实现数据融合。

虽然可以通过数据加密等技术来保护数据隐私，但是无线通信媒介仍然暴露在网络中，一些上下文的隐私信息可能会暴露。典型的上下文隐私主要分为源节点位置隐私、汇聚节点位置隐私和事件发生的时间隐私，这些信息可以轻松地被具有流量分析功能的外部攻击者获得。接下来将着重介绍位置隐私。

5.5.1　位置隐私保护机制

无线传感器网络位置隐私保护主要是指对 WSN 中关键节点位置隐私的保护，因为这些节点有更多的职责，承担着比普通节点更多的任务，攻击者攻击掉这些节点对整个网络的危害最大。无线传感器网络中的关键节点一般分为源节点和汇聚节点两类。因此，无线传感器网络位置隐私保护主要分为源节点位置隐私的保护和汇聚节点位置隐私的保护。在介绍位置隐私保护前，先简要描述一下攻击者。

在 WSN 的位置隐私保护中，主要有两类攻击者会对其发动攻击，即局部攻击者和全局攻击者。局部攻击者的无线监测半径是有限的，因此，同一时间只可以监测到网络局部范围内的流量；而全局攻击者则可以一次监测整个网络的流量，并且很快定位传输节点。逐跳追踪数据包传输的攻击者和全局流量分析的攻击者则是两种典型的攻击者，下面我们分别介绍这两种攻击者。

（1）逐跳追踪数据包传输的攻击者：分为逐跳追踪汇聚节点位置的攻击者和逐跳追踪

源节点位置的攻击者。这里以逐跳追踪源节点位置的攻击者为例进行攻击描述。攻击者通常配备有特定的无线信号定位装置,此类装置可以监测以其为中心的一定半径长度内的节点。一般情况下,此类攻击者的网络监测半径和一般节点的传输半径相差无几,我们认为二者相等。攻击者在对源节点进行攻击时,其追踪方向和数据包传输方向是相反的。详细的攻击过程如下:攻击者潜伏在 Sink 附近来监测一定传输半径内的信号;监测到新的信号后,它会在很短的时间内判断出发送此信号的节点方向,并移动到该节点继续监听;如此反复,直到追踪到源节点。

(2) 全局流量分析的攻击者:这种攻击者具有很强的攻击能力,它能够监测整个网络的无线通信,从而了解整个网络的流量情况。基于此,它可以很快找到源节点或者 Sink 节点。

1. 源节点位置隐私保护

源节点通常是最靠近被监测对象的节点,另外源节点还会把采集到的数据发送到汇聚节点。如果无线传感器网络是为了监测珍稀资源,那么被监测对象的地理位置隐私一旦暴露,将对整个网络的正常运行造成重大危害。如在 Panda-Hunter 模型中,一旦源节点的位置被监测到,熊猫将会面临被攻击者捕获的危险。

2. 汇聚节点位置隐私保护

Sink 是无线传感器网络与外部网络连接的网关。WSN 与外界网络交互必须经过 Sink,同时向整个网络发布监测任务也需要 Sink 来完成。如果 Sink 被攻击了,整个网络可能会瘫痪。除此之外,所有源节点采集到的数据都会传输给汇聚节点,这导致整个网络中的流量不均衡,使流量分析的攻击者可以对汇聚节点进行攻击。

5.5.2 典型的无线传感器网络位置隐私保护方案

通过对无线传感器网络位置隐私保护的研究,并结合一些资料中的观点方案,我们对无线传感器网络中的位置隐私保护方案进行了归类。接下来将主要对典型的汇聚节点位置隐私保护方案和典型的源节点位置隐私保护方案进行介绍。

1. 典型的汇聚节点位置隐私保护方案

保护汇聚节点位置隐私的方案主要分为假包注入、多路径传输、随机行走等。

1) 假包注入

Deng 等阐明了保护汇聚节点位置隐私的重要性,并提出了当网络中没有数据包传输时,可发送假包来迷惑攻击者。在文献中,作者提出了基于多路径传输的假包注入,以此来更好地保护汇聚节点的位置隐私,延长攻击者捕获到汇聚节点的时间。另外,假包的传输是选择一个远邻居来进行传输的,这样保护效果更佳。

2) 多路径传输

所谓多路径传输就是数据包可选择多条路径进行传输,而不是在特定的某条路径中传输。作者在文献中提出了多路径路由和假包传输的融合方案。此方案中,对于某一节点,传入和传出的数据流量是均匀的,因此可以最大限度地限制攻击者利用流量的方向信息来对

节点进行攻击。Biswas 等提出了一种在不影响网络正常寿命前提下的抵御流量分析攻击者的隐私保护方案，即将一些普通节点作为汇聚节点使用，让攻击者认为其中的某个节点为真实的汇聚节点。此外，Chen 和 Lou 提出了双向树、动态双向树和曲折双向树三种多路径传输保护方案。

