# 第5章

# 物联网感知层安全

## 本章要点

物联网感知层安全概述
RFID 安全
无线传感器网络安全
物联网终端安全

## 导入案例

**RFID 安全问题**

2003 年，一位黑客在网站上公布了他攻入一家以无源 RFID 系统作为门禁的公司的方案。该黑客窃取数据之后，破解了 RFID 的安全机制与编码规则，仿制出可用于出入公司的门禁卡。

2005 年，一所大学的研究小组经过 2 年的研究，破解了一种 RFID 的安全机制与编码规则，写出它的模拟软件，并仿真了标签与读写器的工作过程。另外有一份报告称：一名学生已经破解了超过 1.5 亿个安装有 RFID 的汽车钥匙和超过 600 万个购买汽油钥匙扣的密码。解密计算过程只花了 15 分钟。

2006 年意大利举行的学术会议上，有研究者提出病毒可能感染 RFID 芯片。通过伪造沃尔玛、家乐福超级市场里的 RFID 电子芯片，将正常的电子标签替换成恶意标签，即可进入它们的数据库及 IT 系统中发动攻击。

2007 年 RSA 安全大会上，一家名为 IOActive 的公司展示了一款 RFID 克隆器，这款设备可以通过复制信用卡来窃取密码。

2011 年 3 月，业内某安全专家破解了一张英国银行发行的、利用 RFID 来存储个人信息的新型生物科技护照。

2011 年 9 月，黑客通过破解北京公交一卡通，给其非法充值，获取非法利益 2200 元。从此，敲响了整个 RFID 行业的警钟。

上述案例表明，RFID 作为物联网感知的一项关键技术，其应用越来越广泛，其安全问

题逐步成为了社会讨论的热点。讨论的焦点主要集中在 RFID 技术是否存在安全问题？这些安全问题是否需要解决？又该如何解决？

# 5.1　物联网感知层安全概述

## 5.1.1　物联网感知层简介

由物联网体系架构可知，位于物联网最底层的感知层可视为物联网的神经末梢，负责采集物理世界的状态信息即感知数据。感知数据是物联网应用的主要数据来源，发挥着关键作用。诸多物联网安全事件表明由于感知节点数量庞大、终端类型结构多样、数据多源异构，直接面向世间万“物”，物联网感知设备及感知层网络是物联网应用中的薄弱点，经常被攻击者利用进而发动攻击，因此有必要采取相应措施对感知层设备及感知层网络进行保护。感知层网络及感知层设备的安全与否决定了物联网应用能否正常运行。感知层安全防御技术对物联网的安全应用有着重要意义。

物联网感知层的任务是感知外界信息，完成物理世界的信息采集、捕获和识别。感知层的主要设备包括：RFID 标签及其读写器、各类传感器（如温度、湿度、红外、超声、速度等传感器）、图像捕捉装置（摄像头）、全球定位系统装置、激光扫描仪等。这些设备收集的信息通常具有明确的应用目的，例如，公路摄像头捕捉的图像信息直接用于交通监控；使用手机摄像头可以和朋友聊天以及与他人在网络上面对面交流；使用导航仪可以轻松了解当前位置以及前往目的地的路线；使用 RFID 技术的汽车无匙系统，可以自由开关车门。各种感知器在给人们的生活带来便利的同时，也存在各种安全和隐私问题。例如，使用摄像头进行视频对话或监控，在给人们生活提供方便的同时，也会被具有恶意企图的人利用，从而监控个人的生活，窃取个人的隐私。近年来，黑客通过控制网络摄像头窃取并泄露用户隐私的事件偶有发生。因此本章围绕物联网感知层的安全威胁及防护技术，重点介绍感知层中 RFID 安全、无线传感器网络（Wireless Sensor Networks，WSN）安全和物联网终端安全。

## 5.1.2　物联网感知层的安全需求

### 1. 保密性

避免信息在传递过程中被不法分子截取不仅是保障整个感知层信息安全的基础，更是前提。物联网中各传感节点之间发送的数据信息应该只能由该网络中的簇节点或者其他拥有存储与转发能力的节点所接收与处理，任何不属于此网络的攻击节点都应该无法破获此信息。所以，必须有一套完整的信息安全机制来保证网络中信息的安全，其中最常用且有效的策略莫过于一个良好的密钥管理机制与加解密算法。这可借鉴互联网安全中的相关措施，最大限度地降低可能遇到的部分安全问题，保护信息的保密性，增强整个系统的健壮性。

### 2. 完整性

感知层数据在传输过程中，会面临比互联网信息传输过程中更多样化的攻击类型，数据的增加与减少都会影响信息的完整性，从而进一步威胁整个物联网的安全。为了应对这类问题，设计人员常常通过在数据帧中增加校验的方式来缓解。目前有多种校验数据的方式，最常用的是在传输的数据帧中为数据添加摘要或者是数字签名。这种方式可判断数据在传

输过程中是否发生变化，当以此来甄别数据是否合法时，只需判断它是否能够通过摘要的校验即可。

**3. 可用性**

可用性确保授权用户和服务在请求数据和设备时，能够迅速得到响应。在很多物联网应用中，如军事物联网、车联网、医用物联网等，用户通常以实时方式请求服务，如果无法及时传送所请求的数据，则无法进一步安排和提供服务，甚至威胁生命安全和社会基本次序。因此，可用性也是物联网的一个重要安全要求。可用性所面临的最严重的威胁之一是拒绝服务攻击，应使用可用性保障技术（如安全高效的路由协议等）以确保物联网的可用性。

**4. 新鲜性**

新鲜性是指感知层间流动的数据信息都必须是感知节点在最新时间段内生成的。换句话说，节点间每次通信时的信息内容都要发生一定变化（即使传输的基本信息不变，标识信息产生的时间戳也是变化的），以防止攻击者使用旧数据重复发送（如重放攻击）导致数据新鲜性的问题。

### 5.1.3 物联网感知层的安全威胁

根据物联网感知层的功能和应用特征，可以将物联网感知层的安全威胁概括如下。

**1. 物理捕获**

感知设备存在于户外，且被分散安装，因此容易遭到物理攻击，其信息易被篡改，进而导致安全性丢失。RFID 标签、二维码等的嵌入，使接入物联网的用户不受控制地被被动扫描、追踪和定位，这极大可能会造成用户的隐私信息泄露。RFID 技术是一种非接触式自动识别技术，它通过无线射频信号自动识别目标对象并获取相关数据，识别工作无须人工干预。由于 RFID 标签设计和应用的目标是降低成本和提高效率，大多采用“系统开放”的设计思想，安全措施不强，因此恶意用户（授权或未授权的）可以通过合法的读写器读取 RFID 标签的数据，进而导致 RFID 标签的数据在被获取和传输的过程中面临严重的安全威胁。另外，RFID 标签的可重写性使标签中数据的安全性、有效性和完整性也可能得不到保证。

目前试图通过网络安全技术防止感知层设备被物理捕获俘获是不可能的，但可以在设备被俘获后，使攻击者从设备获取有用信息的难度增大。这方面的技术包括芯片封装技术、芯片管理技术、抗侧信道攻击技术等。

**2. 拒绝服务攻击**

物联网感知层节点为节省自身能量或防止被木马控制而拒绝提供转发数据包的服务，造成网络性能大幅下降。感知层接入外在网络（如互联网等），难免会受到外在网络的攻击。目前，最主要的攻击除非法访问外，就是拒绝服务攻击。感知节点由于资源受限，计算和通信能力较低，因此对抗拒绝服务攻击的能力比较弱，可能会造成感知层网络瘫痪。

目前，资源受限的物联网终端设备基本没有什么能力能够应对拒绝服务攻击。但是，休眠却是一种最有效的方法。物联网终端设备可设置合理的休眠机制，定期醒过来检查侦听有没有需要执行的任务。如果有任务，则执行完任务然后再休眠，如果没有任务，则在醒过来一段时间（相对休眠时间，通常为很短的时间）后，再进入下一轮休眠。在拒绝服务攻击下，物联网终端设备侦听不到需要执行的任务，其功耗仅仅在侦听阶段消耗，受影响较小。

因此，休眠虽然是芯片技术的一种管理策略，不是传统意义的网络安全技术，但在非实时物联网终端的抗拒绝服务攻击方面非常有效。例如，一个物联网抄表终端，平时需要抄报、传输数据的机会很少，因此可以每分钟休眠 59s，醒过来侦听 1s。如果在这 1s 的清醒期内没有任务，则继续休眠 59s，然后再醒 1s。当后台服务器需要发送抄表指令时，这种指令的传输需要每秒钟发送不少于 2 次，保证抄表终端在侦听期间能接收到指令，而且需要持续至少 1min，保证在终端醒过来时仍然在发送指令。这样，抄表指令能正常执行，而拒绝服务攻击在 1min 内也只能影响抄表终端 1s 的资源浪费。不过该方法仅适合非实时物联网，对实时性要求较高的物联网应用，如军事物联网、工业物联网、医用物联网、车联网并不适用。

**3. 木马病毒**

由于安全防护措施的成本、使用便利性等因素的存在，某些感知节点可能不会采取安全防护措施或者采取很简单的信息安全防护措施，这可能会导致假冒和非授权服务访问问题的产生。例如，当物联网感知节点的操作系统或者应用软件过时，系统漏洞无法及时修复时，物体标识、识别、认证和控制就易出现问题。

应对木马病毒攻击，对于类似手机、iPad 和各种智能终端等性能较强、资源较多的超级感知层节点，可以参考电脑应对木马病毒攻击的方式，如安装杀毒软件，定期扫描系统、及时更新病毒库、更新系统补丁，查杀病毒等。对于类似二维码、RFID 等资源较贫瘠的感知层节点，它们难以本地识别并处理木马和病毒，只有依靠物联网中性能较强的中继节点进行识别和杀毒。

**4. 数据泄露**

物联网通过大量感知设备收集的数据种类繁多、内容丰富。且为方便部署，经常使用无线通信。由于无线通信的开放特性，如果保护不当，将存在隐私泄露，数据被冒用、篡改、盗取的问题。如果对感知节点所感知的信息不采取安全防护措施或者安全防护强度不够，则这些信息可能会被第三方非法获取。这种数据泄露在某些时候可能会造成很大的危害。

应对数据泄露，即对数据内容的机密性保护，相应的技术方法是数据加密技术。将传输中的数据进行加密，即使攻击者实施了窃听，数据遭受泄露，所获得的密文对掌握数据内容也没有帮助，这实际上保护了数据内容的机密性。例如，要传输的原始数据为 data，而实际传输的数据为对应的密文 $c=E_k(\text{data})$。当攻击者通过信道窃听获得密文 $c$ 后，如果没有解密密钥，则不能恢复原始数据 data，仅获得密文 $c$ 并不能得到数据 data 的内容。这样，通过简单的数据加密技术就可以实现对数据内容的机密性保护。

**5. 节点妥协攻击**

攻击者通过节点妥协攻击能够捕获或者控制物联网中的节点或设备，节点捕获攻击通过替换实体节点，或者篡改节点或设备的硬件信息实现。一旦节点被成功妥协，节点内保存的重要信息（组内通信密钥、频段密钥、匹配密钥等）都会泄露给攻击者。攻击者进一步将妥协节点相关的重要信息复制到恶意节点，并将恶意节点伪装成合法节点连接到物联网。因此，这种攻击也可称为节点复制攻击。节点妥协攻击可能对网络产生极其严重的影响。

应对节点妥协攻击的原则是只要攻击者不能获得终端内的秘密信息即可。同样可以使用对芯片的安全防护技术达到这一安全目标。

**6. 恶意代码注入攻击**

恶意代码注入攻击是一种物理攻击，是指攻击者通过向物联网中的感知节点或设备的内存中注入恶意代码进而达到控制节点和设备的目的。由于物联网设备联网的便捷性，因此允许设备可以提供不安全的应用程序编程接口（Application Programming Interface，API），让应用程序开发者和其他用户可以用 API 来连接和交流；同时，很容易受到未授权实体的恶意代码注入攻击。所以，不安全的软件 API 和硬件接口是物联网设备中这种攻击的主要来源。注入的恶意代码不仅能执行特殊的功能，还能赋予攻击者进入物联网系统的权限，甚至控制整个物联网系统。

为减少这类攻击，在代码初始运行之时，如果认证机制足够，那么就可以建立一个基于信任的安全引导链。这样，需要用定制硬件来替代内建的处理器，从而提高安全性引导支持。

**7. 数据伪造攻击**

攻击者伪装成物联网系统中的一个合法节点，对要攻击的目标节点发送伪造的数据。要攻击的目标节点可以有多个，例如，通过广播形式发送伪造数据的行为，就可以同时针对多个目标进行攻击。

应对数据伪造攻击的方法有很多。一种方法就是使用身份认证与数据传输同时进行，在完成身份验证后决定接收或丢弃数据。为了其他安全因素，此时所传输的数据应该有其他安全保护措施。例如，对数据进行加密处理，甚至在加密处理过程中还添加了其他辅助信息，如身份标识、计数器等。另一种方法是加密技术。由于伪造的数据不能正确执行加密算法，因此接收端可以根据解密后的数据格式判断数据是否合法。需要注意的是，当物联网中所传输的数据不具有固定格式时，如温湿度数据，则无法通过解密后的数据格式来判断是否合法，需要在数据中添加辅助信息，例如发送方或接受方的身份标识。这样，通过解密后验证身份标识那部分数据的格式是否正确，就可以判断数据是否合法，从而可避免数据伪造攻击。

**8. 数据篡改攻击**

攻击者截获正常传输的数据，进行非法篡改，如数据注入、数据删除、数据替换等，然后发给目标接收设备。在接收到错误数据后，物联网作出错误的反馈指令或者提供错误的服务，进一步影响物联网应用和网络的效率。例如，2014 年 5 月，美国一个网络安全公司发布了一份最新的研究报告，指出网络黑客已经能够轻松入侵并操控城市交通信号系统以及其他道路系统，涉及范围涵盖纽约、洛杉矶、华盛顿等美国大城市。黑客能够通过改变交通灯信号、延迟信号改变时间、改变数字限速标记，从而导致交通拥堵甚至车祸，研究者 Cesar Cerrudo 表示，目前根本没有任何方法能够防止交通控制设备被入侵。

应对数据篡改攻击需要数据完整性保护技术。数据完整性保护技术的原理是对数据的任意非法篡改，接收方都能检测到。一种常用的方法是数字签名和消息认证码技术，这两种技术都是基于哈希函数来实现。但这不是实现数据完整性保护的唯一手段，正确使用加密方法也可以保护数据完整性。

**9. 重放攻击**

物联网环境中，攻击者可以使用恶意节点或恶意设备向目的主机发送已经通过认证的合法身份信息欺骗目的主机，使得恶意节点或恶意设备获得物联网的信任。重放攻击通常

发生在认证过程，以破坏认证的有效性为目的。例如，英国埃塞克斯郡的艾平森林区，一辆特斯拉 Model S 汽车在深夜时分遭到盗贼的重放攻击，然后被盗了。

应对重放攻击需要提供数据的新鲜性。数据的新鲜性是指传输的数据携带一种表明数据在时间上是有效的，或在行为上是有效的标签。如果数据接收时间与发送时间差小于预先设置的最大误差，则在时间上有效；如果数据不是最新接收的数据，而是之前发送的任何数据，则在行为上有效。但标注数据新鲜性的标签需要受到安全保护，否则攻击者可以非法篡改，使其失去提供新鲜性的作用。例如，发送数据时添加时间戳 $T$，数据格式为 $T \parallel E_k(T \parallel \text{data})$，则收信方解密后验证时间戳是否在可允许的范围之内即可。不难看出，在加密数据之外还有一个时间戳 $T$，这个数据不是必需的，但可以方便验证，如果时间戳不合法，则直接将数据忽略，无须执行解密算法，因为执行解密算法的功耗要明显大于执行时间戳合法性检验所需功耗。如果物联网终端没有时钟，则可以使用一个计数器值 Ctr 实现消息新鲜性保护，每次发送数据时将计数器的值 Ctr 递增，然后发送 $\text{Ctr} \parallel E(\text{Ctr} \parallel \text{data})$。接收方检查 Ctr 是否比本地记录的值大，以确定数据是否新鲜。同样，放在加密算法之外的部分用于方便验证，放在加密算法之内的部分用于保护数据不受攻击者非法篡改。

**10. 密码分析攻击和侧信道攻击**

密码分析攻击可以使用获取的密文或明文推断加密算法中使用的加密密钥。密码分析攻击的效率十分低下。为了提高效率，攻击者提出一种改进的攻击方式——侧信道攻击。侧信道攻击是指利用分析电路运行的时间消耗、功率消耗或电磁辐射之类侧信道泄漏，探查电路运行规律的攻击手段。即攻击者对物联网的加密设备实施一些技术能够获得物联网用来加解密数据的加密密钥。例如，在受到最小信号干扰的环境下，攻击者能通过中断路由器 Wi-Fi 信号来检测出用户在键盘上的击打记录，然后利用这些数据盗取用户的密码。另一种典型的侧信道攻击是时间攻击，攻击者通过分析执行加密算法需要的时间信息进而获得加密密钥。例如，在密钥算法中，能够通过时间片的分析，对应得到加解密程序中的循环指令的周期；进一步通过该周期和算法分析，能够推算出密钥的可能结果或规律。侧信道攻击的有效性远高于密码分析攻击的数学方法，因此给密码设备带来了严重的威胁。当前防止侧信道攻击的方法及装置多为对电路进行外部隔离或外部加干扰，但这类方法及装置往往容易通过硬件设备拆解方式破除保护层。

**11. 窃听攻击和干扰攻击**

物联网中的大多数设备和节点通过无线网络进行通信，无线网络通信存在固有的漏洞，通过无线链路传递的信息容易遭受非授权用户的窃听。采用相关安全加密算法和密钥管理机制能够有效抵抗窃听攻击。

干扰攻击是指发送噪声数据或噪声信号对无线链路中传输的信息进行干扰，从而使感知层采集的数据不能及时传输到应用层，或因数据的频繁重传导致感知层节点能量消耗过快而失效。利用屏蔽技术或调频技术可以减少电磁干扰。

**12. 睡眠剥夺攻击**

物联网中的多数设备和感知节点采用电池作为能源供给，电量十分有限。为了延长设备和节点的生存周期，物联网中的设备或节点被设计成遵循特定睡眠机制以降低能源消耗。然而睡眠剥夺攻击能够破坏这种特定的睡眠机制，让节点或设备一直处于唤醒状态，直到其

电源耗尽而关机。

应对睡眠剥夺攻击的主要思路是延长设备或节点的存活周期，能源补充策略可以作为备选方案，设备或节点能够通过外界环境补充能源，例如太阳能。除此之外，需要在物联网环境中研究抵抗睡眠剥夺攻击的安全占空比机制。

**13. 女巫攻击**

女巫攻击又称为 Sybil 攻击。攻击者可以通过伪造许多虚假身份或假冒其他设备的身份发送假的数据信息。实施这种攻击无须使用多个真实的物联网设备，可以使用一台计算机另加一个视频模块，用计算机设备伪造或假冒身份制造信息，由视频模块发送伪造的身份和数据，这样一台设备就可以伪造和假冒许多设备，造成网络数据混乱。

应对女巫攻击需要对设备身份进行认证，使得伪造和假冒的身份都不能通过身份认证过程。但是，如果攻击者掌握了一个物联网设备的合法身份标识和密钥，则假冒这个身份是可能的。从接收和处理数据的平台来说，如果发现从同一身份标识发来的信息内容差距很大，则可以通过对终端设备的行为分析发现异常。这种方法不是普通的密码技术，而且在资源受限的物联网终端设备上实现也有一定难度。

### 5.1.4 物联网感知层的安全机制

针对物联网感知层面临的安全威胁，目前采用的物联网安全保护机制主要有以下五种。

**1. 物理安全机制**

感知节点数量庞大，直接面向世间万“物”。感知层安全技术的最大特点是“轻量级”，不管是密码算法、各种通信协议，还是硬软件设计、硬软件资源，都要求不能复杂。“轻量级”安全技术的结果是感知层的安全等级比网络层和应用层要“弱”，如一些低成本的 RFID 标签和二维码具有价格低、安全性差等特点。受资源和成本限制，这种安全机制主要通过牺牲部分标签的功能来实现。

**2. 认证授权机制**

认证授权的目的是保证未授权的设备和应用不能接入物联网，网络中传输的数据均是合法的，设备和应用请求的数据也是合法的。但在物联网中实现对每个数据和设备的识别与认证是一项非常艰巨的任务，因为物联网中存在大量不同类型的设备，产生的数据类型也是多种多样的。因此，设计有效的机制对设备或数据进行认证在物联网中起到关键作用。主要包括内部节点间的认证授权管理和节点对用户的认证授权管理。

**3. 访问控制机制**

访问控制机制旨在保护用户对于节点自身信息的访问控制和对节点所采集数据信息的访问控制，以防止未授权的用户对感知层进行访问。常见的访问控制机制包括强制访问控制、自主访问控制、基于角色的访问控制和基于属性的访问控制。

**4. 加密机制和密钥管理**

加密机制和密钥管理是所有安全机制的基础，是实现感知信息隐私保护的重要手段之一。密钥管理需要实现密钥的生成、分配、更新和传播。

**5. 安全路由机制**

安全路由机制的目的是保证当物联网遭受攻击时，仍能正确地进行路由发现、构建，主

要包括数据保密和鉴别机制、数据完整性和新鲜性校验机制、设备和身份鉴别机制以及路由消息广播鉴别机制。

## 5.2　RFID 安全

随着 RFID 标签应用的日益广泛，其安全问题日益突出。一方面，由于 RFID 标签的存储资源及计算能力有限，复杂的加密算法往往无法在 RFID 标签上使用；另一方面，由于读写器通过开放的无线通信环境与 RFID 标签进行交互，在用户不知情的情况下，其通信容易受到窃听、篡改、重放等攻击，导致数据加密困难，数据安全、用户隐私问题日益严重。例如，在超市中粘贴在一个昂贵商品上的 RFID 标签可能被改写为一个便宜的商品的信息。在军事领域，敌人可以在仓库出入口秘密安装一个读写器，通过掌握部队的物资调度和流转等信息进而推测出部队的兵力及其部署情况。

为了更好地认识、发现、解决 RFID 安全问题，本节将在介绍 RFID 的基本概念、安全属性、安全假设的基础上，将重点对 RFID 安全威胁及其安全解决方案进行探讨。

### 5.2.1　RFID 概述

RFID 即射频识别，俗称 RFID 标签，是一种非接触式的自动识别技术，它通过射频信号自动识别目标对象并获取相关数据，可快速进行物品追踪和数据交换，无须人工干预。由于 RFID 标签具有成本低、耐磨损、识别速度快、读取距离大、使用寿命长、可动态修改数据等优点，因此广泛应用于资产跟踪、供应链管理、库存管理、高速公路 ETC 系统、门禁、仓储物流、银行卡等诸多领域，成为了物联网感知层应用最广泛的一项技术。比如，将 RFID 标签附着在一辆正在生产中的汽车，厂家可以追踪此车在生产线上的进度；将 RFID 标签附着在物资上，仓库可以实时追踪物资所在位置，加快物资出入库；RFID 标签也可以附着于牲畜与宠物上，方便对牲畜与宠物的识别；基于 RFID 的身份识别卡可以使员工得以进入所住的建筑部分，汽车上的射频应答器也可以用来征收收费路段与停车场的费用。

**1. RFID 系统组成**

一套完整的 RFID 系统通常由三类实体构成：RFID 标签、读写器和后台服务器，如图 5-1 所示。

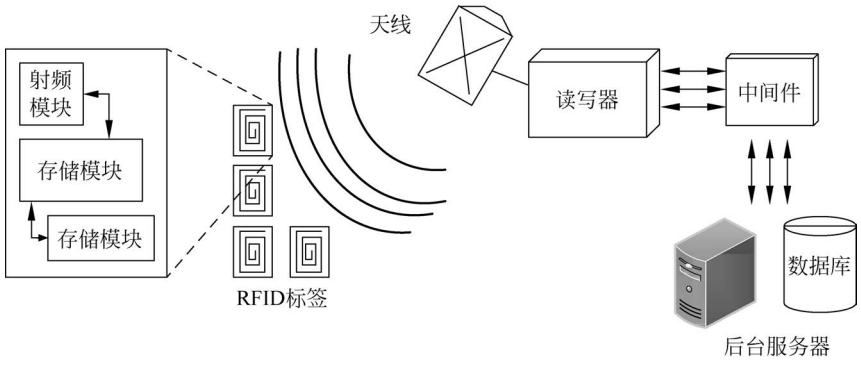



**图 5-1　RFID 系统**

(1) RFID 标签

RFID 标签由芯片、天线及载体组成。其中,芯片用来存储标签 ID 等特定信息,天线主要是用来与读写器通信、接收和发送信息和指令,既可以内置于读写器中,也可以通过同轴电缆与读写器的射频输出端口相连。载体用来安装和保护芯片和天线。

根据能量来源不同,可将 RFID 标签分为被动标签、半被动标签和主动标签三类。被动标签内部没有电源,它通过接收读写器的电磁波信号驱动其内部电路,从而向读写器回传信号。因此,被动标签成本较低且体积较小,在市场上有广泛的应用。与被动标签不同,半被动标签提供内部电源。当收到读写器的询问信号时,半被动标签可以使用内部电源驱动标签工作,具有更高的效率。主动标签内含有电池来支持其通信,它可以主动触发通信并具有 100m 以上的读取距离,但其成本相对较高。

根据工作频率不同,又可将 RFID 标签分为低频标签、高频标签、超高频标签和微波标签。低频标签的工作频率范围为 30～300kHz,典型的工作频率有 125kHz 和 133kHz。此类标签一般为无源标签,其阅读距离通常小于 1m。主要适合廉价、省电、近距离、低速及数据量少的识别应用,如动物识别、自动化生产等。高频标签的工作频率范围为 3～30MHz,典型的工作频率为 15.36MHz。此类标签的工作方式与低频标签类似,但其传输速度有所提高。典型应用有无线 IC 卡、电子身份证、电子车票等。超高频标签的工作频率范围为 850～910MHz。微波标签的工作频率为 2.54GHz。这两种标签存储数据量大、阅读距离远且具有较高的阅读速度,但更容易受到周围无线信号的干扰。目前,低频和高频标签技术已经在物联网中得到了广泛的应用。由于具有低成本及可远距离识别等优势,超高频标签技术将成为未来应用的主流。

(2) 读写器

读写器通常由射频模块、控制单元和耦合单元组成,一般有较好的内部存储和处理能力,复杂的计算,比如各种加密操作也可以在读写器中执行。读写器可通过有线或无线的方式和后台服务器相连,通过天线与 RFID 标签进行无线通信以实现对 RFID 标签的识别和读写。读写器是 RFID 系统中最重要的基础设施,可设计为手持式或固定式。典型读写器示意图如图 5-2 所示。

**图 5-2　典型读写器示意图**

(3) 后台服务器

由于 RFID 标签在数据存储和处理上的局限性,使得标签内存储的消息非常有限,因此关于物品的业务信息(如生成日期、型号、编码等详细描述)通常存储在后台服务器。后台服务器一般具有较强的处理能力,它通过数据库管理它所拥有的读写器和标签的信息。一般地,由于读写器和后台服务器的数据处理和存储能力都比较强,它们之间可以使用各种密码

技术或通信协议，因此在考虑 RFID 系统安全时，通常假设读写器和后台服务器之间的通信信道是安全的。

**2. RFID 系统工作原理**

RFID 系统的工作原理主要分为以下四步。

(1) 读写器通过天线发出一定频率的射频信号(即电磁波)。

(2) RFID 标签进入读写器的工作区域后，对于无源或被动 RFID 标签，通过天线接收到的读写器发出的射频信号，激励起足够的感应电流激活标签，推动标签内部电路工作；标签随即通过天线响应载有数据的射频信号。

对于有源或主动 RFID 标签，由标签主动发送某一频率的带有产品信息的射频信号。

(3) RFID 响应的这些微弱的射频信号再被读写器接收。

(4) 读写器读取信息并解码后，送至后台服务器进行有关数据处理。

**3. RFID 系统的认证模式**

RFID 系统的认证模式一般采用 3 次握手的认证协议，下面以被动 RFID 标签为例进行说明，如图 5-3 所示。

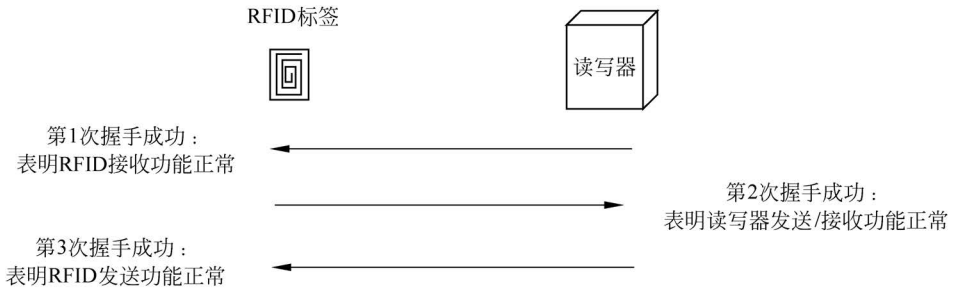



**图 5-3　RFID 系统认证模式**

读写器向 RFID 标签发送身份认证请求信息，验证 RFID 标签是否是合法的。

第 1 次握手，当 RFID 标签接收到该信息后，表明 RFID 标签的接收功能正常。RFID 标签向读写器发送身份认证请求信息的应答消息。

第 2 次握手，当读写器接收到该应答信息后，表明读写器发送和接收功能都正常。读写器向 RFID 标签发送应答消息的确认信息。

第 3 次握手，当读写器接收到该确认信息后，表明 RFID 标签的发送功能是正常的。通过 3 次握手就能表明双方的收发功能均正常，也就是说，可以保证 RFID 标签和读写器建立的连接是可靠的。但是，在 RFID 系统的这种认证过程中，属于同一应用的所有 RFID 标签和读写器共享同一密钥，所以 3 次握手的认证协议具有一定的安全隐患。

## 5.2.2　RFID 安全需求

RFID 系统除了需要保证 RFID 标签和读写器之间无线传输信道上信息的安全，还需要保护 RFID 标签或读写器上的数据及其自身的隐私信息不被泄露。因此，一个安全的 RFID 系统除了有物联网基本安全需求外，还有其特有的安全需求：隐私性和时效性。

**1. 机密性**

机密性是指任何未经授权的实体均无法读取 RFID 标签或读写器的内部秘密数据，也无法读取 RFID 标签和读写器之间传输的秘密信息。机密性对于电子钱包、公交卡等包含敏感数据的 RFID 标签非常关键，但对一些 RFID 广告标签和普通物流标签则不必要。

**2. 完整性**

完整性是指 RFID 标签内部数据及与读写器之间的通信数据不能被非法篡改，或者即使被篡改也能够被检测到。数据被篡改会导致欺骗的发生，因此大多数 RFID 应用都需要保证数据完整性。

**3. 可用性**

可用性是指 RFID 系统的合法用户能够正常访问和使用系统内的信息，攻击者无法阻止合法用户获得他所需的信息。对于 RFID 系统而言，由于空中接口反射信号微弱和防冲突协议的脆弱性等原因，可用性受到破坏或降级的可能性较大。但对一般民用系统而言，通过破坏空中接口获利的可能性比较小，而且由于无线信号很容易被定位，因此这种情况较难发生。但在公众场合，RFID 标签的可用性则很容易通过屏蔽、遮盖、撕毁手段等被破坏，因此也应在系统设计中加以考虑。

**4. 不可否认性**

RFID 标签或 RFID 读写器能够确保节点不会否认它所发出的消息。

**5. 可控性**

这里的可控性是指通过各种技术手段控制 RFID 信号的读写范围、读写频率等，实现对 RFID 标签数据流向及行为方式的安全监控管理，防止被非法利用。如通过控制射频信号的频率控制其工作范围等，通过加密等方式控制标签响应信号即使被非法读写器读入，也不能正确解码。

**6. 可认证性**

可认证性是指在 RFID 系统中进行信息交互的都是合法用户，从而拒绝非法用户的任何请求，和合法用户的非法请求等。对于 RFID 系统而言，真实性主要是要保证读写器、RFID 标签及其数据是真实可信的，要预防伪造和假冒的读写器、RFID 标签及其数据。如果 RFID 标签没有存放敏感数据，则对读写器的真实性要求不高，但由于标签数据要被送到后台系统中进一步处理，虚假数据可能导致较大的损失，因此要求标签及其数据是真实的。

**7. 隐私性**

隐私性一般可分为信息隐私、位置隐私和交易隐私。信息隐私是指用户相关的非公开信息不能被获取或被推断出来。位置隐私是指携带 RFID 标签的用户不能被跟踪或定位。交易隐私是指 RFID 标签在用户之间的交换，或者单个用户新增某个标签、失去某个标签的信息不能被获取。与个人无关的物品，如动物标签等没有隐私性的要求。低频标签通信距离近，隐私性需求不强，但高频、超高频和微波标签对隐私性有一定的要求。对于不同的国家及不同的人而言隐私性的重视程度也不相同。但重要的政治和军事人物都需要较强的隐私性。隐私性决定了哪些信息可以放在 RFID 标签中。

**8. 时效性**

时效性有时也被称为新鲜性。RFID 标签和读写器能够确保接收到的数据的实时性。时效性属性是保障 RFID 能够抵抗重放攻击的基本属性。

### 5.2.3　RFID 安全假设

为更好地对 RFID 安全问题进行研究，学者们通常进行了如下假设。

**1. 信道安全的假设**

由于标签-读写器的通信信道一般采用无线通信方式，读写器-后台服务器的后端网络通信信道一般采用有线方式连接，因此一般假设标签-读写器之间的通信信道是不安全的；读写器-后台服务器之间的通信信道的数据通过某种访问措施来保证安全，因此是安全的信道，如图 5-4 所示。

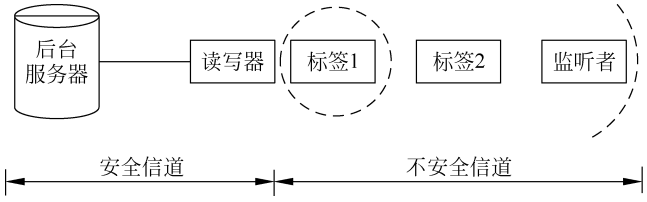



**图 5-4　信道安全假设**

**2. 抗干扰能力的假设**

按照工作频率的不同，RFID 标签可以分为低频、高频、超高频和微波 4 种。低频和高频的 RFID 标签一般采用电磁耦合原理，而超高频及微波 RFID 标签一般采用电磁发射原理，不同频率的 RFID 标签特点不同、应用场景也不同。由无线电信号的物理特性可知，对于超高频远距 RFID 标签，由于 RFID 标签与读卡器之间的通信距离更远，因此更容易受到无线信号的干扰。表 5-1 给出了不同工作频段 RFID 标签的特点。

**表 5-1　不同工作频段 RFID 标签的特点**

| 频　　段 | 特　　点 | 适 用 场 合 |
|---|---|---|
| 低频(30～300kHz) | 不易受干扰、读取距离短 | 工具识别、动物芯片、汽车防盗器 |
| 高频(3～30MHz) | 易受干扰，感应距离较长、读取速度较快，可同时间辨识多个标签 | 门禁系统、图书馆管理、产品管理 |
| 超高频及微波(＞300MHz) | 极易受干扰，读取距离较远、传输速率较快 | 铁路车厢监控 |

**3. 用于安全的硬件资源假设**

RFID 标签得以广泛应用的一个重要原因是其制造成本低，目前一枚 RFID 标签的成本可以控制在 10 美分内，折合人民币在几毛钱内，未来 RFID 标签价格有望降到 5 美分。受成本限制，RFID 标签内部拥有逻辑门的数量非常有限，仅能进行简单的逻辑处理，因此可分配用于安全模块的逻辑门数就更有限了，一般不超过 5000 门。按一个逻辑门对应一位二进制数换算，相当于一个 RFID 标签可用于安全数据的容量为 5000bit，约 5 字节数据。

**4. 数据传输的假设**

为保证 RFID 系统的正常工作，确保每个 RFID 标签能够传输可靠的数据，数据传输量一般不超过 500bit，读取时间不超过 1s。

**5. 抵抗数据篡改能力的假设**

物理攻击下，RFID 标签内部数据一定会泄漏。

**6. 读写功能的假设**

可以限制写入设备向 RFID 标签内存写数据。

### 5.2.4 RFID 安全威胁

RFID 安全威胁主要源于对标签或读写器的攻击、对标签-读写器前端无线通信信道的攻击和对读写器-后台服务器后端网络通信信道的攻击，以达到盗取 RFID 标签数据、扰乱 RFID 标签读写过程和篡改 RFID 标签信息的目的。

**1. 物理攻击**

由于 RFID 标签的应用规模比较大，因此攻击者很容易获得 RFID 标签并对其加以分析或破坏。一般来说，对标签的物理攻击主要包括探测攻击、电磁干扰、故障分析和功率分析等非破坏攻击，和通过小刀等工具破坏标签，使其无法被读写器识别和读取的破坏性攻击。一般的 RFID 标签，特别是低成本的 RFID 标签很难抵抗物理攻击。因此，假设在物理攻击下，RFID 标签内部的数据均会泄漏。但该攻击手段成本过高，对攻击者的吸引力很小。

**2. 窃听攻击**

窃听攻击是指攻击者未经授权而使用无线电接收设备监听并获取 RFID 标签和读写器之间无线通信信道上的数据。如果 RFID 标签和读写器之间传输的数据未经保护，那么攻击者可以直接获得标签和读写器的信息，从而导致用户的信息遭到泄露。

**3. 中间人攻击**

被动的 RFID 标签在收到来自读写器的查询信息后会主动响应，发送证明自己身份的信息，因此攻击者可以伪装成合法的读写器靠近标签，在标签携带者不知情的情况下进行读取，并将从标签中读取的信息直接或者经过处理后发送给合法的读写器，以达到各种非法目的。在攻击过程中，攻击者通过各种技术手段插入或修改标签与读写器之间的通信信息，而不被标签或读写器所察觉，标签和读写器都认为攻击者是正常通信流程中的另一方。应对中间人攻击的方法是在信息交换的两个方向上都提供数据源认证服务。

**4. 假冒攻击**

假冒攻击包含两类：一类是假冒合法读写器获取 RFID 标签的信息；另一类是假冒合法 RFID 标签干扰其他标签和读写器间的正常通信。要成功实施此类攻击，通常需要掌握相关通信协议和秘密信息。在进行攻击时，攻击者需要接收并读取加密消息，然后将虚假信息反馈给标签或读写器。

**5. 克隆攻击**

克隆攻击经常被归类为假冒攻击。然而，二者在本质上是不一样的。假冒攻击是非法

标签或非法读写器通过某种手段(不限于克隆)使其自身具有合法身份,从而参与 RFID 系统的数据通信,而克隆攻击利用 RFID 标签在认证过程中的漏洞将合法 RFID 标签上的数据复制到由攻击者所控制的新标签上。克隆标签可以以合法身份在 RFID 系统中执行攻击者的各种攻击计划,危害性比假冒攻击更大。例如,只使用用户标识(User ID,UID)字段作为验证数据的 RFID 标签,就可以轻松实现克隆攻击。克隆攻击典型的应用场景就是手机复制门禁卡。

**6. 篡改攻击**

篡改攻击是攻击者利用技术手段修改 RFID 的空中接口数据(如无线电频段,调制解调方式,数据编码方式,以及协议)和标签数据等。例如,作为 RFID 的典型应用,公交卡、饭卡和购物卡等卡中均记录有金额、消费记录等信息,通过特定的工具就可以篡改卡片中的金额。

**7. 拒绝服务攻击**

拒绝服务攻击的目的是破坏标签和读写器之间的正常通信。攻击者可以通过驱动多个标签发射信号或设计专门的标签攻击防冲突协议,对读写器的正常工作进行干扰。这样读写器将无法区分不同的标签,进而导致系统服务中断,使得合法的标签无法与读写器正常通信。对于需要动态刷新标签身份标识(ID)的一类协议,容易遭受此类攻击。但这种攻击手段对 RFID 系统本身并不产生破坏,只是干扰系统的通信,且它不可能在公开场合长时间实施,系统恢复较快,所以拒绝服务攻击是所有攻击中危害最小的攻击手段。

**8. 重放攻击**

当读写器向标签发出认证请求后,攻击者截获了合法标签对该认证消息的响应信息;当下一次读写器再次发出认证请求时,攻击者把截获的合法标签的响应信息发送给读写器,从而通过读写器对它的身份认证。比如作为典型的 RFID 的应用,汽车遥控钥匙本身也是一张 RFID 卡,使用的频段是 433MHz/315MHz。采用 HackRF 设备就可以在汽车遥控钥匙开锁的过程中记录下交互的数据,进行逆向解析;对应上频段和波形之后,进行数据重放,就可以远程开启汽车。解决重放攻击的有效方式是在标签响应消息中添加响应时间信息,同时在读写器中增加对时间信息时效性的验证。例如标签在 $t_1$ 时刻的信息不足以用来在 $t_2$ 时刻 ($t_2 > t_1$)识别认证该标签。

**9. 病毒攻击**

RFID 标签本身不能检测它所存储的数据是否有病毒,攻击者可以事先把病毒代码写入标签中,然后让合法的读写器读取其中的数据,这样病毒就有可能植入系统中。当病毒或者恶意程序入侵后台服务器的数据库后,可能会迅速传播并摧毁整个系统。

**10. 屏蔽攻击**

屏蔽攻击是指用机械的方法来阻止读写器对 RFID 标签进行读取。例如,使用法拉第网罩或护罩阻挡某一频率的无线电信号,使读写器不能正常读取标签。攻击者还有可能通过电子干扰手段来破坏 RFID 标签读取设备对 RFID 标签的正确访问。

**11. 略读攻击**

略读攻击实质是一种非法访问攻击,是指在标签所有者不知情、或没有得到所有者同意

的情况下读取存储在 RFID 标签上的数据。它可以通过一个特别设计的读写器与标签进行交互来得到标签中存储的数据。这种攻击之所以会发生，是因为一些标签在不需要认证的情况下也会广播其所存储的数据内容。

**12. 演绎攻击**

演绎攻击也称为推理攻击。任意一个标签的用户，或者能获取标签信息的攻击者，他们通过数据信息演绎来推算出其他标签的信息，甚至可以计算出整个后台服务器中数据库的信息，这种情况也时常出现在系统管理者身上，因为他们具有某些标签的权限，从而获得其他未经许可的信息。