3）随机行走

Chen 和 Lou 提出了四种端到端的保护汇聚节点位置隐私的方案，其中随机行走就是利用随机性来达到保护汇聚节点位置隐私的目的。文献中提出利用定向行走来抵御攻击者对 Sink 或者源节点的攻击。Jian 等提出了 LPR 协议，他将邻居节点分为两组，并且将提出的方案分为两步：第一步，当数据包传到某节点时，节点以一定概率随机选择一个远邻居节点作为数据包的下一跳；第二步，当节点发送数据包给邻居节点（远邻居或者近邻居）时，会在同一时刻向远邻居中的一个随机节点发送一个假包。

4）其他

Nezhad A A 等提出了一种匿名拓扑发现的方法，这种方法可以隐藏汇聚节点的位置。与传统协议不同的是，此协议允许所有节点广播路由发现消息，这样就可以隐藏汇聚节点的位置。k-匿名也可以用来保护源节点或者汇聚节点的位置隐私，它的原理是用 k 个节点来迷惑攻击者，其中只有一个为真实的汇聚节点。

2. 典型的源节点位置隐私保护方案

保护源节点位置隐私的方案主要分为泛洪、随机行走、假包注入和假源策略四类。

1）泛洪

泛洪主要是为了混淆真数据流量和假数据流量，这样攻击者就很难通过流量分析追踪到数据源。泛洪主要分为基准泛洪、概率泛洪和幻影泛洪。

在基准泛洪中，数据源节点发送数据包给其所有邻居节点，同时邻居节点继续发送该数据包给邻居节点的所有邻居节点，直到目的节点接收到该数据包。但是对同一数据包，所有节点都只转发一次。此方案的优点是所有节点都参与了数据包的传输，因此攻击者不能通过跟踪一条路径追踪到源节点。但是，基准泛洪对位置隐私保护的有效性取决于源节点与汇聚节点之间路径的长度（以跳数计），如果路径跳数太少，攻击者很快就会追踪到源节点。同时，此种方案的网络能量消耗很大。基于此，概率泛洪在能量消耗方面对基准泛洪进行了优化。在概率泛洪中，随机选择一些节点对数据包进行转发，并且每个节点以一定的概率转发数据包。显然，这种方案既能减少能量消耗，也可以高效地保护源节点的位置隐私。然而，因为随机性的缘故，并不能保证汇聚节点能接收到所有源节点发送过来的数据包。幻影泛洪主要分为两个阶段：第一阶段为随机转发过程，源节点把数据包随机发送到一个假源节点；第二阶段为假源节点通过基准泛洪把数据包发送给汇聚节点。这样，即使追踪到了假源节点，也很难追踪到源节点。然而，所有泛洪策略对源节点的位置隐私保护程度都不是很好，且能量消耗也相对较高。

2）随机行走

随机行走策略的目的是通过一些随机的路径把数据包从源节点发送到汇聚节点。在幻影源节点单路径方案中，源节点首先按最短路径把数据包发送到一个随机节点，之后随机节点再沿最短路径将其单播发送到汇聚节点。然而，简单的随机行走并不能达到很好保护源

节点位置隐私的目的。为了改善幻影源节点单路径方案的性能,Yong 等提出了贪婪随机行走方案,即源节点和汇聚节点都随机行走。当两条行走路径汇合后,数据包沿着汇聚节点随机行走路径的相反方向发送给汇聚节点。这样的话,数据包传输的路径相当于已经被汇聚节点(或者基站)预先设定好了。Wang 等把源节点位置隐私保护问题简化为增加攻击者追踪到源节点的时间,包括最短追踪时间和平均追踪时间。加权随机行走允许每个节点自己独立选择下一跳节点,由于节点选择转发角度大的节点作为下一跳的概率大,所以大多数的数据包会有比较长的传输路径长度,以此来延长攻击者的追踪时间。

为了加长假源节点和真源节点之间的距离,Kamat 等提出了定向行走。在定向行走中,数据包头携带方向信息,接收到该数据包的节点按照方向信息进行数据包的传输。Yun 等提出了用一个随机中间节点来解决攻击者反向追踪源节点的问题。在随机中间节点方案中,源节点首先按照随机路径发送数据包到一个随机的中间节点,这个中间节点距离源节点至少有 h 跳(h 为提前设置好的)。后来,随机中间节点方案又被用来保护全局源节点位置隐私,文献中提出用一个传输真假包的混合环来迷惑全局攻击者。为了减小能耗,Yun 等提出了基于角度和象限的多中间节点路由方案。在这两种方案中,数据包从源节点传送到汇聚节点需要经过多个中间节点,而这些中间节点又是基于角度而随机选择的。

3) 假包注入

假包注入策略通过向网络中注入假包来抵御流量分析攻击者和数据包追踪攻击者的攻击。在短暂假源路由中,每个节点产生一个假包并且按照一定的概率泛洪传送给网络。此种方法只可以防止局部流量分析攻击者的攻击。为了防止全局流量攻击者的攻击,有学者提出了定期收集和源模拟。在定期收集方案中,每个节点以一定的频率定期独立地发送数据包,这些数据包中既有真包也有假包。而源模拟方案则把每个节点看成一个潜在的源节点。

为了抵御全局攻击者,也为了减小能耗,Yang 等提出了基于统计的源匿名。在 FitProbRate 中,用指数分布来控制假包流量的产生速率。Yang 等在文献中又提出了事件源不可观测的概念,目的是利用一定的丢弃假包原则来隐藏真实事件源,这样可以防止网络风暴。基于代理的过滤方案和基于树的过滤方案被提出的目的都是为了在假包传输到汇聚节点之前丢弃假包,以此减少真包的丢包率等。

4) 假源

假源策略就是选择一个或多个节点来模拟真实源节点的行为,以此来达到迷惑攻击者的目的。当有节点要发送真实数据包时,基站会建立一些假源。通常这些假源距离真实源节点距离很远,但是距离基站的距离与真实源节点距离基站的距离大致相同,且真实源节点和假源以同样的频率同时发送数据包。

5.6 入侵检测机制

无线传感器网络通常被部署在恶劣的环境下,甚至是敌方区域,一般情况下缺乏有效的物理保护,同时由于传感器节点的计算、存储、能量等性能都十分有限,因此无线传感器网络节点与网络很容易受到敌人的捕获和侵害。传感器网络入侵检测技术主要集中在监测节点的异常以及恶意节点的辨别上。鉴于传感器网络资源有限以及容易遭受入侵的特点,传统

的应用于常规网络中的入侵检测技术不适用于无线传感器网络。因此，设计一种适用于传感器网络的安全机制，以防止各种入侵，为无线传感器网络的运行营造一个较为安全的环境，成为了无线传感器网络领域能否继续走下去的关键。

5.6.1　入侵检测概述

现今，关于无线传感器网络安全方面的研究已经有很多了，通过密钥管理、身份认证等安全技术可以提高无线传感器网络的安全性，但是这些大多数都并未包含入侵检测的能力，无法及时有效地预防和发现无线传感器网络中的入侵问题。入侵检测是能够主动发现入侵行为并及时采取防卫措施的一种深度防护技术，这项技术可以通过对网络日志文件进行扫描、对网络流量进行监控、对终端设备的运行状态进行分析，进而发现可能存在的入侵行为，并对其采取相应的防护手段。在常规的网络环境中，入侵检测按数据获取方法可分为基于网络和基于主机两种方式，按检测技术可分为基于误用和基于异常两种方式。但是，无线传感器网络和传统网络在网络拓扑、节点结构、数据传输等诸多方面都有很多差别，而且由于传感器网络自身特点以及所面临的安全问题不同，所以很多传统入侵检测技术不适用于无线传感器网络。传感器网络自身特点包括如下几方面。

(1) 存储空间和计算能力是有限的。由于无线传感器网络中的节点受到能源、大小等因素的限制，导致很多常规的安全协议不能直接运用于传感器网络。

(2) 容易遭受多种途径的攻击。由于无线传感器网络与传统网络存在一些差异，所以仅根据传统的检测手段是很难及时地发现入侵行为的。另外，由于实际的无线传感器网络通常位于野外，很难做到全程监控，所以攻击者可以很方便地从一个网络拓扑中获取一些节点，或利用恶意节点破坏该拓扑结构，这样就使得传统的入侵检测技术难以发现恶意节点的存在，导致很多入侵行为的漏检。

(3) 带宽和通信能量的限制。当前的无线传感器网络都采用低速、低能耗的通信技术。因为无线传感器网络没有持续的能源供给，其整个工作过程期间也不会得到实时监控，所以节能成为了传感器网络存活必须考虑的问题。所以一些复杂的检测算法的功耗开销是传感器网络的低功耗无法承载的。

因此，由于无线传感器网络自身的特点所限，一些传统的入侵检测技术很难应用于其中。然而，既然要发展无线传感器网络，就必须让它拥有与传统网络同样的安全条件，以保证其正常的通信安全。所以设计出适应于无线传感器网络的入侵检测机制是确保无线传感器网络领域继续研究的关键一环。

5.6.2　入侵检测体系结构

传感器网络入侵检测有三个组成部分，分别为入侵检测、入侵跟踪和入侵响应。这三个部分顺序执行，首先执行入侵检测；要是入侵存在，将执行入侵跟踪来定位入侵；然后执行入侵响应来防御攻击者。此入侵检测框架如图 5.11 所示。