**13. 非法跟踪攻击**

非法跟踪攻击的原理是攻击者通过远程识别标签，掌握标签的位置等敏感信息，从而给犯罪活动提供更加便利的目标及相关条件。特别是针对一些对位置信息敏感的物联网应用，如军事侦查，军用物资的存储、运输等，非法跟踪攻击的危害将更大。

### 5.2.5 RFID 安全机制

为了在复杂、异构的物联网环境下实现 RFID 系统安全的目标，学者们提出了两大类安全解决方案：一是基于访问控制的安全机制，一是基于哈希函数的安全机制。因此，设计安全、高效和低成本的 RFID 安全机制仍是物联网安全领域须研究的一个极具挑战性的课题。

**1. 基于访问控制的安全机制**

(1) 封杀标签法

封杀标签法从物理上使标签丧失功能、不能再次使用，从而阻止信息泄露和相关设备对标签的非法跟踪，是一种不可逆的操作。封杀标签法最初是由标准化组织 Auto-ID Center 提出的，用于在零售环节中通过禁用标签来保护消费者隐私。封杀标签法对应 Kill 命令。目前，该 Kill 命令仅在部分类型的标签中使用。通过输入个人识别密码(Personal Indentification Number，PIN)码来触发 Kill 命令，命令启动后，标签的所有信息都被破坏且该标签将永久停用，以确保客户的隐私安全。因此，PIN 码需要被很好地保护，以防攻击者利用获得的 PIN 码来破坏标签的正常使用。PIN 码最早是用于保护手机 SIM 卡的一种安全措施。

(2) 阻塞标签法

阻塞标签法利用称为阻塞器的特殊标签防止隐私区标签被读写器扫描。首先，在标签中加入一个比特，称之为隐私位。隐私位为“0”表示该标签可被公开扫描，隐私位为“1”表示标签是秘密的，无法被扫描。因此，标识符以“1”开头的标签被称为隐私区标签。当读写器发送请求时，阻塞器通过模拟各种可能的标签序列号发送伪造消息给读写器，从而阻止读写器获得真正的标签序列号。需要访问受保护标签时，只要去除阻塞器即可。例如，在商品生产出来到购买之前，即在仓库、运输、货架的时候，标签的隐私比特设置为 0，任何时候都可以扫描它。当消费者购买了使用 RFID 标签的产品，销售终端将隐私比特设置为 1。

(3) 法拉第网罩法

法拉第网罩法通过屏蔽电磁波信号来保护 RFID 标签的隐私信息。具体做法如下：将带有标签的物体放入金属网或金属箔制成的法拉第笼中，由于无线电波无法穿透法拉第笼，

从而使得 RFID 标签无法与外界联系，即阻止标签和读写器通信。然而，攻击者可能利用这个原理屏蔽物品以防止物品被读写器扫描，从而达到盗取物品的目的。此外，当物品较多时，大规模地使用该方法也不太便利。因此，该方案更适用于标签偶尔被使用的场景。如果每件产品都使用一个网罩，成本也较高。

(4) 主动干扰法

主动干扰法的原理是标签用户通过某种设备，主动广播无线电信号用于阻止或破坏附近的读写器。该方法可能干扰附近合法的 RFID 用户，甚至阻塞附近其他无线电信号。

(5) 加密法

加密法的原理是通过对标签端和读写器端的输入或输出数据进行加密，来保证 RFID 系统的安全性。既可以使用对称密码算法来加密数据，也可以使用非对称密码算法来加密数据。在标签中使用密码算法会增加硬件成本。由于多数 RFID 的硬软件资源受限，所以要求用于 RFID 标签数据的加密算法都应是轻量级的。

(6) 物理不可克隆函数(Physical Unclonable Functions，PUF)技术

由于在标签中使用密码算法会增加硬件成本，麻省理工学院的 Srini Devadas 教授及其团队于 2005 年提出了基于 PUF 的方法来保证标签的安全性。PUF 技术是一种硬件安全技术，它利用固有的设备变化来对给定的输入产生不可克隆的唯一设备响应。由于硅加工技术的不完善，所生产的每一块集成电路在物理上都是不同的，主要表现为不同的路径延迟、晶体管阈值电压、电压增益或其他方式。虽然这些变化在不同集成电路之间可能是随机的，但一旦知道，它们是确定的和可重复的。PUF 技术就是利用集成电路的这种内在差异，为每片集成电路生成一个唯一的加密密钥，从而在大大减小计算、存储和通信开销的情况下，抵御物理克隆攻击的发生。PUF 具有鲁棒性、可计算性、唯一性、不可预测性和防篡改性等属性，可应用于认证及密钥生成等领域。

(7) 休眠进制

让标签处于睡眠状态，而不是禁用，以后可使用唤醒口令将其唤醒。困难在于唤醒口令需要和标签相关联，于是这就需要一个口令管理系统。但是当标签处于睡眠时，不可能直接使用空中接口将特定的标签和特定的唤醒口令相连接，因此需要另外一种识别技术，类似条形码，以标识用于唤醒的标签，这显然是不太理想的。

**2. 基于哈希函数的安全机制**

为了解决 RFID 系统中的安全和隐私性问题，早期学者们提出了多种基于哈希函数的 RFID 认证协议，典型的有哈希锁协议、随机哈希锁协议、哈希链协议、基于哈希的 ID 变化、分布式 RFID 询问-应答认证协议和低成本鉴析协议(Low-cost Authentication Protocol，LCAP)等，这类协议由于简单且对系统硬件资源的需求不高，因此适合在无源 RFID 认证中使用。表 5-2 给出了几种协议的对比图。

**表 5-2　RFID 安全认证协议的抗攻击能力对比**

| 安全认证协议 | 防窃听攻击 | 防演绎攻击 | 防拒绝服务攻击 | 防重放攻击 | 防假冒攻击 | 防跟踪攻击 |
|---|---|---|---|---|---|---|
| 哈希锁 | 否 | 否 | 是 | 否 | 否 | 否 |
| 随机哈希锁协议 | 是 | 是 | 否 | 否 | 否 | 是 |
| 哈希链协议 | 是 | 是 | 否 | 否 | 否 | 是 |

续表

| 安全认证协议 | 防窃听攻击 | 防演绎攻击 | 防拒绝服务攻击 | 防重放攻击 | 防假冒攻击 | 防跟踪攻击 |
|---|---|---|---|---|---|---|
| 基于哈希的 ID 变化 | 是 | 是 | 否 | 是 | 否 | 是 |
| 分布式 RFID 询问-应答认证 | 是 | 是 | 是 | 否 | 是 | 是 |
| LCAP | 是 | 是 | 是 | 否 | 是 | 是 |

(1) 哈希锁协议

哈希锁协议是一种完善的抵制标签未授权访问的安全与隐私技术。整个方案只需要采用哈希散列函数给 RFID 标签加锁，成本很低。

认证过程如图 5-5 所示。

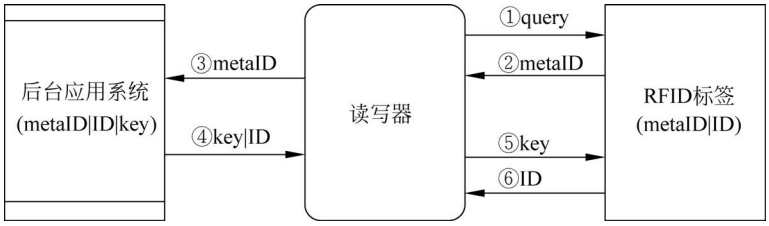



**图 5-5 哈希锁协议原理**

① 当 RFID 标签进入读写器的识别范围内，读写器向它发送 query 消息请求认证。

② RFID 标签接收到读写器的请求命令后，将 metaID 代替真实的标签 ID 发送给读写器，metaID 是由哈希函数映射标签密钥 key 得来，metaID＝Hash(key)，跟真实标签 ID 对应存储在 RFID 标签中。

③ 当读写器收到 metaID 后通过计算机网络传输给后台应用系统。

④ 因为后台应用系统的数据库存储了合法标签的 ID、metaID、key，metaID 也是由 Hash(key)得来。当后台应用系统收到读写器传输过来的 metaID，查询数据库有无与之对应的 ID 和 key，如有就将对应的标签 ID 和 key 发给读写器，如果没有就发送认证失败的消息给读写器。

⑤ 读写器收到后台应用系统发送过来的标签 ID 与 key 后，自己保留标签 ID，然后将 key 发送给 RFID 标签。

⑥ RFID 标签收到读写器发送过来的 key 后利用哈希函数运算 Hash(key)，对比是否与自身存储的 metaID 值相同，如果相同就将标签 ID 发送给读写器，如果不同就认证失败。

⑦ 读写器收到 RFID 标签发送过来的 ID 与后台应用系统传输过来的 ID 进行对比，若相同则认证成功，否则认证失败。

哈希锁协议待改进的地方：哈希锁协议没有实现对标签 ID 和 metaID 的动态刷新，并且标签 ID 是以明文的形式发送传输，不能防止假冒攻击、重放攻击以及跟踪攻击，以及此协议在数据库中搜索的复杂度是呈 $O(n)$线性增长的，还需要 $O(n)$次的加密操作，在大规模 RFID 系统中应用不理想，所以哈希锁并没有达到预想的安全效果，但是提供了一种很好的安全思想。

（2）随机哈希锁协议

RFID标签内存储了标签ID与一个随机数产生程序，RFID标签接到读写器的认证请求后将(Hash($ID_i \| R$)，$R$)一起发给读写器。其中，$ID_i$ 表示数据库中存储的第 $i$ 个标签ID($1 \leqslant i \leqslant n$)，$n$ 表示数据库所有标签的总数，$R$ 是由随机数程序生成的一个随机数，符号“‖”表示连接，$ID_i \| R$ 则表示标签ID和随机数 $R$ 的连接。在收到RFID标签发送过来的数据后，读写器在数据库中查询所有的标签，分别计算是否有一个 $ID_j$ 满足 $Hash(ID_j \| R) = Hash(ID_i \| R)$。如果有，则将 $ID_j$ 发给RFID标签，RFID标签收到 $ID_j$ 后与自身存储的 $ID_i$ 进行对比作出判断。

其认证过程如图5-6所示。

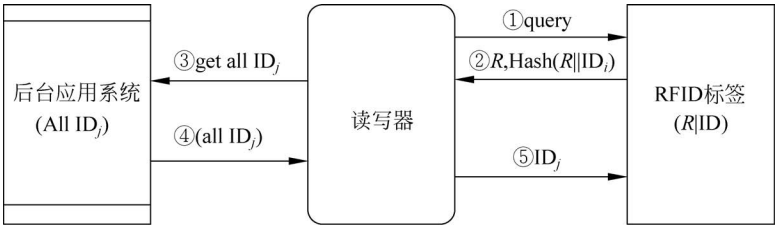



**图5-6　随机哈希锁协议原理图**

① 当RFID标签进入读写器的识别范围内，读写器向它发送query消息请求认证。

② RFID标签接收到读写器的信息后，利用随机数程序产生一个随机数 $R$，然后利用哈希函数对($R \| ID_i$)进行映射求值，$ID_i$ 是RFID标签自身存储的标识，得到 $Hash(ID_i \| R)$，然后RFID标签将($Hash(ID_i \| R)$，$R$)整体发送给读写器。

③ 读写器向后台应用系统数据库发送获得存储的所有标签 $ID_j$ 的请求。后台应用系统接收到读写器的请求后将数据库中存储的所有标签 $ID_j$ 都传输给读写器。

④ 此时读写器收到的数据有RFID标签发送过来的($Hash(ID_i \| R)$，$R$)与后台应用系统传输过来的所有标签 $ID_j$，读写器进行运算，求出是否能在所有标签 $ID_j$ 中找到一个 $ID_j$ 满足 $Hash(R \| ID_j) = Hash(R \| ID_i)$，若有则将 $ID_j$ 发送给RFID标签，没有则认证失败。

⑤ RFID标签收到读写器发送过来的 $ID_j$，验证是否满足与自身存储的 $ID_i$ 相等，若相等则认证成功，否则认证失败。

待改进的地方：标签 $ID_i$ 与 $ID_j$ 仍然是以明文的方式传输，不能预防重放攻击和跟踪攻击。当攻击者获取标签的ID后还能进行假冒攻击，在数据库中搜索的复杂度是呈 $O(n)$ 线性增长的，也需要 $O(n)$ 次的加密操作，在大规模RFID系统中应用不理想，所以随机哈希锁协议也没有达到预想的安全效果，但是促使RFID的安全协议越来越趋于成熟。

（3）哈希链协议

Okubo等提出了基于密钥共享的询问应答安全协议——哈希链协议，该协议具有完美的前向安全性。与上述两个协议不同的是该协议通过两个哈希函数 $H$ 与 $G$ 来实现，其认证过程如图5-7所示。$H$ 的作用是更新密钥和产生秘密值链，$G$ 用来产生响应。每次认证时，标签会自动更新密钥；并且RFID标签和后台应用系统共享一个初始密钥($k_t$，1)。例如，攻击者截获 $H(k_t, 1)$ 后就可以进行重放攻击。所以哈希链协议也不算一个完美的安全协议。

待改进的地方：每一次标签认证时，都要对标签的ID进行更新，增加了安全性，但是也

增加了协议的计算量，成本也相应增加。同时哈希链协议是一个单向认证协议，还是不能避免重放攻击和假冒攻击。

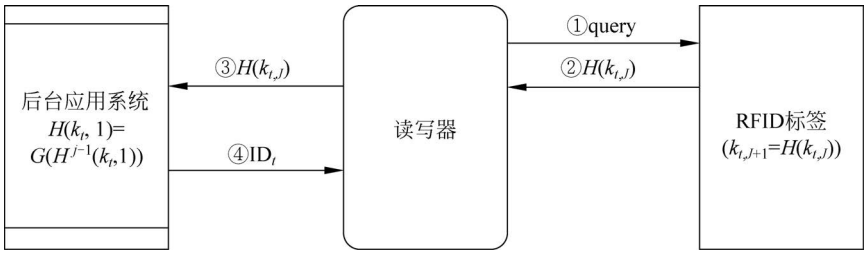



**图 5-7　哈希链协议示意图**

(4) 基于哈希的 ID 变化协议

基于哈希的 ID 变化协议的原理跟哈希链协议有相似的地方，每次认证时 RFID 系统利用随机数生成程序生成一个随机数 $R$ 对 RFID 标签 ID 进行动态更新，并且对 TID(最后一次回话号)和 LST(最后一次成功的回话号)的信息进行更新，该协议可以抵抗重放攻击，其认证过程如图 5-8 所示。

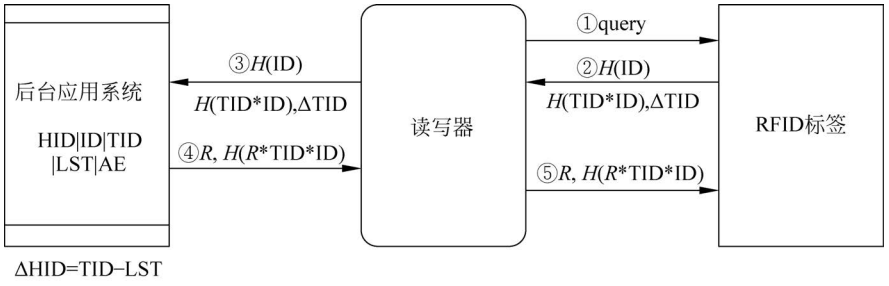



**图 5-8　基于哈希的 ID 变化协议示意图**

待改进的地方：该协议的弊端是后台应用系统更新标签 ID、LST 与标签更新的时间不同步，后台应用系统更新是在第 4 步，而标签的更新是在第 5 步，而此刻后台应用系统已经更新完毕，此刻如果攻击者在第 5 步进行数据阻塞或者干扰，导致 RFID 标签收不到($R$，$H$($R$ * TID * ID))，就会造成后台存储标签数据与 RFID 标签数据不同步，导致下次认证的失败，所以该协议不适用于分布式 RFID 系统环境。

(5) 分布式 RFID 询问-应答认证协议

该协议是 Rhee 等基于分布式数据库环境提出的询问-应答的双向认证 RFID 系统协议，其示意图如图 5-9 所示。当 RFID 标签进入读写器的识别范围后，读写器向其发送 query 消息以及读写器产生的秘密随机数 $R_R$，请求认证。RFID 标签接到读写器发送过来的请求后，生成一个随机数 $R_T$，并计算出 $H(ID \| R_R \| R_T)$，其中，ID 是标签的 ID，$H$ 为标签和后台应用系统共享的哈希函数。然后，RFID 标签将($H(ID \| R_R \| R_T)$，$R_T$)发送给读写器。读写器收到该信息后，向其中添加之前自己生成的随机数 $R_R$，并将($H(ID \| R_R \| R_T)$，$R_T$，$R_R$)一同发给后台应用系统。后台应用系统收到读写器发送来的数据后，检查存储的标签 ID 中是否有一个 $ID_j$($1 \leqslant j \leqslant n$)满足 $H(ID_j \| R_T)=H(ID \| R_R \| R_T)$)，若有，则认证通过，并把 $H(ID_j \| R_T)$发送给读写器。读写器把接收到的 $H(ID_j \| R_T)$发送给 RFID 标签进行验证，若 $H(ID_j \| R_T)=H(ID \| R_T)$，则认证通过，否则认证失败。

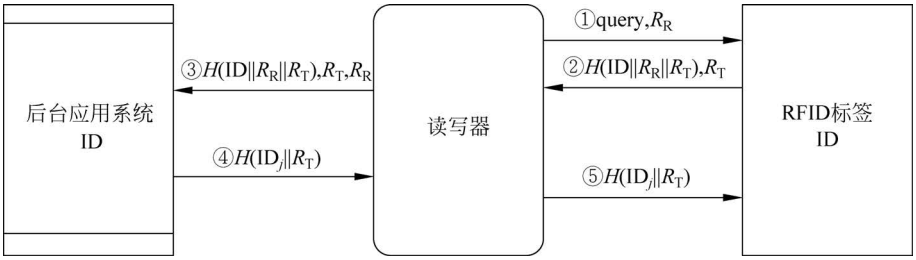



**图 5-9　分布式 RFID 询问-应答认证协议示意图**

待改进的地方：该协议跟基于哈希的 ID 变化协议一样，虽然目前为止还没有发现明显的安全缺陷和漏洞，但成本太高，因为一次认证过程需要两次哈希运算，读写器和 RFID 标签都需要内嵌随机数生成函数和模块，不适合小成本 RFID 系统。

（6）LCAP

LCAP 是基于标签 ID 动态刷新的询问-应答双向认证协议。与前几种协议不同的是它每次执行之后都要动态刷新标签的 ID。其示意图如图 5-10 所示。

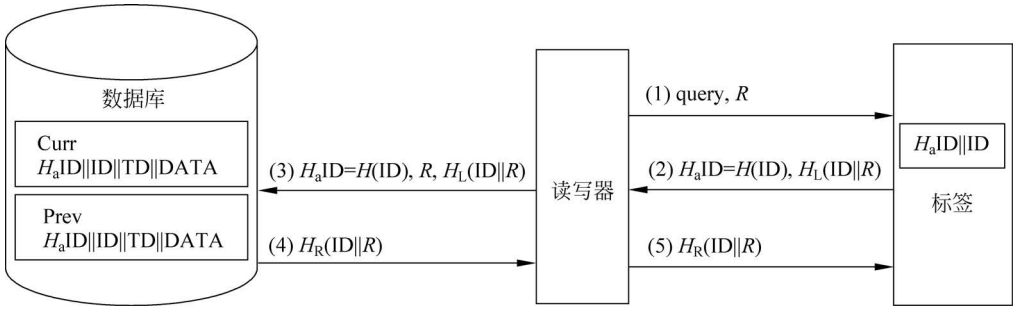



**图 5-10　LCAP 示意图**

当标签进入读写器的识别范围后，读写器通过向它发送 query 消息以及读写器产生的一个秘密的随机数 $R$，请求认证。标签收到读写器发送过来的认证信息后，利用哈希函数计算出 $H_a\mathrm{ID}=H(\mathrm{ID})$和 $H_L(\mathrm{ID}\|R)$，其中，ID 为标签的 ID，$H_L$ 表示哈希函数映射值的左半部分，即 $H(\mathrm{ID}\|R)$的左半部分；之后标签将($H_a\mathrm{ID}$，$H_L(\mathrm{ID}\|R)$)一起发送给读写器。读写器收到上述消息后，在其中添加之前发送给标签的秘密随机数 R，将消息($H_a\mathrm{ID}$，$H_L(\mathrm{ID}\|R)$，$R$)发送给后台数据库。后台数据库收到读写器发送过来的数据后，检查数据库存储的 $H_a\mathrm{ID}$ 是否与读写器发送过来的一致。若一致，则利用哈希函数计算 $R$ 和数据库存储的 $H_a\mathrm{ID}$ 的 $H_R(\mathrm{ID}\|R)$，$H_R$ 表示哈希函数映射值的右半部分，即 $H(\mathrm{ID}\|R)$的右半部分，同时后台数据库更新 $H_a\mathrm{ID}$ 为 $H(\mathrm{ID}\oplus R)$，ID 更新为 $\mathrm{ID}\oplus R$，并将之前存储的数据中的 TD 数据域设置为 $H_a\mathrm{ID}=H(\mathrm{ID}\oplus R)$，然后将 $H_R(\mathrm{ID}\|R)$发送给读写器。读写器收到 $H_R(\mathrm{ID}\|R)$后将其转发给标签。标签收到 $H_R(\mathrm{ID}\|R)$后验证其有效性，若有效，则认证成功。