现今的体系结构中根据检测节点间的关系，大致可分为以下三种类型。

1. 分治而立的检测体系

为了降低网络中能源的损耗，入侵检测程序只会安装在某些关键的节点中。每个装有

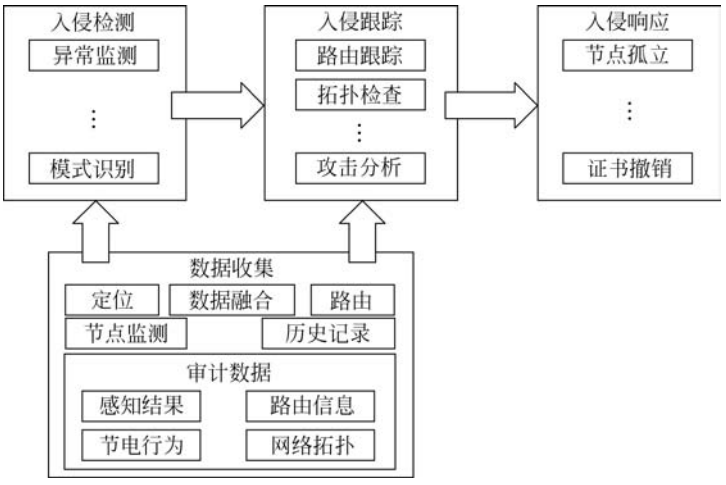

图 5.11 入侵检测框架

检测程序的节点的优先级和作用相同,既负责采集网络中的数据,又要对网络环境的检测结果进行分析。之后它们会将自己的分析结果传给基站,不会与其他检测节点进行数据交互。

这种方法的优点是设计思路简洁,容易部署和实现。缺点是各个检测节点之间没有数据交互,分别独立进行检测,不能协同工作,这会导致网络环境中产生大量的冗余信息,浪费时间,同时也浪费了传感器网络中宝贵的能源,而且独立的检测对于整个网络环境的入侵行为监控是不利的。

2. 对等合作的检测体系

无线传感器网络对采用广播的数据传输方式,每个节点可以方便地检测自身邻居节点的数据流向。对等合作的检测体系是基于分治而立的检测体系之上的,首先还是各个检测节点独立检测。当遇到某些特殊的入侵行为时,各检测节点会相互交换信息来共同处理检测结果。

这种检测体系对于上一种方案在性能上有一定的提升,但是这种体系要求网络环境中的大部分节点安装入侵检测系统(intrusion detection system,IDS),这就会导致普通入侵行为出现时资源的重复性浪费。另外,检测节点间的数据交互需要广播大量的数据包,这必然会影响正常情况下的网络带宽。

3. 分层次的检测体系

为了避免上述两种方案造成的资源浪费以及带宽占用,研究人员提出了分层次的检测体系。它的基本思想是把无线传感器网络中的全部节点按照其各自的功能不同划分为不同的层次:底层节点进行数据采集与检测任务,顶层节点进行数据融合及综合处理等工作。

这种检测体系能够很好地提高检测的准确性,大大减少了资源开销,同时网络的整体运行性能也受到了不同程度的提升。此外,在进行数据融合的过程中降低了整个网络中的数据冗余性,但这也是以降低网络的鲁棒性为代价的。

5.7　节点俘获攻击

一个典型的传感器节点由低成本的硬件构成，在电源、通信和计算能力等方面受到限制。传统的安全机制无法应用于传感器节点，从而使得无线传感网络面临许多方面的安全挑战。节点俘获攻击被认为是最严重的安全威胁之一，它容易发动，又难以检测和防范，是复制攻击、sybil、虫洞、黑洞等攻击的基础。一般情况下，无线传感器网络中的攻击呈多种攻击相互结合的方式。

作为一种新式的攻击方法，在节点俘获攻击中，攻击行动有三个阶段。

(1) 物理俘获传感器节点并获取记录在内存或者缓存中的密钥，然后运用已经俘获的密钥窃听链路中传输的内容。

(2) 将俘获节点重新部署在网络中，破译收其他节点传输过来的信息。

(3) 攻击者发动内部攻击。

所以防范节点俘获攻击最有效的方法是在防范攻击者利用俘获节点窃听网络通信的同时，防止俘获节点重新部署到网络中。

研究无线传感器网络的攻击算法有利于为研究网络安全提供攻击模型，因此本节着重介绍如何设计和提高节点俘获攻击的效率，为后续网络安全的研究提供模型基础。

5.7.1　模型定义

1. 网络模型

1) 静态网络

为了方便研究，我们将静态网络用一个离散的有向图模型 $G=(N,L)$ 表示，其中 N 代表各个节点的集合，L 代表有向图中的链路的集合，即 (i,j) 表示一条从节点 i 到 j 的可靠安全的链路，i 可以将数据发送给 j 而无须将数据中继给其他节点。

如果一对节点 i,j 共享密钥 $K_{i,j}=K_i \cap K_j$（K_i 表示分配给节点 i 的密钥集合），且两者的通信范围重合，则可以建立一条可靠链路 (i,j)。

2) 动态网络

因为节点位置会随着时间的变化而变化，所以我们将它放在一个封闭的网络中，即节点始终在一个封闭的区域内运动。

2. 网络部署模型

1) 随机分布

随机分布是指系统中的节点随机分布在一个矩形网络区域内。根据节点间的距离，每个节点建立路由器表记录邻居节点。

2) 标准分布

标准分布是指在网络中，节点会以 $M \times N$ 的网络模型进行分布，节点处于交汇处。

3) 簇结构

在基于簇结构的网络中，附近节点被划分在同一个簇中，每个簇中选举一个簇头节点，

管理簇结构内的簇成员与簇头节点之间的通信。

3. 密钥分配模型

为改善无线传感网络节点存储量小、计算能力低下的特点,模型采用对称加密的方法保证传输过程中的信息安全。定义 K 为所有密钥的集合,密钥预分配协议为每个节点 i 分配一个密钥子集 K_i,满足 $K_i \subset K_j$。两个节点 i 与 j 之间的共享密钥计算方法为 $K_{i,j}=K_i \cap K_j$。例如,节点 i 与节点 j 相互在对方的传输半径 r 内,$K_i=\{K_1,K_2,K_3\}$,$K_j=\{K_1,K_3,K_4\}$,则 $K_{i,j}=\{K_1,K_2,K_3\} \cap \{K_1,K_3,K_4\}=\{K_1,K_3\}$。