待改进的地方：通过对以上流程的分析不难看出，LCAP 存在与基于哈希的 ID 变化协议一样的不足，就是标签 ID 更新不同步，后台数据库更新在第 4 步，而标签更新是在它更新之后的第 5 步，如果攻击者攻击导致第 5 步不能成功，就会造成标签数据不一致，进而导致认证失败以及下一次认证的失败。因此该协议不适用于分布式数据库 RFID 系统。

## 课程思政

2020年12月8日从WAPI产业联盟获悉，我国自主研发的一项物联网安全测试技术（TRAIS-P TEST）由ISO/IEC发布成为国际标准，编号为：ISO/IEC 19823-16：2020，标准全称是：《信息技术 安全服务密码套件一致性测试方法 第16部分：用于空中接口通信的密码套件ECDSA-ECDH安全服务》。**这是我国在物联网安全技术领域获发布的又一项拥有自主知识产权的国际标准，标志着我国在全球物联网安全测试技术规则领域取得首个突破，也是我国加强关键领域自主知识产权创造储备战略背景下的又一重要成果。**该标准是TRAIS-P（ISO/IEC 29167-16：2015）国际标准的测试标准，它规范了RFID安全密码套件一致性测试方法。该标准发布后，将从技术到产品测试两个层面共同构成国际标准体系，用于保护有源RFID产品和系统安全，为全球RFID系统提供强健的空口安全连接能力。

西电捷通公司、无线网络安全技术国家工程实验室、国家商用密码检测中心、国家信息技术安全研究中心、中国通用技术研究院、国家无线电监测中心检测中心、天津市无线电监测站等十余家单位全程参与了标准开发工作，西电捷通公司是主要技术贡献者。至此，我国在ISO国际标准方面贡献技术并作出必要专利声明的标准共26项，其中涉及网络安全的标准占12项。

通过该标准成为国际标准的案例进行爱国强国意识教育，希望学生刻苦钻研，激发学员学术科技报国的家国情怀和科技强军的使命担当。让学生产生对科学和技术的热爱，也希望他们体会到技术进步、技术领先对国家的重要性，了解到没有自主技术和知识产权，一个国家是难以真正强大。我们为祖国的发展和强盛而自豪，同时要树立提升国家民族科技实力的责任感和使命感。

## *案例

### 传感器竟成“窃听器”

2020年国际四大信息安全会议之一的“网络与分布式系统安全会议”上，一项来自浙江大学、加拿大麦吉尔大学、多伦多大学学者团队的最新研究成果显示：部分智能手机App可在用户不知情且无须系统授权的情况下，利用手机内置的加速度传感器来采集手机扬声器所发出声音的振动信号，实现对用户语音的窃听。其原理主要是由于声音信号是一种由振动产生的、可以通过介质传播的声波，手机扬声器发出的声音会引起手机的震动，而加速度传感器可以灵敏地感知这些震动，因此攻击者可以通过它来捕捉手机震动进而破解其中所包含的信息。在关键字检测任务中，这种窃听攻击识别用户语音中所携带关键字的平均准确率达到了90%。

手机加速度计可以收集语音信息，这意味着攻击者可以从用户的手机中窃取多种隐私数据。比如，攻击者也许可以从语音信息中提取用户的家庭住址、信用卡信息、身份证号、用户名密码等一系列重要信息；通过窃听手机地图的语音导航系统，攻击者也许能提取出一些跟位置有关的关键字，推断出用户目前的位置以及目的地；通过窃听用户手机播放的音乐和视频，攻击者可以推断出用户在这些方面的偏好。因此，这种攻击方式对用户隐私安全具有很大威胁。

从上述案例可以看出，“传感器数据”亟待重新审视。现行的法律法规对个人敏感信息

的保护，主要是针对证件号码、金融账户等具体的个人敏感信息。由于加速计数据本身并不属于个人敏感信息，攻击者可以利用计步软件等必须用到加速计的App“合理”地对加速计数据进行收集，因此采集加速计数据这种行为本身并不违法。这就意味着，这种攻击方式目前仍处于法律法规的灰色地带。

为有效防御此类攻击，相关专家建议首先应该从技术层面加大对移动设备物理层安全的研究投入，了解各类传感器的实际数据采集能力以及它们可能造成的隐私问题，对可能存在的各类攻击做到心中有数。然后依此重新设计智能手机操作系统中各类传感器的权限使用机制，从技术的角度尽可能地降低数据被滥用的可能性。此外，还应当从法律法规上细化对敏感信息的定义和使用规范。除了对证件号码、银行账户、通信记录和内容等具体的个人敏感信息进行保护外，还应对可能包含这些信息的原始传感器数据进行保护，规范和限制这类数据的采集和使用方式。

那么作为普通消费者，我们目前有机会防止自己的手机被窃听吗？在各大手机厂商提出进一步的解决方案之前，消费者能够采取的最有效也最便捷的防御方式，就是通过耳机来接听电话或语音信息。手机中的加速度计与耳机间存在着物理隔离，使加速度计无法监测到耳机发出的振动，所以通过耳机播放的声音是不会被这种攻击窃听的。

## 5.3　无线传感器网络安全

无线传感器网络的安全技术研究是当前的热点和富有挑战性的一项课题，特别是无线传感器网络在军事与公共安全领域的应用中，安全性要求很高。

### 5.3.1　无线传感器网络概述

#### 1. 无线传感器网络的定义

无线传感器网络是大量的静止或移动的传感器以自组织和多跳的方式构成的网络，其目的是协作地感知、采集、处理和传输网络覆盖地理区域内感知对象的监测信息，并报告给用户。

#### 2. 无线传感器网络基本结构

无线传感器网络的基本结构如图5-11所示，一般包括传感器节点、汇聚节点（或称为基站）和管理节点（用户）。

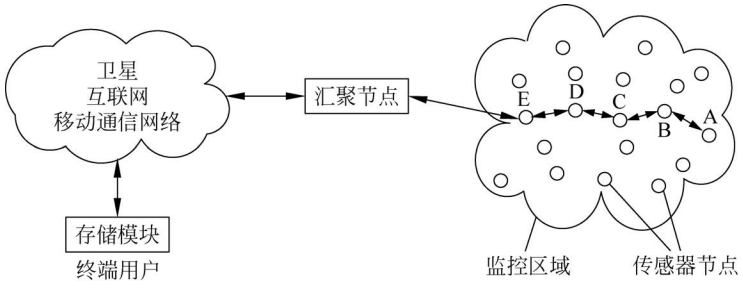



**图5-11　无线传感器网络基本结构**

首先，大量的传感器节点被随机地部署在目标监测区域，通过自组织和多跳的方式构成

网络。传感器节点采集到的监测区域数据沿着其他传感器节点逐条进行传输；在传输过程中，监测区域数据可能被多个节点处理，经过多条路由至汇聚节点，最后通过互联网或卫星到达管理节点。

（1）传感器节点

传感器节点一般由数据采集模块、数据处理与控制模块、通信模块和电源模块四部分组成，如图 5-12 所示。

① 数据采集模块：信息采集、数据转换。

② 数据处理与控制模块：控制、数据处理、网络协议。

③ 通信模块：无线通信，交换控制信息和收发采集数据。

④ 电源模块：提供能量。

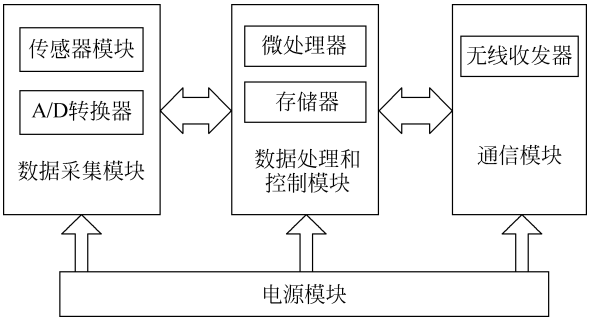



**图 5-12　传感器节点结构**

（2）汇聚节点

汇聚节点既可以是一个具有增强功能的传感器节点，有足够的能量提供给更多的内存与计算资源，也可以是没有监测功能仅带有无线通信接口的特殊网关设备。

**【思考】** 无线传感器网络和物联网的异同？

**3. 无线传感器网络的协议栈**

无线传感器网络协议栈如图 5-13 所示，包括物理层、链路层、网络层、传输层和应用层，与互联网协议栈的五层协议相对应。此外，无线传感器网络协议栈还包括能量管理平台、移动管理平台、任务管理平台和安全管理平台。这些管理平台使得传感器节点能够按照能源高效的方式协同工作，在节点移动的无线传感器网络中转发数据，并支持多任务和资源共享。

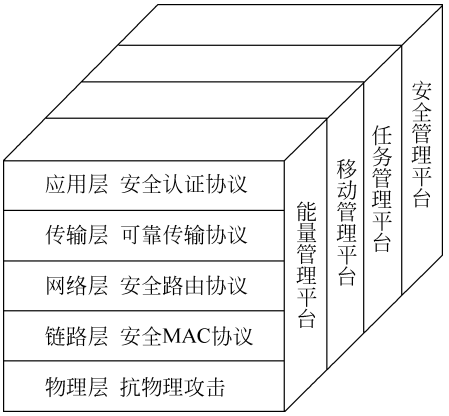



**图 5-13　无线传感器网络协议栈**

（1）物理层

无线传感器网络属于无线通信，无线传感器网络物理层的主要技术包括介质和频段的选择、调制/解调技术和扩频技术。

① 介质和频段选择

无线通信的介质包括电磁波和声波。电磁波是最主要的无线通信介质，而声波一般仅用于水下的无线通信。根据波长的不同，电磁波分为无线电波、微波、红外线和光波等，其中

无线电波在无线网络中使用最广泛。无线电波的传播特性与频率相关。

② 调制和解调技术

调制和解调技术是无线通信系统的关键技术之一。通常信号源的编码信息(即信源)含有直流分量和频率较低的频率分量,称为基带信号。基带信号往往不能作为传输信号,因而要将基带信号转换为相对基带频率而言频率非常高的带通信号,以便于进行信道传输。通常将带通信号称为已调信号,而基带信号称为调制信号。

调制技术通过改变高频载波的幅度、相位或频率,使其随着基带信号幅度的变化而变化。解调是将基带信号从载波中提取出来以便预定的接收者(信宿)处理和理解的过程。

根据原始信号所控制参量的不同,调制分为幅度调制(Amplitude Modulation,AM)、频率调制(Frequency Modulation,FM)和相位调制(Phase Modulation,PM)。

③ 扩频技术

扩频又称为扩展频谱,它的定义如下:扩频通信技术是一种信息传输方式,其信号所占有的频带宽度远大于所传信息必需的最小带宽;频带的扩展是通过一个独立的码序列来完成,用编码及调制的方法来实现,与所传信息数据无关;在接收端用同样的码进行相关同步接收、解扩和恢复所传信息数据。

扩频技术按照工作方式的不同,可以分为以下四种:直接序列扩频(Direct Sequence Spread Spectrum,DSSS)、跳频扩频(Frequency Hopping Spread Spectrum,FHSS)、跳时扩频(Time Hopping Spread Spectrum,THSS)和宽带线性调频扩频(Chirp Spread Spectrum,Chirp-SS,简称 Chirp 扩频)。

直接序列扩频:利用高速率的扩频码序列在发射端扩展信号的频谱,而在接收端用相同的扩频码序列进行解扩,把展开的扩频信号还原成原来的信号。

跳频扩频:利用整个带宽(频谱)并将其分割为更小的子通道。发送方和接收方在每个通道上工作一段时间,然后转移到另一个通道。发送方将第一组数据放置在一个频率上,将第二组数据放置在另一个频率上,以此类推。

跳时扩频:是使发射信号在时间轴上跳变。首先把时间轴分成许多时片。在一个帧内哪个时片发射信号由扩频码序列进行控制。可以把跳时理解为:用一定码序列进行选择的多时片的时移键控。

宽带线性调频扩频:如果发射的射频脉冲信号在一个周期内,其载频的频率作线性变化,则称为线性调频。

(2) 链路层

无线传感器网络链路层主要负责多路数据流、数据结构探测、媒体访问和误差控制,从而确保通信网络中可靠的点-点与点-多点连接。然而,无线传感器网络节点协同工作与面向应用的性质,以及无线传感器网络节点的物理约束(如能量和处理能力约束)决定了完成这些功能的方式。

多跳自组织无线传感器网络 MAC 层协议需要实现两个目标:①基于感知区域内密集布置节点的无线多跳通信,需要建立数据通信连接以获得基本的网络基础设施。②为了使无线传感器网络节点公平有效地共享通信资源,需要对共享媒体的访问进行管理。无线传感器网络的 MAC 协议必须具有固定能量保护、移动性管理和失效恢复策略。

考虑现有的 MAC 层协议的解决方案,主要包含以下几种访问方式:

① 基于网络时分多址(Time Division Multiple Access,TDMA)的媒体访问。

② 基于混合 TDMA/FDMA 的媒体访问,FDMA 为频分多址(Frequency Division Multiple Access)。

③ 基于载波监听(Carrier Sense Multiple Access with Collision detection,CSMA)媒体访问技术。一般基于自动重发请求(Automatic Repeat reQuest,ARQ)的误差控制,主要采用重新传送恢复丢失的数据包/帧。虽然其他无线网络的数据链路层利用了基于 ARQ 的误差控制方案,但由于无线传感器网络节点能量与处理资源的不足,无线传感器网络应用中 ARQ 的有效性受到了限制。另外,前向纠错(Forward Error Correction,FEC)方案具有固有的解码复杂性,需要无线传感器网络节点消耗大量处理资源。因此,具有低复杂度编码与解码方式的简单误差控制码可能是无线传感器网络中误差控制的最佳解决方案。

(3) 网络层

网络层负责对传输层提供的数据进行最优路由。大量的传感器节点散布在无线传感器网络的监测区域中,因此需要设计一套最优的路由协议(能量最高效、路径最短、时延最小、可靠性最好等)来供采集数据的传感器节点和汇聚节点之间的通信使用。

(4) 传输层

传输层用于维护无线传感器网络中的数据流,是保证通信服务质量的重要部分。当无线传感器网络需要与其他类型的网络连接时,例如,汇聚节点与任务管理节点之间的连接就可以采用传统的 TCP 或者用户数据协议(User Datagram Protocol,UDP)协议。但是在无线传感器网络的内部是不能采用这些传统协议的,这是因为传感器节点的能源和内存资源都非常有限,它需要一套代价较小的协议。

(5) 应用层

根据应用的具体要求的不同,不同的应用程序可以添加到应用层中,它包括一系列基于监测任务的应用软件。

管理平台包括能量管理平台、移动管理平台和任务管理平台。这些管理平台用来监控无线传感器网络中能量的利用、节点的移动和任务的管理。它们可以帮助传感器节点在较低能耗的前提下协作完成某些监测的任务。能量管理平台可以管理一个节点怎样使用它的能量。例如,一个节点接收到一个邻近节点发送过来的消息之后,就把自己的接收器关闭,避免收到重复的数据。同样,一个节点的能量太低时,它会向周围节点发送一条广播消息,以表示自己已经没有足够的能量来转发数据,这样它就可以不再接收邻居节点发送过来的需要转发的消息,进而把剩余能量留给自身消息的发送。移动管理平台能够记录节点的移动。任务管理平台用来平衡和规划某个监测区域的感知任务,因为并不是所有节点都要参与到监测活动中,在有些情况下,剩余能量较高的节点要承担多一点的感知任务,这时需要任务管理平台负责分配与协调各个节点任务量的大小,有了这些管理平台的帮助,节点可以以较低的能耗进行工作,可以利用移动的节点来转发数据,可以在节点之间共享资源。

**4. 无线传感器网络的应用**

无线传感器网络具有众多不同类型的传感器,可以探测包括地震、电磁、温度、湿度、噪声、光强度、压力、土壤成分、移动物体的大小、速度和方向等周边环境中多种多样的物理量和化学量。基于微机电系统(Micro Electromechanical System,MEMS)的微传感技术和无

线网络技术，为无线传感器网络赋予了广阔的应用前景。这些潜在的应用领域可以归纳为：军事、航空、反恐、防爆、救灾、环境、医疗、保健、家居、工业、商业等领域。典型的军事应用如下。

(1) 智能微尘

“智能微尘”是一个由具有计算能力的低成本、低功耗(相当于手机使用功率的 1/1000)的超微型传感器(一些传感器只有阿司匹林药片那么大，但绝大部分传感器的体积相当于一个传呼机)所组成的网络，该网络可以监测周边环境的温度、光亮度和振动程度，它甚至还可以察觉到周围是否存在辐射或有毒的化学物质。“智能微尘”使用微电子机械系统技术设计，能够通过飞机散播到敌方公路、阵地上。以电池驱动的“智能微尘”能够感应到敌方的活动，并能够把得到的信息传送回总部，用于侦察附近敌方部队的活动。智能微尘示意图和实物图如图 5-14 所示。

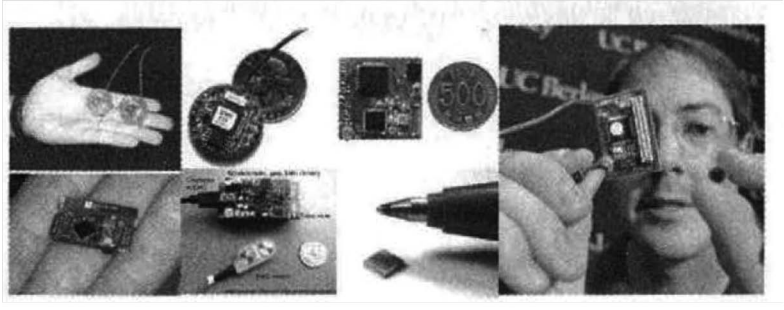


**图 5-14　智能微尘示意图和实物图**

(2) “热带树”和“远程战场监视传感器系统”

通过在敌方阵地附近的道路、桥梁、港口等关键地区部署各种类型的传感器，可以了解敌方动向，以及武器装备的部署情况。分布式传感器在军事领域的应用已有几十年的历史。早在越南战争期间，美军就使用了当时被称为“热带树”的无人值守无线传感器网络来对付北越的“胡志明小道”，如图 5-15 所示。“热带树”在越战中的成功应用，促使许多国家战后纷纷研制和装备各种无人值守的地面传感器系统(Unattended Ground Sensors，UGS)。美军的远程战场监视传感器

**图 5-15　胡志明小道**

系统(Remotely Monitories Battle Area Sensors System,REMBASS)项目已经为 UGS 的成功使用进行了验证。REMBASS 使用了远距离监视传感器。由人工放置在敌人可能经过的道路,这些传感器可以对敌人的活动引起的信号作出响应,记录诸如地面震动、声音、红外和磁场变化等物理量。

(3) 无人值守地面传感器群

"无人值守地面传感器群"项目由美国陆军于 2001 年提出,其主要目标是使基层部队指挥员具有在他们所希望部署传感器的任何地方灵活地部署传感器的能力,并且能详尽地收集战场各种精确信息,比如丛林地带的地面坚硬度和干湿度,为更准确地制定战斗行动方案提供情报依据。部署的方式依赖于需要执行的任务,指挥员可以将三种传感器进行最适宜的组合来满足任务需求。无人值守地面传感器作为美军未来战斗系统的一部分,主要分为战术 UGS 和城区 UGS 两种类型。战术 UGS 主要包括情报侦察监视 UGS 和化学、生物、辐射和核 UGS; 城区 UGS 也称为城市地形军事行动先进传感器系统,用于城区环境下的态势感知和部队保护,以及在城市地形军事行动环境中对已清理区域内滞留部队的保护。

(4) 传感器组网系统

"传感器组网系统"项目由洛克希德·马丁公司开发。传感器组网系统可以实现传感器工作自动化,同时通过管理和协调不同传感器,可在动态环境下获得、综合并生成高质量的数据。传感器组网系统的核心是一套实时数据库管理系统。该系统可以利用现有的通信机制对从战术级到战略级的传感器信息进行管理,而管理工作只需通过一台专用的商用便携机即可完成,不需要其他专用设备,该系统以现有的带宽进行通信,并可协调来自地面和空中的监视传感器以及太空监视设备的信息,并且该系统可以部署到各级指挥单位。

(5) 沙地直线

在美国国防高级研究计划局的资助下,美国俄亥俄州开展了"沙地直线"项目开发,这是一种无线传感器网络系统,能够散射"电子绊网"到整个战场以侦测运动的高金属含量目标,这种能力意味着一个特殊的军事用途,如侦察和定位敌军坦克和其他车辆。在"沙地直线"项目的基础上,美军进一步进行了超大规模无线传感器网络的研究。美军在 2004 年 12 月进行了史上最大规模的无线传感器网络试验。在名为"ExScal"的网络中 1300m×300m 的地域内部署了 1200 个网络节点,成功检验了网络稳定性、网络冗余配置等方面的研究成果。

(6) 目标定位网络嵌入式系统

目标定位网络嵌入式系统技术是美国国防高级研究计划局主导的一个战场应用实验项目,它将实现系统和信息处理的融合。项目短期目标是建立包括 10～100 万个计算节点的可靠、实时、分布式应用网络。这些节点包括连接传感器和控制器的物理和信息系统部件。基础嵌入式系统技术节点采用现场可编程门阵列(Field Programmable Gate Array,FPGA)模式。该项目应用了大量的微型传感器、微电子、先进传感器融合算法、自定位技术和信息技术方面的成果。该项目的长期目标是实现传感器信息的网络中心分布和融合,显著提高作战态势感知能力。该项目成功验证了无线传感器网络技术能够准确定位敌方狙击手,它采用多个廉价音频传感器来协同定位敌方射手并标示在所有参战人员的个人计算机中,三维空间的定位精度可达到 1.5m,定位延迟仅为 2s,甚至能显示出敌方射手采用跪姿和站姿射击的差异。

(7) 全资产可视化系统

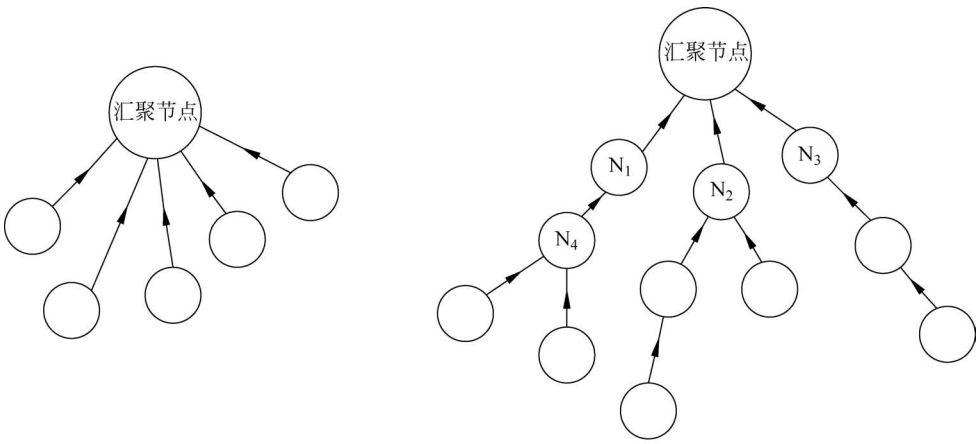
利用无线传感器网络对军事装备、弹药等物资进行管理与调配,实现物资管理的"可视

化”，从而可以在战场瞬息万变的情况下缩短供应时间，提高战场保障效率。比如，在油库安装无线传感器网络节点设备，对油料进行监控，当油料缺少时报告系统油库缺油，然后由工作人员及时补充油料，此举可以大大减少人力的支出，缩短了时间。在伊拉克战争期间，美军在后勤保障上应用了大量无线传感器网络，战争结束后，美军军方进行数据统计，发现未使用无线传感器网络的物资调配要比使用无线传感器网络的物资调配多浪费30%人力和25%的时间。因此美军反思了后勤保障体系的缺陷，提出了全资产可视性计划，命名为全资产可视化(Total Asset Visibility，TAV)系统。全资产可视化系统是基于信息化作战的需要，通过构建军队资产信息网络系统，为军队各级指挥员和资产使用管理人员(用户)及时准确地提供全部资产的有关位置、运动和状况的全面信息，以及识别部件、人员、装备和补给品的管理能力。该系统是随着信息化和高科技战争后勤保障对资产管理提出的新需求而阐释的一种新概念。依托该系统，美军可以在几秒内计算出数月内后勤保障的准确情况，包括物资的消耗状况以及后勤保障需求。该系统不仅可以对后勤资源实施全面监控，还能对部队机动、军事交通运输、伤员后送等保障活动进行全程动态跟踪。

### 5.3.2　无线传感器网络特点

#### 1. 多跳路由

由于传感器节点的无线传输范围有限，两个无法直接通信的节点往往会通过多个中间节点的转发来实现通信。传感器节点需要传输的数据从一个节点跳到另一个节点，直到抵达目的节点。图5-16给出了直接传输模式和多跳传输模式的示意图。




(a) 直接传输模式　　(b) 多跳传输模式

**图5-16　传感器节点多跳**

#### 2. 每个节点兼具路由器和主机两种功能

(1) 作为主机，节点需要运行面向用户的应用程序；

(2) 作为路由器，节点需要运行相应的路由协议，根据路由策略参与分组转发和路由维护工作。

#### 3. 网络拓扑结构动态变化

由于传感器节点容易失效、无线信道的相互干扰、节点发送功率的变化、地形对无线信

号的影响等各种因素的影响，无线传感器网络的拓扑结构随时可能产生变化，因此无线传感器网络的拓扑结构具有动态变化性。

**4. 分布式控制方式**

无线传感器网络没有专门的控制中心，它把网络的控制功能分散配置到各节点，网络的建立和调整是通过各节点的有机配合实现的。各节点没有重要和次要之分，所有节点地位平等，是一个对等式网络，能防止一旦控制中心被破坏而引起全网瘫痪的危险，提高了网络的抗毁性。

**5. 使用广播式信道**

由于无线传感器网络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，冲突的存在会导致信号传输失败，信道利用率降低。在密集型的无线传感器网络中，这是个尤为重要的问题。

**6. 节点数量较大**

由于无线传感器网络通常需要覆盖很广泛的地理区域，单个节点的通信范围有限，为获取监测目标的精确信息，节点的部署比较密集，因此，无线传感器网络中的节点数量巨大，可以达到成千上万，甚至更多。

### 5.3.3 无线传感器网络安全需求

在传统信息安全需求的基础上，无线传感器网络又具有一些特殊的安全需求。

**1. 机密性**

无线通信是开放的，无法确定网络中是否存在窃听行为，这就要求即使信号被攻击者截获，也能保证攻击者无法分析出所截获信息的内容，确保信息的机密性。

**2. 完整性**

机密性确保了在数据传输过程中，攻击者无法获取真实的信息内容，但是不能确保接收者收到的数据是正确的，因为恶意的中间节点可以截获、篡改和干扰信息的传输，完整性则可以确保发出的和收到的消息是完全一致的。

**3. 新鲜性**

数据是具有时效性的，传感器节点必须确保发出的和收到的信息都是当前最新的数据，杜绝接收重复的信息，以确保数据的新鲜性，防止重复攻击。

**4. 可用性**

无线传感器网络的可用性是指当无线传感器网络被攻击者伪造的信号干扰而处于部分或全部瘫痪状态时，还能够按照原有的工作方式向合法用户提供信息访问服务。

**5. 鲁棒性**

无线传感器网络是动态的，节点的失效或新添加、环境因素、人为破坏、自然灾害等，都会导致网络拓扑的变化，鲁棒性可使无线传感器网络受到的影响最小化，不会使整个网络瘫痪。

**6. 访问控制**

访问控制是指网络能够认证访问者身份的合法性。传感器节点因物理访问而无法使用

防火墙；类似非对称密码体制的数字签名和公钥证书等传统网络方法受资源限制，也无法使用防火墙。

### 5.3.4　无线传感器网络安全脆弱性

**1. 分布的开放性**

传感器节点必须分布于待感知的事件的周围，一般是部署在恶劣的环境、无人区域或敌方阵地，无人值守或监管，容易被物理地直接访问，并因成本因素一般不具备防拆装的能力，安全无法保证，节点易失效。例如我国渔民屡屡打捞到外国的海洋探测装置。

**2. 网络的动态性**

网络的动态性包含两层含义：一是网络规模的变化，节点数量增减是常态。二是网络拓扑结构动态变化。无线传感器网络节点随机部署在目标区域，一般具有大量而密集的节点分布特征，因缺少固定基础设施，没有中心管理点，各节点是否存在直接连接，连接又能维持多久均是未知的。因此，网络规模可变化，节点增减是常态，拓扑结构动态性强。

**3. 资源的有限性**

由于受到应用和成本的限制，传感器节点的硬件资源极其有限，而这种硬件资源的有限性决定了无线传感器网络存在着以下几方面的限制，表 5-3 给出了相关单片机的资源分配图。

(1) 能量有限。能量是限制传感器节点能力、寿命最主要的约束性条件，现有的传感器节点一般都是通过电池供电，为了减小体积，电池一般采用纽扣电池，电池容量十分有限，且传感器的使用环境决定了传感器基本不可能重新充电。这就决定了无线传感器网络的首要设计目标是能源的高效利用，这也是传感器网络和传统网络最重要的区别之一。

(2) 计算能力有限。传感器节点的 CPU 一般只具有 8bit～8MHz 的处理能力。这种有限的处理能力决定了传感器节点基本不可能进行复杂的计算。因此，轻量级的密码算法是无线传感器网络的一个重要研究方向。

(3) 存储能力有限。传感器节点一般包括三种形式的存储器：RAM、程序存储器、工作存储器。RAM 用于存放工作时的临时数据，一般不超过 2KB；程序存储器用于存储操作系统、应用程序以及安全函数等；工作存储器用于存放获取的传感器信息，这两种存储器一般也只有几十 KB。

(4) 通信能力有限。为了节约信号传输时的能量消耗，传感器节点收发模块的传输功率一般为 10～100mW，传输的范围也局限于 100m～1km。

(5) 安全性有限。传感器节点一般布置在敌对或者无人看管的区域，传感器节点的物理安全没有很多保证，攻击者很容易攻占节点，且节点没有防篡改的安全部件，攻击者一旦获取传感器节点就很容易获得和修改存储在传感器节点中的密钥信息以及程序代码等。由于信道的脆弱性和广播特性，攻击者不需要物理基础网络部件，恶意攻击者可以轻易地进行网络监听和发送伪造的数据报文。

**4. 通信的不可靠性**

无线传感器网络采用无线通信方式。无线通信的广播属性，因缺少基础设施和难以控制的通信环境，往往表现出通信的开放性和不可靠性，为敌方实施攻击提供了便利，主要包括监听无线信道、窃听通信数据、篡改传感器节点内容等。

表 5-3　相关单片机的资源分配

| 型号<br>STC8 系列是 STC 价格最低/功耗最低/速度最快的 8051 单片机<br>绝大部分指令 1 个时钟完成 | 工作电压（V） | Flash 程序存储器 10 万次 字节 | 内部大容量扩展 SRAM 字节 | 强大的双 DPTR 可增可减 | EEPROM 10 万次 字节 | I/O 口 最多数量 | 串行口 可掉电唤醒 | SPI | $I^2C$ | 定时器/计数器（T0-T4 外部管脚也可掉电唤醒） | RTC 实时时钟 万年历 | 16 位高级 PWM 定时器 互补对称死区 | 45 路 15 位增强 PWM 满足舞台灯光控制要求 | 传统 PCA/CCP/PWM 定时器 当部断可电醒 可外中并掉唤 | 掉电唤醒专用定时器 | 触摸按键 LED 直接驱动自动扫描显示 | ADC 高速 15 路 测池压作压道 专电电工电通 PWM 可当 D/A 使用 | 比较器 也可作外部掉电检测 | 内部低压检测供电电压 复位/中断/查询 | 看门狗 复位定时器 | 内部高可靠复位 可选复位门槛电压 | 内部高精准时钟 36MHz 以下可调 追频 | 可对外输出时钟及复位 | 程序加密后传输让您的客户自己升级程序 | 可设置下次更新程序需口令 | 支持 RS485 下载 | 支持 USB 下载 硬件或软件模拟 | 全速 USB | MDU16 硬件 16 位乘除法器单元 | 本身就可在线仿真 | 主力产品供货信息<br>部分封装<br>LQFP64 QFN64〈8×8mm〉<br>LQFP48 QFN48〈6×6mm〉<br>LQFP44 用 LQFP48 取代 LQFP44<br>LQFP32 QFN32〈4×4mm〉<br>TSSOP20 QFN20〈3×3mm〉<br>SOP16 用 TSSOP20 取代 SOP16<br>SOP8 DFN8〈3×3mm 优先推荐〉 | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | LQFP64 | QFN64 | LQFP48 | QFN48 | LQFP44 | LQFP32 | QFN32 | TSSOP20 | QFN20 | SOP16 | SOP8 | DFN8 | |
| STC8G1K08 | 1.9-5.5 | 8K | 1K | 2 | 4K | 6 | 1 | 有 | 有 | 2 | - | - | - | - | 有 | - | - | - | 有 | 有 | 4 级 | 有 | 是 | 有 | 是 | 是 | 软 | - | 有 | 是 | | | | | | | | | | 0.65 | 0.7 | 现货 |
| STC8G1K17 | 1.9-5.5 | 17K | 1K | 2 | IAP | 6 | 1 | 有 | 有 | 2 | - | - | - | - | 有 | - | - | - | 有 | 有 | 4 级 | 有 | 是 | 有 | 是 | 是 | - | - | 有 | - | | | | | | | | | | 0.75 | 0.8 | 现货 |
| STC8G1K08A | 1.9-5.5 | 8K | 1K | 2 | 4K | 6 | 1 | 有 | 有 | 2 | - | - | - | 3 | 有 | - | 10 位 | - | 有 | 有 | 4 级 | 有 | 是 | 有 | 是 | 是 | 软 | - | 有 | 是 | | | | | | | | | | 0.75 | 0.8 | 现货 |
| STC8G1K17A | 1.9-5.5 | 17K | 1K | 2 | IAP | 6 | 1 | 有 | 有 | 2 | - | - | - | 3 | 有 | - | 10 位 | - | 有 | 有 | 4 级 | 有 | 是 | 有 | 是 | 是 | - | - | 有 | - | | | | | | | | | | 0.85 | 0.9 | 现货 |
| STC8G1K08 | 1.9-5.5 | 8K | 1K | 2 | 4K | 18 | 2 | 有 | 有 | 3 | - | - | - | 3 | 有 | - | 10 位 | 有 | 有 | 有 | 4 级 | 有 | 是 | 有 | 是 | 是 | 软 | - | - | 是 | | | | | | | 1.15 | 1.20 | 1.30 | | | 现货 |
| STC8G1K17 | 1.9-5.5 | 17K | 1K | 2 | IAP | 18 | 2 | 有 | 有 | 3 | - | - | - | 3 | 有 | - | 10 位 | 有 | 有 | 有 | 4 级 | 有 | 是 | 有 | 是 | 是 | - | - | - | - | | | | | | | 1.30 | 1.35 | 1.40 | | | 现货 |
| STC8G2K16S2 | 1.9-5.5 | 16K | 2K | 2 | 48K | 45 | 2 | 有 | 有 | 5 | - | - | 8 | 3 | 有 | - | 10 位 | 有 | 有 | 有 | 4 级 | 有 | 是 | 有 | 是 | 是 | 软 | - | 有 | 是 | | | ¥1.6 | ¥1.8 | | | | | | | | 现货 |
| STC8G2K32S2 | 1.9-5.5 | 32K | 2K | 2 | 32K | 45 | 2 | 有 | 有 | 5 | - | - | 8 | 3 | 有 | - | 10 位 | 有 | 有 | 有 | 4 级 | 有 | 是 | 有 | 是 | 是 | 软 | - | 有 | 是 | | | ¥1.8 | ¥2.0 | | | | | | | | |
| STC8G2K32S4 | 1.9-5.5 | 32K | 2K | 2 | 32K | 45 | 4 | 有 | 有 | 5 | - | - | 45 | 3 | 有 | - | 10 位 | 有 | 有 | 有 | 4 级 | 有 | 是 | 有 | 是 | 是 | 软 | - | 有 | 是 | | | ¥2.0 | ¥2.2 | | ¥2.0 | | | | | | |

续表

| 型号<br>STC8系列是STC价格最低/功耗最低/速度最快的8051单片机<br>绝大部分个指令1个时钟完成 | 工作电压（V） | Flash程序存储器 10万次 字节 | 内部大容量扩展SRAM 字节 | 强大的双DPTR可增可减 | EEPROM 10万次 字节 | I/O口 最多数量 | 串行口 可掉电唤醒 | SPI | $I^2C$ | 定时器/计数器（T0-T4外部管脚也可掉电唤醒） | RTC 实时时钟 万年历 | 16位高级PWM定时器 互补对称死区 | 45路15位增强PWM满足舞台灯光控制要求 | 传统PCA/CCP/PWM定时器 当部断可电醒 可外中并掉唤 | 掉电唤醒专用定时器 | 触摸按键 LED直接驱动自动扫描显示 | ADC高速路15 测池压作压道 专电电工电通 PWM可当D/A使用 | 比较器 也可作外部掉电检测 | 内部低压检测供电电压 复位/中断/查询 | 看门狗 复位定时器 | 内部高可靠复位 可选复位门槛电压 | 内部高精准时钟 36MHz以下可调 追频 | 可对外输出时钟及复位 | 程序加密后传输让您的客户自己升级程序 | 可设置下次更新程序需口令 | 支持RS485下载 | 支持USB下载 硬件或软件模拟 | 全速USB | MDU16 硬件16位乘除法器单元 | 本身就可在线仿真 | 主力产品供货信息<br>部分封装<br>LQFP64 QFN64〈8×8mm〉<br>LQFP48 QFN48〈6×6mm〉<br>LQFP44 用LQFP48取代LQFP44<br>LQFP32 QFN32〈4×4mm〉<br>TSSOP20 QFN20〈3×3mm〉<br>SOP16 用TSSOP20取代SOP16<br>SOP8 DFN8〈3×3mm优先推荐〉<br>LQFP64 | LQFP64 | QFN64 | LQFP48 | QFN48 | LQFP44 | LQFP32 | QFN32 | TSSOP20 | QFN20 | SOP16 | SOP8 | DFN8 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| STC8G2K60S4 | 1.9-5.5 | 60K | 2K | 2 | 4K | 45 | 4 | 有 | 有 | 5 | - | - | 45 | 3 | 有 | - | 10位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | 软 | - | 有 | 是 | | | ¥2.2 | ¥2.4 | | ¥2.2 | | | | | | 现货 |
| STC8G2K64S4 | 1.9-5.5 | 64K | 2K | 2 | IAP | 45 | 4 | 有 | 有 | 5 | - | - | 45 | 3 | 有 | - | 10位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | 软 | - | 有 | 是 | | | ¥2.2 | ¥2.4 | | ¥2.2 | | | | | | |
| STC8H1K08 | 1.9-5.5 | 8K | 1K | 2 | 4K | 17 | 2 | 有 | 有 | 3 | - | 8 | - | - | 有 | - | 10位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | 软 | - | - | 是 | | | | | | | 0.90 | 0.95 | | | | |
| STC8H1K17 | 1.9-5.5 | 17K | 1K | 2 | IAP | 17 | 2 | 有 | 有 | 3 | - | 8 | - | - | 有 | - | 10位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | - | - | - | - | | | | | | | 1.15 | 1.20 | | | | |
| STC8H1K16 | 1.9-5.5 | 16K | 1K | 2 | 12K | 29 | 2 | 有 | 有 | 5 | - | 8 | - | - | 有 | - | 10位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | 软 | - | - | 是 | | | | | ¥1.4 | ¥1.4 | | | | | | |
| STC8H1K24 | 1.9-5.5 | 24K | 1K | 2 | 4K | 29 | 2 | 有 | 有 | 5 | - | 8 | - | - | 有 | - | 10位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | 软 | - | - | 是 | | | | | ¥1.5 | ¥1.5 | | | | | | |
| STC8H1K28 | 1.9-5.5 | 28K | 1K | 2 | IAP | 29 | 2 | 有 | 有 | 5 | - | 8 | - | - | 有 | - | 10位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | 软 | - | - | 是 | | | | | ¥1.6 | ¥1.6 | | | | | | |

续表

| 型号<br>STC8系列是STC最低价格/最低功耗/最快速度8051单片机<br>绝大部分指令1个时钟完成 | 工作电压（V） | Flash程序存储器 10万次 字节 | 内部大容量扩展SRAM 字节 | 强大的双DPTR可增可减 | EEPROM 10万次 字节 | I/O口 最多数量 | 串行口 可掉电唤醒 | SPI | $I^2C$ | 定时器/计数器（T0-T4外部管脚也可掉电唤醒） | RTC 实时时钟 万年历 | 16位高级PWM定时器 互补对称死区 | 45路15位增强PWM满足舞台灯光控制要求 | 传统PCA/CCP/PWM定时器 当部断可电醒 可外中并掉唤 | 掉电唤醒专用定时器 | 触摸按键 LED直接驱动自动扫描显示 | ADC高速15路 测池压作压道 专电电工电通 PWM可当D/A使用 | 比较器 也可作外部掉电检测 | 内部低压检测供电电压 复位/中断/查询 | 看门狗 复位定时器 | 内部高可靠复位 可选复位门槛电压 | 内部高精准时钟 36MHz以下可调 追频 | 可对外输出时钟及复位 | 程序加密后传输让您的客户自己升级程序 | 可设置下次更新程序需口令 | 支持RS485下载 | 支持USB下载 硬件或软件模拟 | 全速USB | MDU16 硬件16位乘除法器单元 | 本身就可在线仿真 | 主力产品供货信息<br>部分封装<br>LQFP64 QFN64〈8×8mm〉<br>LQFP48 QFN48〈6×6mm〉<br>LQFP44 用LQFP48取代LQFP44<br>LQFP32 QFN32〈4×4mm〉<br>TSSOP20 QFN20〈3×3mm〉<br>SOP16 用TSSOP20取代SOP16<br>SOP8 DFN8〈3×3mm优先推荐〉 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | LQFP64 | QFN64 | LQFP48 | QFN48 | LQFP44 | LQFP32 | QFN32 | TSSOP20 | QFN20 | SOP16 | SOP8 | DFN8 | |
| STC8H8K32U | 1.9-5.5 | 32K | 8K | 2 | 32K | 60 | 4 | 有 | 有 | 5 | - | 8 | - | - | 有 | - | 12位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 硬 | 有 | 有 | 是 | ￥2.9 | ￥3.1 | ￥2.4 | | | | | | | | | | 送样中 |
| STC8H8K64U | 1.9-5.5 | 64K | 8K | 2 | IAP | 60 | 4 | 有 | 有 | 5 | - | 8 | - | - | 有 | - | 12位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 硬 | 有 | 有 | 是 | ￥3.4 | ￥3.6 | ￥2.9 | | | | | | | | | | |
| STC8H3K32S4 | 1.9-5.5 | 32K | 3K | 2 | 32K | 43 | 4 | 有 | 有 | 5 | - | 8 | - | - | 有 | - | 12位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 软 | - | 有 | 是 | | | ￥2.2 | ￥2.4 | | | | | | | | | |
| STC8H3K64S4 | 1.9-5.5 | 64K | 3K | 2 | IAP | 43 | 4 | 有 | 有 | 5 | - | 8 | - | - | 有 | - | 12位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 软 | - | 有 | 是 | | | ￥2.4 | ￥2.6 | | | | | | | | | |
| STC8G1K08T | 1.9-5.5 | 8K | 1K | 2 | 4K | 16 | 1 | 有 | 有 | 3 | - | - | - | 3 | 有 | 16 | 10位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 软 | - | - | 是 | | | | | | | 1.40 | | | | | 内部测试中 |
| STC8G1K17T | 1.9-5.5 | 17K | 1K | 2 | IAP | 16 | 1 | 有 | 有 | 3 | - | - | - | 3 | 有 | 16 | 10位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | - | - | - | | | | | | | 1.50 | | | | | |
| STC8H2K32T | 1.9-5.5 | 32K | 2K | 2 | 32K | 44 | 4 | 有 | 有 | 5 | 有 | 8 | - | - | 有 | 16 | 12位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | 软 | - | 有 | 是 | | ￥2.7 | ￥2.9 | | | | | | | | | |
| STC8H2K64T | 1.9-5.5 | 64K | 2K | 2 | IAP | 44 | 4 | 有 | 有 | 5 | 有 | 8 | - | - | 有 | 16 | 12位 | 有 | 有 | 有 | 4级 | 有 | 是 | 有 | 是 | 是 | 软 | - | 有 | 是 | | ￥2.9 | | | | | | | | | | |