当节点 i 与 j 通信的时候,$K_{i,j}$ 中的所有密钥将用于加密数据。因此一个链路(i,j)的安全性与链路两端节点共享密钥合集的大小 $K_{i,j}$ 有直接关系,$K_{i,j}$ 越大,安全性越高,反之安全性越低。

4. 路由模型

在无线传感器网络中,源节点周期性地将数据发送给 Sink 节点。定义 S 和 D 分别为源节点和 Sink 节点的集合,$S \subset N$,$D \subset N$。运用路由协议,建立从源节点到 Sink 节点的路径(path) 和路由(route)。路径和路由的区别和联系是:路径由一系列首尾相连的数据链路组成;路由是一组具有相同源节点和 Sink 节点的路径的集合,由一条或多条路径组成。

在静态网络中,我们研究三种不同方式的路由协议:单路径路由协议、多独立路径路由协议和多依赖路径路由协议。单路径路由协议是指一条路由只包含一条单独固定的路径,例如 GBR(gradient based routing)路由协议。多独立路径路由是指消息在传输的过程中沿着不同的路径从一个源节点发送至同一个 Sink 节点,例如 AODV 路由协议。多依赖路径路由协议是指在传输的过程中,采用网络编码的方法将数据分成多个相互依赖的部分,再沿着不同的路径从源节点传输到 Sink 节点。多依赖路径路由和多独立路径路由协议统称为多路径路由协议。在单路径路由协议中,一条路径即为一条路由;而在多路径路由协议中,一条路由由多条路径组成。另外,从端到端安全角度而言,如果在一条路径或路由中传输的数据被源节点和 Sink 节点之间的共享密钥加密,那么这样的路径或路由就称为端到端安全路径或路由。

在动态网络中,我们研究 AODV 路由协议,着重研究在动态无线传感器网络中,攻击者如何通过传播恶意软件的方法破坏网络的安全性与保密性。

5. 攻击模型

假设攻击者具有足够的资源和能力监听网络中传输的信息、俘获节点、从节点的缓存中获取节点的密钥信息,且攻击者还掌握着节点密钥分配和路由信息的背景知识,则在攻击中,攻击者可以任意选择除 Sink 节点之外的节点实施节点俘获攻击。一旦节点被俘获,攻击者便会从俘获节点的缓存中获取该节点分配的密钥集合,随后利用密钥解密网络中传输的数据。当网络中所有的信息都被破译时,节点俘获攻击便结束了。在节点俘获攻击中,攻击者俘获节点的方法有物理攻击法和恶意软件传播法两种。

在物理攻击法中,攻击者物理地从网络中选取节点并俘获,直接从节点缓存中获得节点的密钥分配信息。

在恶意软件传播法中，攻击者运用已经俘获的节点传播恶意软件。一旦普通节点与已俘获节点之间存在共享密钥，攻击者便可以运用俘获节点将恶意软件传播给该节点，通过恶意软件获得该节点的路由表信息和密钥分配信息，进而俘获其他节点。宏观上来说，恶意软件传播法是一种传播性的攻击方法。

从攻击形式来说，节点俘获攻击主要分为集中式攻击法和分布式攻击法两种。

1）集中式攻击法

集中式攻击法始于攻击者俘获网络中的一个节点或者一小部分节点，随后在已俘获节点的邻居节点之间散播恶意软件，运用恶意软件来控制普通节点。

2）分布式攻击法

在分布式攻击法中，攻击者可以任意选择网络中的节点发动攻击、俘获节点、攫取密钥、解密网络中传播的信息。

6. 节点移动模型

假设所有的节点都在一个封闭的区域内运动，节点的初始化位置随机。每一轮节点都会选择一个目的地，并随即前往该目的地。节点到达后，会选择下一个目的地，整个过程不断重复进行。节点的移动服从 Random Way Point（RWP，随机路径点）和 Continuous Markov Chain（CMC，连续马尔可夫链）两种模型下网络的脆弱性。

RWP 模型是所有移动模型的基础模型，其节点的速度、加速度随时间变化而变化。由于系统具有简便性和实用性，通常被当作移动模型对比的基准。

CMC 模型将整个系统分为 M 个区域，每个节点存储一个矩阵，矩阵表示从当前位置转换到另一个位置的概率。每当节点到达目的地后，便会使用该矩阵动态计算出下一个目的地。