在一个无线传感器网络中，可能有成百上千个传感器节点协同工作，而同时可以有几十个或上百个传感器在发送数据包，因此容易导致数据通信冲突或延迟。且无线传感器网络传输一位消息和执行 8000～10 000 条指令所消耗的能量相当。为提高无线传感器网络的存活性，一般采用低速率、低功耗的无线通信技术以节约能量开销，这使得无线传感器网络的通信范围、通信带宽十分有限，容易面临干扰、丢包、碰撞、延迟等一系列通信不可靠问题。

**5. 标准的不统一性**

虽然无线传感器网络有 IEEE 802.15.4、IEEE 802.15.4C、ZigBee 及 IEEE 1451 等相关标准，但没有形成统一的无线传感器网络通信标准，导致产品的互操作性和易用性较差。路由协议、节点行为管理、密钥管理技术不实用，导致无线传感器网络难以大规模使用。

无线传感器网络的上述特点和安全脆弱性，给其安全问题研究带来了困难。目前无线传感器网络的安全性不强，其安全方面表现出“易攻难守”的特点，很多问题有待于进一步地研究和解决。

**【思考】**

为什么说物联网感知层具有易攻难守的特点？你是否联想到了“弱国无外交”“落后就要挨打”？如何规避风险？这对你的人生成长有何启迪？

### 5.3.5　无线传感器网络安全攻击和防御

目前，无线传感器网络可能受到的攻击手段和防御方法如表 5-4 所示。本节将逐一介绍。

**表 5-4　无线传感器网络遭受的攻击手段和防御方法**

| 网络层次 | 攻 击 手 段 | 防 御 方 法 |
|---|---|---|
| 物理层 | 阻塞攻击 | 扩频通信、休眠策略 |
| | 物理破坏 | 增加物理损害感知机制，对敏感信息在合适存储区进行加密存储 |
| | 假冒攻击 | 数字签名，公钥基础设施 |
| 链路层 | 耗尽攻击 | 限制网络发送速度；对过度频繁的请求不予理睬；<br>限制同一个数据包的重传次数等 |
| | 非公平竞争攻击 | 使用短包策略和非优先级策略 |
| | 碰撞攻击 | 纠错编码技术、信道监听和重传机制 |
| | 确认欺骗攻击 | 不完全数据链路层确认消息的路由算法 |
| 网络层 | 汇聚节点攻击 | 加强路由信息的安全级别；<br>增加对汇聚节点地理位置信息的加密强度；<br>增加汇聚节点的冗余度和灵活多样选择机制 |
| | 伪造路由攻击 | 对路由信息加签名、加计数值或加时间戳 |
| | 黑洞攻击 | 认证、多径路由、采用基于地理位置的路由协议 |
| | 怠慢和贪婪攻击 | 身份认证、冗余路径 |
| | 女巫攻击 | 身份认证、资源探测法 |
| | 虫洞攻击 | 安全等级策略、采用基于地理位置的路由协议 |
| | 方向误导攻击 | 出口过滤、认证、监测机制 |
| | 流量分析攻击 | “迷惑”攻击者 |

续表

| 网络层次 | 攻击手段 | 防御方法 |
|---|---|---|
| 传输层 | 异步攻击 | 身份认证 |
| | 泛洪攻击 | 客户端谜题、入侵检测机制 |
| | Hello 泛洪攻击 | 认证 |
| 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 |
| | 节点不合作 | 信任管理、入侵检测 |

**1. 物理层攻击**

物理层协议负责频率选择、载波频率产生、信号探测、调制和数据加密。无线传感器网络使用基于无线电的介质，所以容易发生干扰攻击，而且节点往往部署在不安全的地区，节点的物理安全得不到充分保障，因此无线传感器网络在物理层容易遭受如下攻击。

(1) 阻塞攻击

阻塞攻击本质是一种干扰攻击，攻击原理如图 5-17 所示，是利用无线网络的开放性，通过一个强大的干扰源，如扩散的无线电信号，用噪声信号干扰正常节点通信所使用的无线电波频率，达到使无线传感器网络瘫痪的目的。一种典型实施方法：攻击者只需要在节点数为 $N$ 的网络中随机布置 $K(K \gg N)$ 个攻击节点，使它们的干扰范围覆盖全网，就可以使整个无线传感器网络瘫痪。

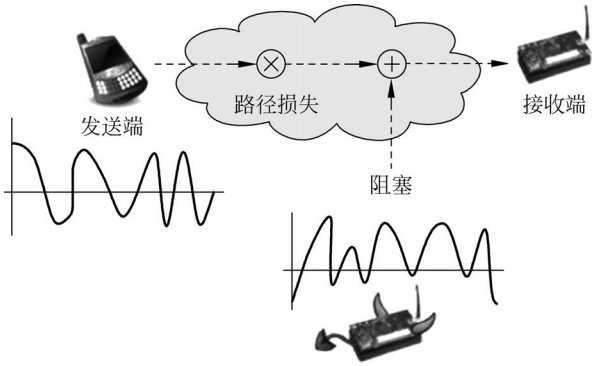



**图 5-17 阻塞攻击示意图**

针对阻塞攻击的常用防御方法有：

① 扩展频谱通信。对于物理层的阻塞攻击可以使用扩频通信技术来防止。扩展频谱通信，简称扩频通信，是一种信息传输方式，其信号所占有的频带宽度远大于所传信息必需的最小带宽，图 5-18 给出了直接序列扩频示意图。图中，(a)表示原始信号。(b)是用待传输的数据信息与伪随机序列异或，用来扩展传输信号的带宽，使其信号功率谱密度下降。(c)表示当扩频后的信号在传输过程中受到噪声干扰，导致信号失真。(d)表示接收端对信号解扩后，噪声功率谱密度下降，信号功率谱密度上升，原始信号将从噪声干扰中恢复处理。可见，原始信号若经过扩频后传输，可以提高其抗噪声能力。

典型的扩频技术码分多址(Code Division Multiple Access，CDMA)是第二次世界大战期间因战争的需要而研究开发的，其初衷是防止敌方对己方通信的干扰，后来由美国高通公司更新成为商用蜂窝电信技术。其原理是将原数据信号的带宽扩展，再经载波调制并发送

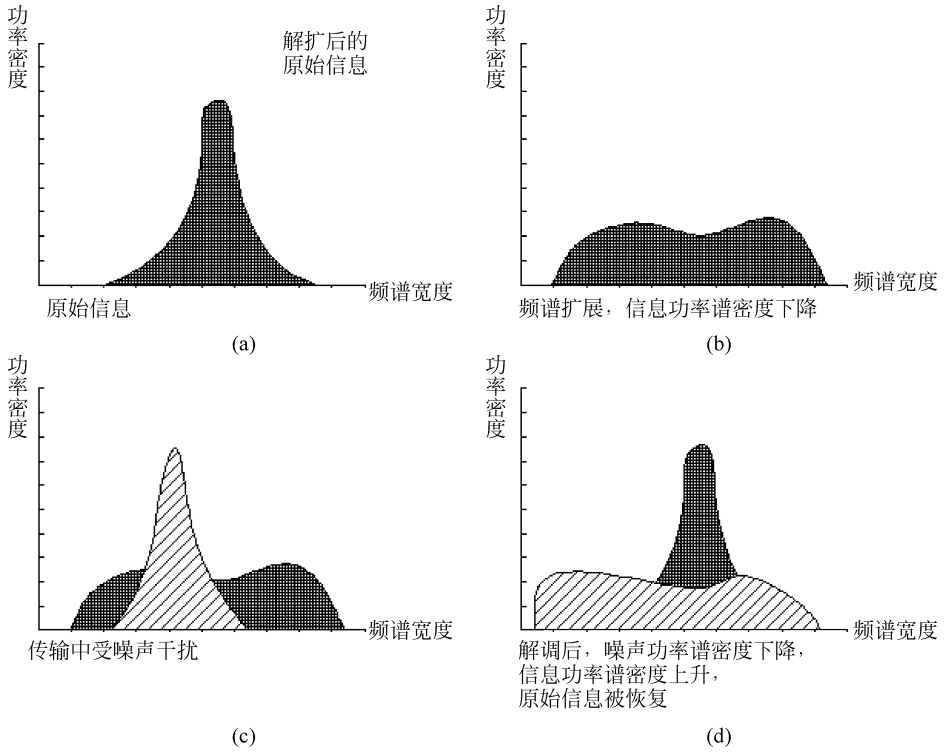



**图 5-18　直接序列扩频通信示意图**

出去。接收端使用完全相同的伪随机码，与接收的带宽信号作相关处理，把宽带信号解扩来实现通信。CDMA 可以在一定程度上实现抗干扰通信，但在资源有限的无线传感器网络中，CDMA 可能会导致较高的通信开销。

② 休眠策略。被攻击节点附近的节点觉察到阻塞攻击之后进入睡眠状态，保持低能耗。然后定期检查阻塞攻击是否已经消失，如果消失则进入活动状态，同时向网络通报阻塞攻击的发生。

此外，上海交通大学科研团队提出一个防御框架，该团队设计的阻塞攻击防御框架结构如图 5-19 所示，主要包括 4 个子模块，分别为攻击者推断模块、频谱分配模块、Client Puzzle 协议产生模块、客户端抵御阻塞模块，其核心思想是：当一个阻塞攻击事件出现时，客户端抵御阻塞模块会将这个事件上报给数据库的攻击者推断模块，而后攻击者推断模块根据频道分配情况更新相关次级用户是攻击者的推测概率。当一个次级用户向数据库查询可用频谱信息时，根据该次级用户的推测概率，数据库使用频谱分配模块分配相应的频谱资源以及使用 Client Puzzle 协议产生模块生成相应难度的 Client Puzzle（对应得到这些频谱资源所需要付出的代价）。当攻击过于严重时，次级用户也可以通过客户端抵御攻击模块，使用一些扩频技术（FHSS/DSSS）来缓解攻击带来的危害。该研究成果于 2016 年发表在网络领域顶级期刊 IEEE JSAC 中。

（2）物理破坏攻击

因为传感器节点往往分布在一个很大的区域内，所以要保证每个节点的物理安全是不现实的，敌人很可能俘获一些节点，对它们进行物理上的分析和修改，如借助相关的仪器仪

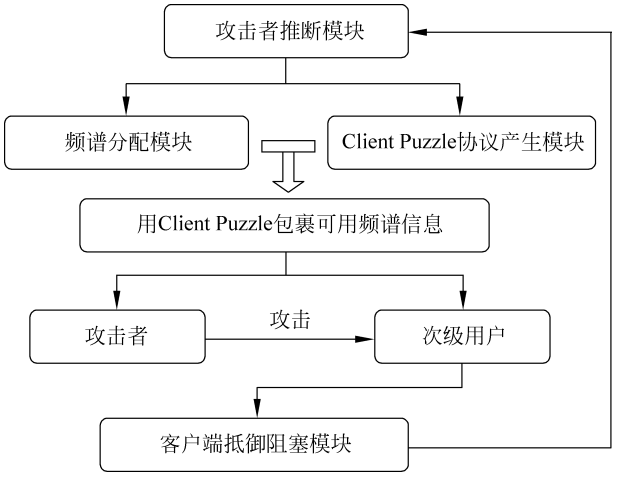



**图 5-19　阻塞攻击防御框架**

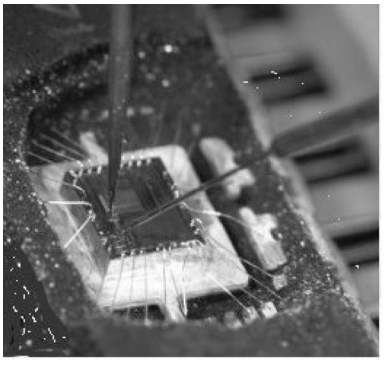


**图 5-20　通过探针物理破坏节点芯片示意图**

表等对节点的物理特征进行窥探(如电压、时钟、能量辐射等),以及对节点进行破坏行为(如对芯片的剖片、物理克隆等),如图 5-20 所示,从而达到获取内部程序或数据的目的,并利用它来干扰网络的正常功能,甚至可以通过分析其内部敏感信息和上层协议机制,破解网络的安全外壳。

针对无法避免的物理破坏,需要无线传感器网络采用更精细的控制保护机制。

① 增加物理损害感知机制。节点能够根据它收发数据包的情况、外部环境变化和一些敏感信号的变化,判断是否遭受物理侵犯。例如,当传感器节点上的位移传感器感知自身位置被移动时,可以把位置变化作为判断它可能遭到物理破坏的一个要素。节点在感知到被破坏以后,可以采取相应的策略,如销毁敏感数据、脱离网络、修改安全处理程序等,这样攻击者就不能正确地分析系统的安全机制,从而保护了网络其他部分的节点免受安全威胁。

② 对敏感信息在恰当存储区加密存储。现代信息安全技术依靠密钥来保护和确认信息,而不是依靠安全算法,所以对通信的加密密钥、认证密钥和各种安全启动密钥需要进行严密的保护。对于攻击者来说,一般读取系统动态内存中的信息比较困难,所以他们通常采用静态分析系统的方法来获取非易失存储器中的内容,因此敏感信息尽量存放在易失存储器上。如果不可避免地要存储在非易失存储器上,则必须首先要进行加密处理。易失存储器和非易失存储器的区别在于:前者在电源关闭时会丢失其储存的内容,而非易失存储器在电源关闭时不会丢失其储存内容。如图 5-21 所示,常用的非易失存储器有硬盘、闪存和各种只读储存器,如可编程只读储存器(Programmable Read Only Memory,PROM)、电可擦可编程只读储存器(Electrically Erasable Programmable Read Only Memory,$E^2$PROM)和可擦可编程只读储存器(Erasable Programmable Read Only Memory,EPROM)等。常用的易失存储器有内存和各类随机存储器,如动态随机存储器(Dynamic Random Access

Memory，DRAM）和静态随机存储器（Static Random Access Memory，SRAM）等。

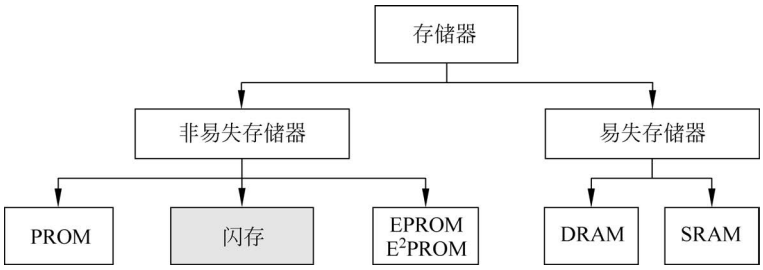



**图 5-21　储存器分类**

（3）假冒攻击

由于攻击者可以捕获节点，所以攻击者可以通过盗取、篡改节点上所保存的任何信息，如用于身份认证的密钥等信息，将恶意节点假冒为合法节点接入网络。要识别出这些“合法”的恶意节点所发出的报文，仅仅使用数字签名机制是不够的，还需要其他方法，如公钥基础设施的配合。

**2. 链路层攻击**

链路层负责管理数据的多路复用、数据帧的探测、介质存取和纠错控制，它保证网络中点对点、单点对多点的可靠连接。针对链路层的攻击主要有耗尽攻击、非公平竞争攻击、碰撞攻击和确认欺骗攻击等。

（1）耗尽攻击

耗尽攻击是利用了 MAC 层协议（如 IEEE 802.15.4 标准）关于消息重传和消息响应的机制而发起的一种攻击方式，攻击者通过对网络通信的故意干扰或对节点存活期的持续骚扰，从而快速消耗网络和节点资源（如带宽、内存、CPU 和能量），最终使节点失效，网络瘫痪。比如，对网络通信故意干扰的一种实施方式是攻击者侦听网络中节点的正常通信，当节点快发送完一帧时，攻击者马上发出干扰信号，导致该节点的数据发送失败。此时，传统 MAC 协议中的控制算法往往会要求节点重传该帧，反复重传势必造成节点能量快速耗尽。对节点存活期持续骚扰的一种实施方式是攻击者一直对被攻击节点发送请求信号，如不间断攻击，就导致被攻击节点因忙于接收、响应请求，其电源很快耗尽。

针对耗尽攻击的常用防御方法有：①限制网络发送速度，节点自动抛弃多余数据请求，但会降低网络效率。②对过度频繁的请求不予理睬。③限制同一个数据包的重传次数等。

（2）非公平竞争攻击

由于无线信道是单一访问的共享信道，MAC 层协议中通常采取竞争方式进行信道分配。非公平竞争攻击是指如果网络数据包在通信机制中存在优先级控制，那么恶意节点通过一些设置，例如不断在网络上发送高优先级的数据包、设置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不公平地长时间占用信道，就会导致网络中其他节点难以有机会传输数据，使网络失效。

针对非公平竞争攻击的常用防御方法有：①短包策略，不使用过长的数据包（如各种通信协议中一般会规定数据包的最大长度），缩短每包占用信道的时间。②非优先级策略，即不采用优先级策略或者弱化优先级差异，如采用时分复用的方式进行数据传输。

(3) 碰撞攻击

由于无线传感器网络的承载环境是开放的,两个邻居节点同时发送信息会导致信号相互重叠而不能被分离,从而产生碰撞(有时也被称为冲突)。只要有一个字节产生碰撞,整个数据包均会被丢弃。碰撞攻击的原理就是攻击者发送恶意报文故意碰撞正在传送的正常数据包,从而引起接收方校验和出错,导致数据传输失败。而在一些 MAC 层协议中认为发生链路层碰撞,将引发指数退避机制,造成网络延迟甚至瘫痪。

数据链路层的一个核心功能是介质访问控制,具体来说就是围绕避免碰撞解决如下三个问题:①该哪个节点发送数据?②发送时会不会出现碰撞?③出现碰撞了怎么办?解决碰撞攻击的主要方法有以下两种。

① 使用纠错编码技术。通过在数据包中增加冗余信息来纠正数据包中的错误位;通过采用一位或二位纠错编码。如果攻击者采用瞬间碰撞攻击,只影响个别数据位,那么使用纠错编码是有效的。

② 使用信道监听和重传机制。节点在发送数据前先对信道监听一段时间(如能量检测法、载波检测法和能量载波混合检测法),预测信道在一段时间内空闲的时候开始发送,从而降低碰撞的概率,如带冲突避免的载波侦听/多路访问(Carrier Sense Multiple Access with Collision Avoid,CSMA/CA)协议。当发送端准备发送数据时,它首先侦听信道是否空闲。如果检测到信道此时空闲,发送端就等待一个附加的、随机的时间周期后再次侦听信道,如果此时信道仍然是空闲的,则开始发送数据帧。这样做的好处是由于每个发送端采用的随机时间不同,所以可以减小冲突的概率。

接收端如果正确收到发送端的数据帧,则经过一段时间间隔后,向发送端发送确认(Acknowledgement,ACK)帧。一旦该 ACK 帧被发送端成功接收,则表明数据帧发送成功。如果该 ACK 帧没有被发送端检测到,要么是因为数据帧没有被接收端成功接收,要么是 ACK 帧没有被发送端成功接收,那么此时就假定发生了一个冲突。发送端在等待另一个随机的时间后,重发一次数据帧。

CSMA/CA 协议因此提供了一种空中共享访问的方法。这种显式 ACK 机制也对处理干扰问题和其他与无线电有关的问题非常有效。但 CSMA/CA 协议发送数据包的同时不能检测信道上有无冲突,只能尽量“避免”冲突。因为无线电传输链路的一个重要特征是存在远近效应。所谓远近效应,是指一个附近的无线电信号强度大大强于一个来自远处信号的现象。远近效应表明,在一个节点,其发射功率要比同一信道上任何其他节点的功率大得多。因此,当一个节点正在发送数据时,它“听”不到有冲突。

CSMA/CA 的工作原理如图 5-22 所示。

(4) 确认欺骗攻击

确认欺骗攻击又名 ACK 欺骗攻击。为了实现建立路径的可靠性,一些无线传感器网络路由算法依赖于显性或者隐性的链路层确认(ACK)。确认欺骗攻击利用无线链路的广播特性,攻击者通过偷听通向邻近节点的数据包,发送伪造的链路层确认,从而使被攻击节点相信某个失效节点仍在工作,或者相信一个弱链路是一个强链路。其结果是,被攻击节点将在这些链路上传输数据包,但实际情况是这些数据包永远不可能传送到目的节点,从而导致网络瘫痪。

针对确认欺骗攻击的常用防御方法有:运用不完全数据链路层确认消息的路由算法,

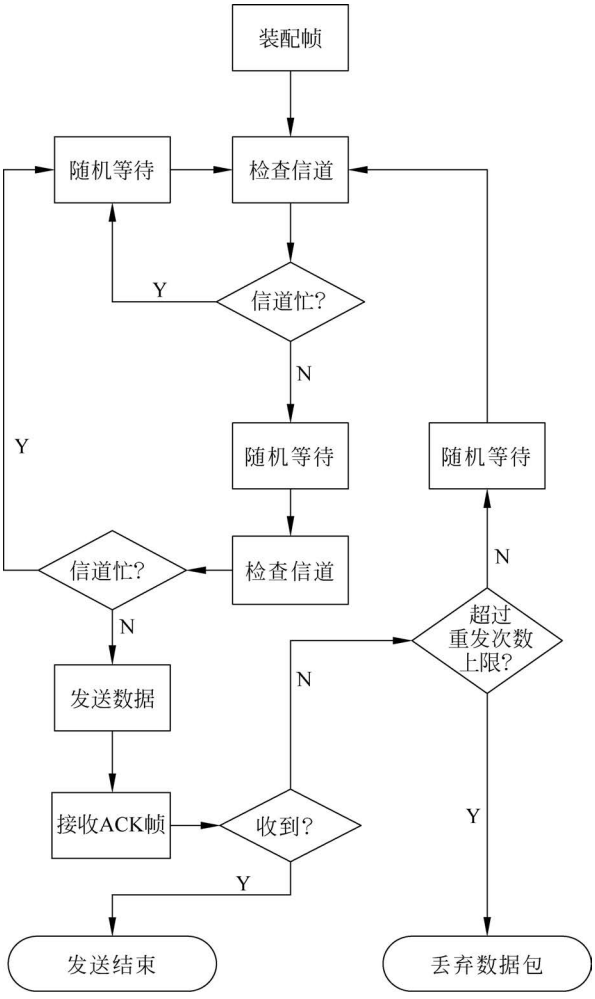



**图 5-22　CSMA/CA 的工作原理**

比如设计适应这种攻击的路由机制，使得在部分节点被破解的情况下，网络只是在性能或功能上有一定的退化，但仍能继续工作。

**3. 网络层攻击**

网络层负责通过数据路由的确定实现与其他网络相结合，能量高效的路由是网络层协议设计的首要目标。所以针对网络层的攻击方式有汇聚节点攻击、伪造路由攻击、黑洞攻击、怠慢和贪婪攻击、女巫攻击、虫洞攻击、方向误导攻击和流量分析攻击等。

（1）汇聚节点攻击

无线传感器网络中有些节点执行路由转发功能，一般称其为汇聚节点、簇头、群头等。汇聚节点承担更多的责任，在网络中的地位相对重要。汇聚节点攻击就是针对这一类节点开展的。具体实施方式如下。

攻击者首先需要确定汇聚节点的位置。比如，监听网络通信相关信息，如信号的强度、网络活跃度，就能锁定汇聚节点位置。一般在无线传感器网络中，由于汇聚节点要担负路由转发功能，所以其信号强度和网络活跃度都较高。另外，由于普通传感器节点要

将采集到的数据包发送给汇聚节点，必然形成一条或多条从普通传感器节点到汇聚节点的传输路径。攻击者就可以利用这些数据包传输所形成的路径找到汇聚节点的位置，如图 5-23 所示。

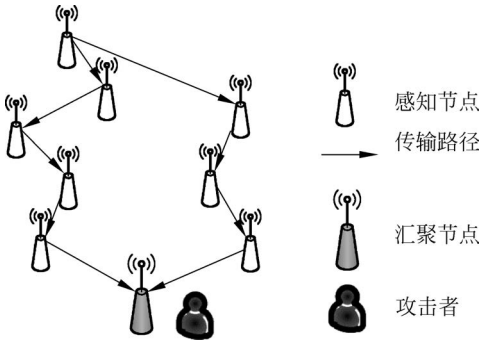



**图 5-23　攻击者根据数据包传输所形成的路径找到汇聚节点位置**

然后攻击者对汇聚节点发动攻击（如阻塞攻击、物理捕获、耗尽攻击、拒绝服务攻击等），目的是使汇聚节点失效，如转发的数据包丢失、能量消耗过快直至瘫痪。汇聚节点失效后，在一段时间内整个无线传感器网络都将不能工作。

针对汇聚节点攻击的防御方法有以下三种。

① 加强路由信息的安全级别，如对在任意两个节点之间传输的数据包（包括产生的和转发的）都进行加密和认证保护，并采用逐条认证的方法抵制异常数据包的插入。

② 增强对汇聚节点地理位置信息的加密强度，加强位置信息重点保护或增加其移动性。

③ 增加汇聚节点的冗余度和灵活多样选择机制。一旦网络的汇聚节点被破坏，可以使用选举机制和网络重组方式进行网络重构。

（2）伪造路由攻击

无线传感器网络中所有数据传输都是由路由协议控制的。一个传输路径是通过相关传感器节点之间的协议消息建立的。攻击者伪造路由攻击主要面向节点之间的路由信息交换，包括篡改路由、欺骗路由和重放路由三种方式，从而产生路由环（如图 5-24 所示）、吸引或排斥网络流量、延长或缩短源路由、产生虚假错误信息、分割网络、增加端至端延迟等情况。前两种方式可以通过对路由信息加签名来防御，第三种方式可以通过在消息中加计数值或时间戳来防御。

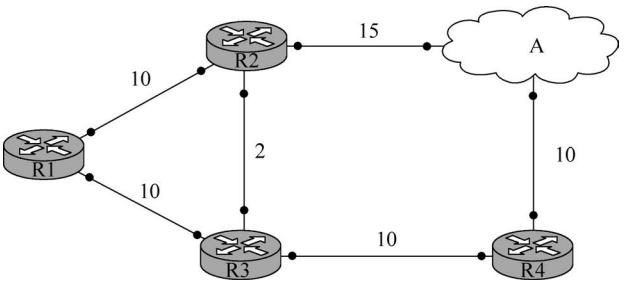



**图 5-24　路由环**

（3）黑洞攻击

黑洞攻击又称为排水洞攻击，如图 5-25 所示。攻击者通过功率更大、发射距离更远的恶意节点将无线通信信息发送到很远的区域，声称自己具有一条到汇聚节点的高质量路径，比如广播“我到汇聚节点的距离为零”，吸引收到该信息的节点会把需要转发的数据包发送给恶意节点。由于无线传感器网络的多跳性，大量数据包会涌入到恶意节点的邻居节点，因为它们都要给恶意节点转发数据包，从而造成信道的竞争。由于竞争，邻居节点的能量很快被耗尽，这一区域就成了黑洞，通信无法传递过去。而即使收到数据包，恶意节点不予正常处理，一般是丢弃。所以黑洞攻击破坏性很强，基于距离矢量的路由算法很容易受到黑洞攻击，因为这些路由算法将距离较短的路径作为发送数据包的优先选择路径。

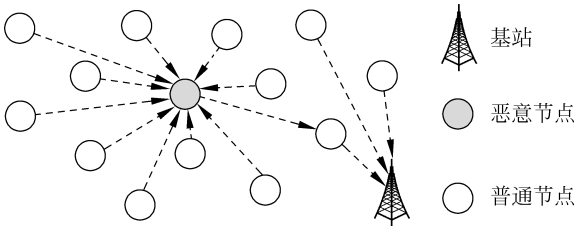



**图 5-25　黑洞攻击示意图**

针对黑洞攻击的常用防御方法有：①认证。②多径路由。多径路由示意图如图 5-26 所示。这样即使攻击者丢弃待转发的数据包，数据包仍可从其他路径到达目标。目标节点通过多径路由收到数据包的多个副本，通过对比可发现某些中间数据包的丢失，进而判定攻击节点的存在和具体位置。③采用基于地理位置的路由协议。基于地理位置的路由协议利用位置信息指导路由的发现、维护和数据包转发，其拓扑结构建立在局部信息和通信上，通过接收节点的实际位置自然寻址，只需要使用局部交互信息而不需要汇聚节点的初始化信息就可以构建路由拓扑，能够实现信息的定向传输，避免信息在整个网络的泛洪，减少路由协议的控制开销，优化路径选择，易于进行网络管理，实现网络的全局优化。基于地理位置的路由协议主要有贪婪周边无状态路由（Greedy Perimeter Stateless Routing，GPSR）协议和图嵌入（Graph Embedding，GEM）协议等。

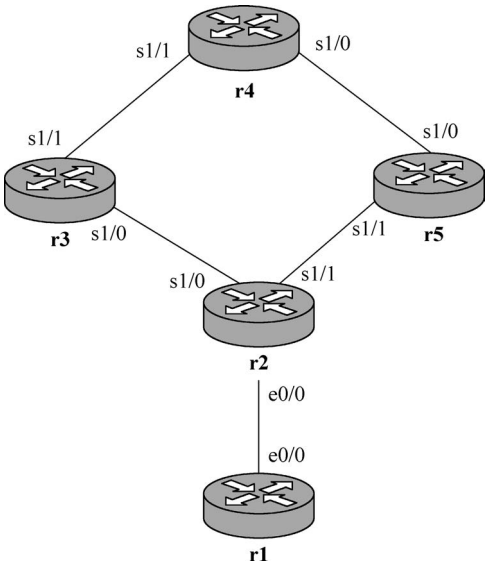



**图 5-26　多径路由示意图**

（4）怠慢和贪婪攻击

怠慢和贪婪攻击也称为选择性转发攻击，攻击示意图如图 5-27 所示，攻击者处于路由转发路径上，随意地少转发、不转发或多转发收到的数据包。如果攻击者向消息源发送收包确认，但是把数据包丢弃不予转发，该攻击称为怠慢攻击。如果攻击者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，该攻击称为贪婪攻击。

针对怠慢和贪婪攻击的常用防御方法有：①利用身份认证机制来确认路由器的合法

性；②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节点。

（5）女巫攻击

女巫攻击是指一个节点冒充多个节点，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。例如，一个分布式存储协议需要保持同一数据的三个副本来保持系统所要求的冗余度，但在女巫攻击下，它可能只能保持一个数据副本。再比如，如图 5-28 所示，无线传感器网络的定位服务中，当接收到节点 S 的定位请求时，恶意节点 $B_4$ 以 $ID_1$、$ID_2$、$ID_3$ 三个不同的身份发送三组定位参数$\{(ID_1, x_1, y_1), (ID_2, x_2, y_2), (ID_3, x_3, y_3)\}$给节点 S，节点 S 虽然已经接收到三个不同节点的定位信息，但是这三个参数实际都是从 $B_4$ 发送出来的，故 $B_4$ 破坏了信息的真实性，将会致使节点 S 的坐标计算错误。

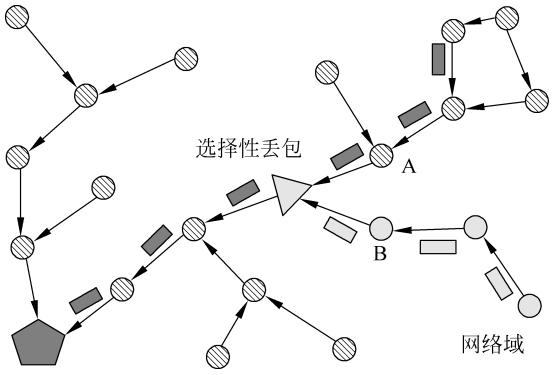



图 5-27　选择性转发攻击示意图

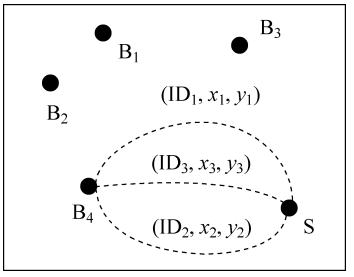



图 5-28　女巫攻击实例

针对女巫攻击的常用防御方法有两种：①节点身份认证，通过密钥、数字证书等对节点身份进行认证，从而防止假冒节点。比如，每个节点都与可信任的基站共享一个唯一的对称密钥，两个需要通信的节点可以使用类似 Needham-Schroeder 协议确认对方身份和建立共享密钥。然后相邻节点可通过协商的密钥实现认证和加密链路。②资源探测法。资源探测法又分为硬件资源探测法和无线电资源探测法。硬件资源探测法即检测每个节点是否都具有应该具备的硬件资源。女巫节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节点大得多时，攻击者也可以利用丰富的资源伪装成多个女巫节点。无线电资源探测法通过判断某个节点是否有某种无线电发射装置来判断是否为女巫节点，但这种无线电探测非常耗电。

（6）虫洞攻击

什么是“虫洞”？这个概念来自物理学，1916 年由奥地利物理学家路德维希·弗莱姆首次提出。简单地说，物理学家认为时空是弯曲的，在一个弯曲时空中旅行，除了沿着时空的弯曲表面行走外，也可以在弯曲时空中挖出一条小道，然后沿着小道快速旅行，这条小道就是虫洞。例如一条虫子要从 U 型槽的左侧前往右侧，它可以顺着 U 形槽表面爬行，但如果能在 U 形槽的左右两端架起一条管道，虫子就可以快速从管道一侧到达另一侧。虫洞无处不在，但却转瞬即逝，物理学家认为存在某种物质可以让虫洞进入稳定状态，这样人类就可以通过虫洞快速到达遥远星系，实现星际旅行，甚至星际移民。当然虫洞还只是理论概念，

迄今为止，物理学家并未在实验中观测到虫洞。

虫洞攻击也称为隧道攻击，攻击示意图如图 5-29 所示，需要两个恶意节点串通合谋进行攻击，其中一个恶意节点位于汇聚节点附近；另一个距离汇聚节点较远，且这两个节点声称它们之间可以建立一条低时延高质量的链路（如高速光纤等），以此吸引其他节点将此链路作为路由链路。通过虫洞转发数据包，可以使得两个远距离的节点认为是相邻的。监测区域 A 与监测区域 B 内的黑色的点为正常节点，在正常的情况下节点 $a$ 点到 $c$ 点需要 5 跳的距离。但是在网络中存在 $X$，$Y$ 恶意节点之后，使得 $a$ 点到 $c$ 点之间就变成 3 跳的距离。在多数无线传感器网络的网络层协议中是基于跳数或是距离选择路由路径，所以恶意节点 $X$ 和 $Y$ 之间的链路会吸引节点 $a$ 点与 $c$ 点附近的通信量，即 $a$ 点和 $c$ 点之间通信不再通过原来正常链路的 5 跳路由，而是改由经过恶意节点的 3 跳路由。因此，虫洞攻击破坏了网络中邻居节点的完整性，使得实际距离在多跳以外的节点误认为彼此相邻，严重的情况下可能导致网络中大部分的通信量被吸引到攻击者所控制的链路上。实施虫洞攻击的最终目的是实施诸如丢弃数据包、篡改数据包内容、进行通信量分析或在特定时刻关闭隧道造成网络路由震荡等。虫洞攻击不一定需要内部被捕获的节点参与，而且检测和抵御的难度都非常大。当然，如果消息源非常接近于汇聚节点，那么发动虫洞攻击就不那么容易了。虫洞攻击也可以和其他攻击（如选择性转发攻击）相结合，而且检测这种攻击十分困难。

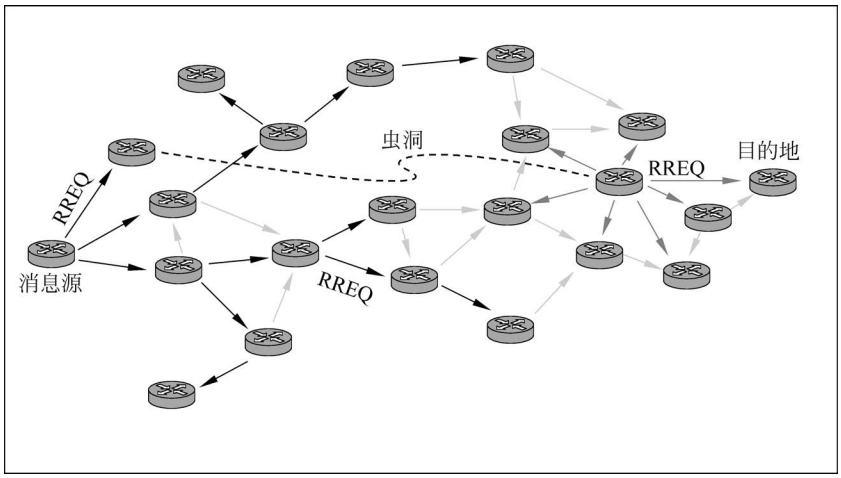



**图 5-29　虫洞攻击示意图**

奇思妙想：假设一个邮差需要将一些重要信件从重庆市运送到成都市。在一般情况下，他会路过很多邮局。尽管过程很慢，但是这种多跳路径是安全的。但是，如果有人说，“嗨，我给你建立了一个路径。这个路径连接了重庆市附近的一个邮局（简称 A）和另一个成都市附近的邮局（简称 B）。从 A 到 B，仅仅需要 30 分钟的路程，因为在它们之间有高速列车”。基于正常的邮寄服务规则，邮差应找到最快捷的方式运输最重要的邮件。因此，他将采取这条路径传送邮件。但实际上，那条路径被攻击者完全控制了。然后，攻击者可以做任何想做的事情了（例如打开每一封邮件，进行阅读）。

针对虫洞攻击的常用防御方法有：①在路由协议设计中加入安全等级策略。安全等级策略是指使用一个安全参数来衡量路由的安全级别。考虑无线传感器网络能量的有限性，在路由设计中加入安全等级策略，由汇聚节点完成监听和检测任务，可使改进后的路由具有

抵御虫洞攻击、陷洞攻击的能力。②采用基于地理位置的路由协议。虫洞攻击难以觉察是因为攻击者使用一个私有的、对传感器网络不可见的、超出频率范围的信道。基于地理位置的路由协议中每个节点都保持自己绝对或是彼此相对的位置信息，节点之间按需形成地理位置拓扑结构，当虫洞攻击者试图跨越物理拓扑时，局部节点可以通过彼此之间的拓扑信息来识破这种破坏，因为“邻居”节点将会注意到两者之间的距离远远超出正常的通信范围。

(7) 方向误导攻击

这里的方向是指数据包转发的方向。恶意节点在接收到数据包后，对其源地址和目的地址进行修改，使得数据包沿错误路径发送出去，造成数据包丢失或网络混乱。如果被攻击者所控制的路由器将收到的数据包发给错误的目标节点，则源节点受到攻击，因为它要求转发的数据包无法到达目标节点；如果将所有数据包都转发给同一个正常节点，则该节点很快因接收过多的数据包而导致通信阻塞和能量耗尽，最终失效。

针对方向误导攻击的常用防御方法有：

① 出口过滤。因为方向误导攻击的防御方法与网络层协议相关。对于层次式路由机制，通过出口过滤方法认证源路由的方式确认一个数据包是否是从它的合法子节点发送过来的，直接丢弃不能认证的数据包。这样，攻击数据包在前几级的节点转发过程中就会被丢弃，从而达到保护目标节点的目的；

② 认证。

③ 监测机制。通过建立节点数据包监测机制，当发现节点接收的数据包数量发生异常，如明显过多时，可以触发相应的保护机制，如启动数据包的来源节点的身份认证或自动休眠，从而避免自身能量被快速耗尽。

(8) 流量分析攻击

无线传感器网络的主要目的是从大量远程节点中收集数据传输到汇聚节点。因此，网络中的传输模式是多对一，这样就给了攻击者对网络发动攻击的机会。在无线传感器网络中，数据流的种类通常包括：从汇聚节点到节点传输的命令流；从节点到汇聚节点的数据流；一些和簇头节点选举或数据融合相关的局部通信数据流。攻击者通过侦听通信，可以发起流量分析攻击，试图从诸如数据包、数据流模式、路由协商信息等方面发现那些为网络提供关键服务的节点(例如，簇头节点、密钥管理节点，甚至汇聚节点或靠近汇聚节点的节点等)位置，然后发动其他攻击，谋求更大的攻击利益。例如，攻击者可以分析传输模式，收集无线传感器网络的拓扑结构，以及通过观察流量和模式确认汇聚节点位置。攻击者通过观察流量，推断出多个路径的交叉点上的“重要”节点；然后攻击者攻击和破坏这些“重要”节点，最终将网络分割为几个相互分离的子网络。攻击者可以通过观察其邻近节点的数据包发送速率，然后关注具有更高数据包发送速率的节点；或者可以观察一段时间内节点间数据包的发送情况，并尝试跟踪被转发数据包的发送路线，最终到达汇聚节点。