7. 定义受到攻击时的模型

定义 C_n 为攻击者俘获的节点集合，C_k 是对应的已俘获密钥集合，令 $C_k=\bigcup_{\forall i\in C_n} K_i$，其中 K_i 是节点 i 分配的密钥。例如，一个攻击者已经俘获 i 和 j 两个节点，$C_n=\{i,j\}$，$K_i=\{K_1,K_2,K_3\}$，$K_j=\{K_1,K_3,K_5\}$，则 $C_k=K_i\cup K_j=\{K_1,K_2,K_3,K_4\}$。当一个消息在一条链路、路径或路由中传输的时候，如果其中的某一条链路被 C_k 的子集加密，那么这条消息就会被攻击者破解。

定义 5.1　当且仅当 $K_{i,j}\subseteq C_k$，一条链路 $(i,j)\in L$ 被俘获。

定义 5.2　当且仅当路径中存在一条或多条被俘获的链路，一条路径 $p\in P$ 被俘获。

定义 5.3　当且仅当路由中的所有路径都被俘获，一条路由 $r\in R$ 被俘获。

定义 5.4　当且仅当有一条链路被俘获而且 $K^E(P_i)\subseteq C_k$，一个端到端安全路径 P_i 被俘获，其中 $K^E(P_i)$ 是路径 P_i 的源节点和 Sink 节点之间的共享密钥。

定义 5.5　当且仅当路由中所有的路径都被俘获且 $K^E(r_i)\subseteq C_k$，一个端到端安全的路由 r_i 被俘获，其中 $K^E(r_i)$ 是路由 r_i 源节点和 Sink 节点之间的共享密钥。

5.7.2 基于矩阵的攻击方法

首先攻击者将网络、密钥、能耗等信息输入到算法中,并建立矩阵 $\mathrm{PK}=[\mathrm{pk}_{i,j}]_{|P|\times|K|}$(路径-密钥矩阵,表示俘获单个密钥能否导致一条路径被俘获,计算方法如式(5-1)所示)和 $\mathrm{KN}=[\mathrm{kn}_{i,j}]_{|K|\times|N|}$(密钥-节点关系矩阵,说明节点与路径之间的俘获关系,计算方法如式(5-2)所示),得到密钥和节点之间的关系。在下列计算公式中,$|P|$是路径的数目,$|K|$为密钥池的大小,k_i 表示密钥池中的第 i 个密钥,p_j 为第 j 条路径。

$$\mathrm{pk}_{i,j}=\begin{cases}1, & \text{俘获 } k_i \text{ 能俘获 } p_j\\ 0, & \text{其他}\end{cases} \tag{5-1}$$

$$\mathrm{kn}_{i,j}=\begin{cases}1, & k_i\in K_j\\ 0, & \text{其他}\end{cases} \tag{5-2}$$

随后计算矩阵 $\mathrm{PN}=[\mathrm{pn}_{i,j}]_{|P|\times|N|}$(路径-节点矩阵,用于分析攻击一个节点会导致多少路径被俘获,计算方法如式(5-3)所示),得到节点和路径之间的直接俘获关系。在矩阵 PN 中,如果元素 $\mathrm{pn}_{i,j}\geqslant 1$,表示俘获节点 n_j 会导致路径 p_i 被俘,我们称这种攻击关系为直接俘获。但是在节点俘获攻击中,仅仅考虑直接俘获是不够的。当一条链路被多于一个密钥加密时,如果仅仅获得其中的一个或者部分密钥,虽然无法使得路径被俘获但是仍然能够降低该路径的安全性。我们定义这种俘获为间接俘获。为了描述间接俘获,我们建立矩阵 $\mathrm{PLN}=[\mathrm{pln}_{i,j}]_{|P|\times|N|}$ 表示当攻击者攻击 n_j 时,攻击者会获得的密钥在路径 p_i 中的比值。

$$\mathrm{PN}=\mathrm{PK}\times\mathrm{KN} \tag{5-3}$$

在计算 PLN 矩阵时,对于每个节点来说,先要判断是否能够间接俘获每一条路径,如果能则记录这个节点对于路径中的每一条链路之间的密钥共享关系,结果记录在 PLN 的元素中,其中 $\mathrm{pln}_{i,j}=\dfrac{1}{e}\sum_{t=1}^{e}\dfrac{|K_j\cap K_{t,t+1}|}{|K_{t,t+1}|}$,$e$ 表示路径中链路的数量,P 是路径的集合,N 为节点的集合。$K_{t,t+1}$ 表示在路径中第 t 个链路拥有的共享密钥,即为第 t 和 $t+1$ 节点之间的共享密钥。

获得了矩阵 PN 和 PLN 之后,我们将两个矩阵的元素进行合并,用一个新的矩阵 $\boldsymbol{M}=[m_{i,j}]_{|P|\times|N|}$ 表示节点与路径之间的俘获关系。$\boldsymbol{M}$ 的计算方法如式(5-4)所示,其中 α 是一个(0,1)之间的参数,表示直接俘获和间接俘获的重要性关系。

$$\boldsymbol{M}=\alpha\times\mathrm{PN}+(1-\alpha)\times\mathrm{PLN} \tag{5-4}$$

在无线传感器网络的节点俘获研究中,另一个研究重点是能耗问题。攻击者需要以最低的能耗对网络造成最大的破坏,因此我们将攻击节点的能耗与矩阵 $\boldsymbol{M}$ 相结合,得出矩阵 MC,计算方法如式(5-5)所示。

$$\mathrm{mc}_{i,j}=\frac{m_{i,j}}{w_j} \tag{5-5}$$

得到上述矩阵以后,攻击的过程就开始了。攻击者从矩阵 MC 中找到能够满足 $t=\underset{j\in N}{\operatorname{argmin}}\sum_{i=i}^{P}\mathrm{mc}_{i,j}$ 的节点 n_t,并攻击节点 n_t。这是因为攻击这个节点能够造成最大数量的路

径被俘获，将攻击破坏性最大化，并且能耗最低。

一轮攻击结束后，攻击者运用式(5-5)调整矩阵 MC 中的元素。一旦一个节点被俘，攻击这个节点的能耗将变为$+\infty$，这种方法能够保证一个节点最多只能被攻击一次。

当网络被俘获之后，攻击过程结束。这种矩阵的攻击方法中，每轮攻击者都能够找到网络中造成破坏性最大且能耗最低的节点进行攻击。这种矩阵的攻击方法能够为网络的脆弱性评估提供一个良好方法，即选出网络中最脆弱的节点，从而加强这种节点的安全措施，从整体上提高网络的抗攻击性。

5.7.3　基于攻击图的攻击方法

为了直观地描述无线传感器网络中节点俘获攻击的过程，可将该过程用攻击图表示。与一般图类似，攻击图也是由点和线组成的，其中点称为路径点，路径点和路径之间一一对应。如果一条路径被俘获，那么对应的路径点也视作被俘获。我们用图的方法表示节点与路径点之间的关系，称之为全图。一个全图可表示为 $G^f=(N,\mathrm{PV},E^d,E^i)$，其中 N 表示网络中节点的集合，PV 是网络中路径点的集合，E^d 为直接攻击线集合(指攻击一个节点后使一条路径被直接俘获的路径点)，E^i 为间接攻击线集合(攻击节点时对路径造成间接俘获)。直接俘获和间接俘获的定义如下。

定义 5.6　节点 $i\in N$ 与路径 $\mathrm{pv}_t\in\mathrm{PV}$ 之间存在一条直接攻击线，当且仅当攻击节点 i 会导致 pv_t 对应的路径被俘获，可表示为 $i\rightarrow\mathrm{pv}_t$，称之为节点 i 和路径 pv_t 具有直接俘获关系。

定义 5.7　节点 $i\in N$ 与路径点 $\mathrm{pv}_t\in\mathrm{PV}$ 之间有一条间接攻击线，当且仅当攻击节点 i 会导致 pv_t 满足以下两个条件。

(1) pv_t 对应的路径没有被俘获；

(2) 节点 i 与 pv_t 中的一条或者多条链路具有相同的共享密钥。pv_t 中存在一条链路 (j,l)，满足 $1\leqslant|K_{j,l}\cap C'_k|<|K_{j,l}|$，我们称节点 i 与 pv_t 之间存在间接俘获关系。

下面通过一个全图实例来深刻地理解链路被俘获和直接俘获、间接俘获之间的关系。在图中，实线箭头表示直接攻击线，虚线箭头表示间接攻击线。在图 5.12 中，路径 p 由 3 条链路组成，即 $p=\{(s,i),(i,j),(j,d)\}$，图中介绍了节点的密钥分配情况和链路的共享密钥。在图 5.13 中，路径 p 用一个路径点 pv 表示。从图中可以看出节点 m 具有密钥 k_1，因此攻击节点 m 会导致链路(i,j)被俘获。因此在图 5.13 中，节点 m 与 pv 之间有一条直接攻击线，从 m 指向 pv。节点 n 拥有密钥 k_3，攻击 n 只能导致 pv 中的链路(s,i)被部分俘获，因此攻击节点 n 只能导致 pv 被间接俘获，故在全图中有一条间接攻击线从 n 指向 pv。

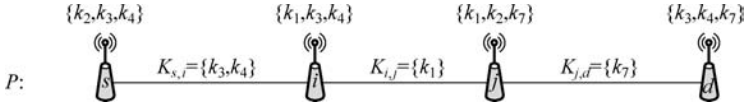

图 5.12　链路直接俘获

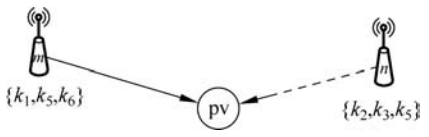

图 5.13 链路间接俘获

全图建立完成以后,可以采用一种基于全图的无线传感器网络节点俘获算法(全图攻击算法)对目标网络进行攻击。在整个攻击过程中,首先进行网络的初始化,每个节点被分配一定数量的密钥,节点与周围节点建立链路;随后采用不同的路由协议(例如单路径路由协议、多独立路径路由协议、多依赖路径路由协议)建立从源节点到 Sink 节点的路径;网络初始化结束后,攻击者开始建立网络对应的全图,所有的路径都被抽象成路径点;之后攻击者开始计算每个节点和每个路径点之间的直接俘获关系和间接俘获关系,并在全图中将节点与路径点用对应的箭头连接起来;全图建立好之后,攻击者便开始对网络发动节点俘获攻击。在每一轮攻击中,攻击者会为每个节点计算直接攻击值和间接攻击值,然后对比每两个节点之间的破坏等级,并从中选取破坏等级最高的节点进行攻击。这种方法可以降低需要俘获的节点数量,提高攻击效率。

5.7.4 动态网络攻击方法

1. 网络骨架

在动态网络中,由于节点自始至终处于运动状态,因此难以对节点的运动模型、运动轨迹建模。故建立虚拟网络骨架,将与其他节点具有较高相遇概率的节点作为网络的骨架,从动态网络的拓扑结构出发建立网络的联通支配集。攻击的目标节点将从网络的虚拟骨架中选择,用于破坏网络的联通支配集。

2. 连通支配集

一个网络 $G=(N,L)$ 的支配集(dominating sets,DS)是一个节点的子集,所有不在集合 DS 中的节点至少与 DS 中的一个点存在链路相连。

支配集的定义指出,所有的链路至少存在一端在 DS 中。如果攻击者能够俘获 DS 中的所有节点,就可以控制整个网络。因此从攻击者的角度而言,在攻击时只要俘获整个 DS 即可。

当攻击者向网络发动攻击时,它会不断地向普通节点注入恶意软件。但是通常情况下,支配集中的节点会相互远离。在这种情况下,如果攻击者想要通过一个 DS 中的节点传播恶意软件给另一个 DS 中的节点,需要等待一段时间,直到节点相遇。

$G=(N,L)$ 中的每一个节点都属于 DS 或者与其中一个 CDS(connected dominating set,连通支配集)中的节点相连。

连通支配集弥补了支配集的不足,攻击者在攻击时只需要俘获 CDS 中的节点即可实现对整个网络的俘获。由于在建立骨架时需要考虑到预测节点的未来相遇概率,所以定义节点的相遇概率矩阵 $P_{\mathrm{FIP}}=[p_{i,j}]_{|N|\times|N|}$,$p_{i,j}=\dfrac{T_{i,j}}{T_i}$。$P_{\mathrm{FIP}}$ 与先前相遇时间有关,即将先前相遇时间作为先验知识,推测出未来相遇的概率,其中 $T_{i,j}$ 表示节点 i 与节点 j 在之前相遇的时间之和,T_i 表示节点 i 在系统中逗留的时间。

在建立 DS 时,我们从 FIP 中找到最大概率的节点,这种节点在未来的移动中更容易与

其他节点相遇。DS 的建立完成以后，攻击者在 DS 的邻居节点中寻找最大 FIP 的节点，将这类节点加入到 DS 中，建立 CDS。

3. 通用攻击算法

由于 CDS 的建立与网络拓扑无关，仅仅与节点的移动模型有关，所以动态网络的攻击算法同样适用于静态网络，因此基于 CDS 的攻击算法可以看作无线传感器网络中的一种通用攻击算法。

首先进行网络的初始化，在节点与邻居节点之间建立链路；随后计算 FIP 矩阵，建立网络 CDS；在攻击过程中，每一轮，攻击者从 CDS 中选择具有邻居节点最多的节点，原因是攻击这种节点可以导致更多的链路被俘获；这种攻击过程不断迭代下去，直到网络被俘获，最后攻击者俘获的节点集合作为算法输出被返回。

5.8　本章小结

本章讨论了无线信息安全中的无线传感器网络安全问题，分别对无线传感器网络安全路由协议、密钥管理及其认证机制、位置隐私保护和入侵检测进行了介绍，首先介绍了安全路由，并分析了现在的路由协议容易遭受的安全攻击；接下来分析了现今的一些密钥管理分类方法，并着重介绍了组密钥管理以及设计过程中需要考虑的问题；随后介绍了无线传感器网络中的认证机制，主要包含实体认证机制和信息认证机制这两方面；最后介绍了无线传感器网络中的位置隐私保护方案、入侵检测技术和节点俘获攻击技术。

思考题

1. 无线传感器网络常见的安全威胁有哪些？
2. 典型的路由协议有哪些？
3. 密钥管理的分类方法有哪些？其各自的分类原则是什么？
4. 无线传感器为什么需要保护节点的位置隐私？
5. 节点俘获攻击的目标是什么？

参 考 文 献

[1]　林驰. 安全关键无线传感器网络高效可信协议研究[D]. 大连：大连理工大学，2013.
[2]　康林. 无线传感器网络位置隐私保护方案研究[D]. 大连：大连理工大学，2013.
[3]　魏松铎. 无线传感器网络的认证机制研究[D]. 南京：南京邮电大学，2009.
[4]　孔贝贝. 无线传感器网络的密钥管理与安全路由技术研究[D]. 成都：西南交通大学，2010.
[5]　张聚伟. 无线传感器网络安全体系研究[D]. 天津：天津大学，2008.