针对流量分析攻击一个可能的解决方案是“迷惑”攻击者。例如，在一个源节点和目的节点之间，建立随机和多跳路径，或者使用概率路由，或者在网络中引入假消息。在一个基于地理位置的概率路由中，它根据邻近节点一个子集中节点的链路质量和剩余能量随机选择下一跳。实验结果显示，基于地理位置的概率路由高效节能，并具有较高的网络吞吐量。但使用“迷惑”信息可能会增加网络的能源消耗和网络内流量。

**4. 传输层攻击**

传输层负责管理端到端的连接，异步攻击和泛洪攻击是针对这一层的主要攻击手段。

(1) 异步攻击

异步攻击，也称破坏同步攻击，是指攻击者破坏目前已经建立的连接。比如，两个节点正常通信时，攻击者监听并向双方发送带有错误序列号的数据包，使得双方误以为发生了丢失而要求对方重传，从而耗尽其能量。攻击者还可以反复地向接收节点发送欺骗信息，使得接收节点要求发送节点重传丢失的帧，如果时间标记准确，攻击者可以降低甚至完全破坏接收节点交换数据的能力。

针对异步攻击的常用防御方法有：要求在交换数据包时进行双方节点身份确认，但由于无线传感器网络中节点的物理安全得不到保障，所以节点使用的身份确认机制也可能被攻击者知道，从而无法判断数据的真假。

(2) 泛洪攻击

泛洪攻击示意图如图 5-30 所示，是指攻击者不断地要求与邻居节点建立新的连接，从而耗尽邻居节点用来建立连接的资源，使得其他合法的对邻居节点的请求不得不被忽略。

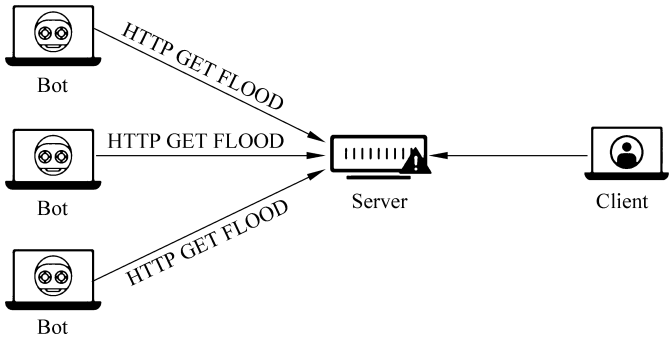



**图 5-30　洪泛攻击示意图**

针对泛洪攻击的常用防御方法有：①客户端谜题。利用限制连接数量和客户端谜题的方法进行抵御。要求客户成功回答服务器的若干问题后再建立连接，它的缺点是要求合法节点进行更多的计算、通信从而消耗了更多的能量。②入侵检测机制。引入入侵检测机制，汇聚节点可限制这些泛洪攻击报文的发送。如规定在一定时间内，节点发包数量不能超过某个阈值。

(3) Hello 泛洪攻击

在一些无线传感器网络和物联网路由协议中，节点需要定时发送 Hello 包来表明自己的身份，而收到该信息的节点认定自己处在发送节点信号有效范围内，发送节点是自己的邻居。当存在恶意节点利用其强大的功率广播 Hello 包，收到信息的节点就将该恶意节点作为自己的邻居节点。在以后的路由中，这些节点可能会使用恶意节点的路径，从而导致网络流量的混乱，使得网络不能正常运行。作为 Hello 泛洪攻击的节点甚至不需要拥有一个合法的身份也能利用 Hello 信息来攻击网络，只要该节点拥有足够大的发射功率，就可以达到破坏原来网络拓扑结构的目的。因此，在某种意义上，Hello 泛洪攻击是一种单向的广播虫洞。

针对 Hello 泛洪攻击的常用防御方法有：在身份认证中为确保通信一方或双方的真实性，要对数据的发起者或接收者进行认证。认证能够确保每个数据包来源的真实性，防止伪

造，拒绝为来自伪造节点的信息服务。例如，通过信任的汇聚节点使用身份确认协议认证每一个邻居的身份、且用汇聚节点限制节点的邻居个数，当攻击者试图发起 Hello 泛洪攻击时，必须被大量邻居认证，这将引起汇聚节点的注意。

**5. 应用层攻击**

应用层攻击包括感知数据的窃听、篡改、重放、伪造等，以及节点不合作行为，例如对应用层功能如节点定位、节点数据收集和融合等的攻击，使得这些功能出现错误。

针对应用层攻击的常用防御方法：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、信任管理，入侵检测。

## 5.4 物联网终端安全

### 5.4.1 物联网终端安全概述

物联网终端处于感知层的末端，是整个物联网的“神经末梢”，物联网安全首先要解决的是终端的安全问题。近年来，随着物联网应用的不断深入，物联网终端渗透进智慧物流、智慧仓储、智能交通、智慧医疗、智慧电网、智慧农业等各行各业，走进人民的生产生活，全面推动物联网终端呈指数增长态势。物联网终端通常可分为两类：一种是感知识别型终端，以二维码、RFID、传感器为主，实现对“物”的识别或环境状态的感知；另一种就是应用型智能终端，包括输入/输出控制终端，如计算机、平板电脑、智能手机、摄像机，智能手环、智能手表等各种穿戴式设备，疫情时代的红外测温仪等。在全球范围内，物联网终端数量高速增长。截至 2019 年，全球物联网终端连接数量达到 110 亿个。其中，消费物联网终端连接数量达到 60 亿个，工业物联网终端连接数量达到 50 亿个。据 GSMA 预测，2025 年全球物联网终端连接数量将达到 250 亿个。其中，消费物联网终端连接数量将达到 110 亿个，工业物联网终端连接数将达到 140 亿个，占全球终端连接数量的一半以上，具体如图 5-31 所示。未来，工业物联网将引领整体连接数量持续增长，从 2017 年到 2025 年将实现 4.7 倍的增长，年均增长率达 21%。

然而，物联网终端安全事件频发，安全隐患凸显，安全形势严峻。物联网终端被破坏、被控制、被攻击，物联网卡被滥用，不仅影响应用服务的安全稳定，导致隐私数据泄露、生命财产安全受损，还会危害网络关键基础设施，甚至威胁国家、军队安全。

**1. 标准缺失**

物联网终端应用场景多，种类多样，操作系统不同，缺乏统一的安全标准。同时，物联网终端功能差异较大，难以实现统一的安全要求，导致终端安全能力水平不一。

**2. 体系缺失**

物联网终端安全防护体系尚未建立，终端可控性差，达不到电信级管理要求，难以实现集中管控，因此，终端安全监控、日常巡检不足，终端安全问题难以被及时发现与处置。

**3. 评测缺失**

针对物联网终端未有效开展安全评测，终端缺乏入网安全管控，“带病”联网问题突出，安全隐患长期存在。


**图 5-31　物联网终端增长图**

**4. 技术缺失**

物联网终端安全能力不同，缺乏必要的安全防护机制，终端自身应对安全攻击的能力不足。

**5. 意识缺失**

安全意识缺失，在终端生产时并未同步进行安全设计，系统及设备源头上存在安全隐患；同时，用户在使用终端时安全意识缺失，安全配置并未广泛启用。例如，为贪图使用的便利性，很多用户使用物联网终端的默认密码或根本不知道如何修改密码。

**6. 终端安全能力低**

物联网终端受成本所限，通常系统处理能力也不会很高。这意味着，它们缺乏强有力的安全解决方案和加密协议，而这些往往导致物联网终端难以抵抗暴力攻击。

### 5.4.2　物联网终端安全需求

物联网终端的安全需求主要包括物理安全防护、访问控制、机密性、私密性、完整性、可用性等多个方面。

**1. 物理安全防护**

物联网终端需要具备足够的物理安全防护措施以保证工作期间自身物理实体不被损坏，为终端功能的正常运行提供必要的保障。对于户外安装的终端设备，如用于安防、交通的摄像机，水下探测设备等需要具备足够的防水功能，具有足够的机械强度。对于只允许专业人员开启的设备，可以加装锁具、进行铅封。

**2. 访问控制**

物联网终端必须加强访问控制，防止非授权用户的访问。比如使用网络摄像头时，必须对网络摄像头默认的账户密码进行修改。对于一些使用 ZigBee、蓝牙等短距离通信技术的

智能表计，当其他设备要与之通信时必须进行身份验证，防止非授权设备读取表计数据。

例如，赛门铁克公司的研究人员最近发现了一种新的 Linux 蠕虫病毒，能感染家庭路由器、机顶盒、安全摄像头，以及其他一些能够联网的家用设备。这种名叫 Linux.Darlloz 的蠕虫病毒已被归类为低安全风险，因为当前的版本只能感染 X86 平台设备。但是这种病毒在经过一些修改之后产生的变种已经能够威胁到使用 ARM 芯片以及 PPC、MIPS、MIPSEL 架构的设备。这种蠕虫病毒会利用设备的弱点，随机产生一个 IP 地址，通过常用的 ID 以及密码进入机器的一个特定路径，并发送 HTTP POST 请求。如果目标没有打补丁，它就会从恶意服务器继续下载蠕虫，同时寻找下一个目标。虽然 Linux.Darlloz 还没有在世界范围内造成巨大的危害，但也暴露出目前大多数联网设备的一大缺陷：它们大多都是在 Linux 或者其他一些过时的开源操作系统上运行。

**3. 机密性**

物联网终端在传输数据时需要对数据进行必要的加密，以防止他人恶意窃取数据，获取用户机密。现实中，终端厂家在开发加密机制的终端时，需要考虑算法的选择、密钥的分发和存储机制等，这存在一定的研发难度，而且除非出现安全事故，否则用户一般无法确认物联网终端是否具有加密机制，这就导致一些终端厂家索性忽略机密性，安全隐患极大。

例如，2014 年 3 月 27 日，中央电视台重点报道家庭监控器存在较高安全隐患，引发社会广泛关注。家庭监控器在近年来越发普及，广泛地被普通市民用来防范家庭安全隐患。如今曝出监控器被大量监控无疑引起人们的高度恐慌，对家庭、人身财产安全造成不可估量的威胁。黑客可以轻松通过这些缺陷控制整个摄像头，达到窥视的目的。不仅如此，黑客还可以通过欺骗手段，让用户在远程查看自己家里的监控器画面时，永远是一个静止的画面，而非真实现场环境。更可怕的是，存在安全隐患的监控器并不仅仅是家用监控器，应用于其他公共场所、银行、办公室、监狱等的监控器，同样存在隐私泄露的风险。

**4. 私密性**

物联网终端内存有用户的私密数据，比如身份证号码、指纹、声纹、虹膜等个人信息，通信录等隐私信息。物联网终端需要有足够的安全机制保证这些私密信息在无用户授权的情况下，他人无法读取。终端通常可以采用单独的安全处理器、存储区或者 TrustZone 等来保证私密性。

**5. 完整性**

物联网终端应当保证自身软件的完整性，不能被外部恶意程序入侵。对于支持安装应用的终端，必须对应用开发者进行验证，不允许安装无法通过验证和来源不明的应用。物联网终端在进行系统软件升级时也要对升级软件包进行验证。终端在与外界进行通信时，也要防止恶意程序经由各种漏洞入侵终端的软件系统。终端开机时，需要对自身的文件系统进行完整性和一致性的检验，出错后可以从备份中恢复受损的文件系统。

**6. 可用性**

多数物联网终端一经部署就进入无人值守的自动工作状态，这就要求终端具备一定的可靠性，保证在使用寿命范围内的持续可用性。比如低功耗广覆盖（Low Power Wide Area，LPWA）领域，某些终端具备 5W 电池 10 年续航能力，这不仅是对终端的低功耗要求，也是对终端持续可用性的要求，终端在无人值守的情况下能够至少正常工作 10 年。

### 5.4.3　物联网终端的安全威胁

近年来，随着物联网终端品类的快速增长，各种应用爆发，涉及到的软件、硬件组件越来越多，各种安全问题也有愈演愈烈的趋势。本书主要从以下七方面讨论物联网终端安全问题中危害大、防范难的软件安全问题。

**1. 非授权访问**

非授权访问是恶意入侵物联网终端的第一步。随着物联网终端智能化程度和处理能力的增强，很大一部分终端都内置了 Linux 系统，又由于种种原因，很多设备的 root 口令被公开，通过 SSH 登录后，就获得了对终端的完全控制。除了根口令，其他口令如果不够复杂，也存在一定的安全隐患。实际上，Mirai 恶意软件之所以成功，是因为它可以识别易受攻击的物联网设备，并使用默认用户名和密码登录并感染它们。尽管许多政府工作报告都要求制造商不要销售带有默认密码的物联网设备，例如使用“admin”作为用户名和/或密码，有两个潜在问题还是从一定程度上妨碍了人们加强密码安全措施：首先，多数用户，特别是消费级用户可能根本不了解如何更改默认密码；其次，制造商为了提供用户对设备的便捷的消费体验，将用户名和密码硬编码到设备中，而不给用户更改它们的能力。

2011 年，计算机科学家兼黑客 Ralf Weinmann 博士设计了一个假冒 GSM 基站。当 iPhone 在这个基站上注册时，在鉴权过程中，假基站发出一条专门设计的非法消息，iPhone 使用的基带芯片解码这条消息时会发生缓冲区溢出，之后将打开自动接听功能。于是，iPhone 就变成了一部窃听器。2017 年 4 月，Ralf Weinmann 发现了华为海思巴龙基带处理器的 MIAMI 漏洞，利用该漏洞，同样可以把使用了该芯片的手机、笔记本或者其他物联网设备变成窃听器。这种利用基带处理器实现的在线升级（Over The Air，OTA）入侵应该引起足够的重视。非授权访问的攻击点下沉到通信处理器芯片层面，这是一个需要警惕的现象。

为了防止此类问题的发生，一方面要注意加强系统口令的保护，另一方面也要注意操作系统的升级。

**2. 信息泄露**

物联网终端部署在无人值守的户外时，很容易被物理捕获或窃取，因此存在信息泄露的风险。若大量被控设备同时访问服务器，则极易导致大规模分布式拒绝服务攻击（详见 7.4 节）。信息泄露可能会给终端用户带来直接危害。比如根据水表、电表或者燃气表的详细计量，可以准确地推断出某处住房是否有人、有多少人。不法分子根据这些数据完全可以做到“远程踩点”。保证信息不泄露的关键在于保证终端不被非法入侵。但是，还有一些不需要入侵的“无创”型信息泄露。以智能手机为例，各种传感器、无线通信功能携带了非常多的“旁路”信息可供利用：网页里的 JavaScript 程序无须授权就可以读取陀螺仪数据，而陀螺仪会受人讲话的干扰，JavaScript 程序记录并分析陀螺仪数据，虽然当采样率不足（一般最高为 200Hz）时无法完全还原出人声，但是在说话人声音识别、孤立词识别方面取得了一定的成功率。再比如通过手机中加速度传感器的输出判断手机姿态，进而判断是否在通话也有较高的成功率。当手指点击屏幕时会对无线信号的传播产生微弱影响，点击的位置不同影响也不同，据此通过考察 Wi-Fi 信号的信道状态信息（Channel State Information，CSI）的

变化可以推断出用户的点击位置，从而实现用户密码的窃取等。类似的旁路攻击隐蔽性强，防范困难。

### 案例

从理论上说，通过一个普通路由器使用 Wi-Fi 信号准确检测出用户的击键记录是可能的，来自美国密歇根州立大学和中国南京大学的研究人员就找到了这种方法。研究人员指出，在受到最小信号干扰的环境下，攻击者能通过中断路由器 Wi-Fi 信号来检测出用户在键盘上的击打记录，然后利用这些数据盗取用户的密码，研究人员已经通过 WiKey 实验演示过这样的情景。

### *案例

**智能家用电器在给生活带来便利的同时，也易引发泄密问题**

目前，智能家用电器越来越受欢迎。人们喜欢将空调、冰箱、电视和电热水器等家用电器与网络连接。这种设计给生活带来方便，同时也引发一些问题。俄罗斯专家警告，一旦遭到黑客袭击，智能家用电器不但可能导致用户信息被窃取，甚至会沦为大规模网络攻击的“帮凶”。为此，俄罗斯专家为如何避免使用智能家用电器时成为黑客的受害者支招。

俄罗斯《消息报》报道称，随着物联网技术的推广应用，将智能功能嵌入家用电器成为发展潮流。从冰箱、空调、电视等大型家用电器，到音箱、吸尘器、体重秤等小型家用电器，均配备无线接口，以便通过网络进行远程激活和数据传输，旨在方便人们的生活。然而，这些智能家用电器在接入网络后会带来网络安全漏洞，黑客能借此拦截用户信息或生物识别数据，其跟踪方法因智能设备和传感器不同而各异。俄罗斯专家称，内置语音助手的扬声器能记录人们的对话，并将音频数据发送至第三方服务器。内置摄像头的设备能发送照片和视频数据，而带 GPS 模块的设备能进行定位。例如，机器人吸尘器能根据在房屋周围的移动情况绘制房屋平面图，然后将其发送至第三方服务器。同样，黑客还可通过智能家用电器从无线网络中获取用户密码，并掌握电器使用情况和用户活动时间，基于这些数据，可了解用户生活规律等隐私。例如，用户在哪里与谁共度时光。

俄罗斯专家表示，用于收集用户信息最常见的设备是智能手机、监控设备和各种智能家用电器。它们收集的数据范围很广，从照片、视/音频材料，到信件、邮件等都难“幸免”。收集到的数据可用于各种目的：勒索、破坏商业活动及获取个人利益。对用户来说，这样的信息收集活动不易被察觉。

如何避免被监视呢？俄罗斯专家表示，如果用户自身网络安全意识薄弱，则极易遭到黑客入侵。实际上，很多智能家用电器都带有安全功能，但用户往往不知道，或为使用方便将其禁用。最典型的做法是不更改制造商分配的默认密码。目前，最大的威胁是黑客可以使用特殊应用程序访问用户智能手机，进而访问由手机控制的所有智能家用电器。

如何保护自己免受智能家用电器的监视？专家建议通过设置复杂密码保护无线网络和设备，并避免使用任何用户、设备或程序均可访问的智能家用电器。另外，为防止黑客访问智能手机，勿安装未知来源的应用程序。在解锁智能手机时，须监视已安装的设备并启用强制性密码输入。使用智能摄像头时尽量选购带加密功能的产品，使用时应启用双重认证，即

登录时需要密码和验证码双重认证。此外，还应尽量避免使用同一账号和密码登录多个平台，密码也应尽量复杂。避免被监视最好的方法是仅使用必要的智能家用电器，并定期更新设备软件。另外，还可通过物理断开方法控制它们，如将智能咖啡机断电，将智能手机放在屏蔽盒中，用超声波干扰器削弱扬声器上的麦克风等。

请结合上述案例思考，我们如何在享受智能家用电器给生活带来便利的同时，保护好相关信息不被泄露？

**3. 系统漏洞风险**

系统漏洞及软件漏洞难以避免，物联网终端部署分散，现场升级不易实施，而远程升级一旦失败会影响业务正常运营。同时，大部分漏洞可能并不影响业务正常运行，因此，部分用户升级意愿较低，导致大量设备会长期“带病”运行，极容易被黑客恶意控制。

例如，2014 年 10 月，研究人员发现西班牙所使用的智能电表存在安全漏洞，该漏洞可以导致电费诈骗甚至进入电路系统导致大面积停电。原因主要在于电表内部保护不善的安全凭证可以让黑客获取到并成功控制电路系统。发现该漏洞的研究人员 Javier Vazquez Vidal 表示，该漏洞影响范围非常之广，西班牙提高国家能源效率的公共事业公司所安装的智能电表就在影响范围之列。研究人员将会公布逆向智能电表的过程，包括他们是如何发现这个极其危险的安全问题，以及该漏洞将如何使得入侵者成功进行电费欺诈、甚至关闭电路系统。该漏洞存在于智能电表中，而智能电表是可编程的，并且同时包含了可能用来远程关闭电源的缺陷代码，影响范围极广。

**4. 拒绝服务攻击**

一些具备关键功能的物联网终端有可能受到拒绝服务攻击，比如门禁功能失效后，会危及财产安全。为了尽量减少遭受拒绝服务攻击的可能性，一方面终端需要识别攻击并采取一定的防御措施，另一方网络设备也需要基本的攻击鉴别能力并较早地将攻击方进行隔离。

**5. 假冒节点攻击**

物联网终端被入侵后，可能被远程控制成为他人发动 DDoS 攻击的工具。比如 2016 年 Linux Mirai 恶意软件入侵了大量的家用路由器、网络摄像头、数字摄像机等设备，这些设备在远程控制下成功发起了多起 DDoS 攻击，其中在 2016 年 9 月 20 日对某博客网站的攻击中流量超过 620Gb/s，9 月底的另一次攻击中流量为破纪录的 1.5Tb/s。

**6. 自私性威胁**

物联网终端接入网络后不能出于自私而滥用网络资源。为了避免终端出现此类自私行为，需要对终端进行入网认证测试，确保终端行为符合网络协议及无线网络监管规定。

**7. 恶意代码攻击**

恶意代码入侵终端后，可以获取信息、修改终端行为，乃至使终端完全丧失功能。终端内运行的软件需要经过严格的测试、验证，尽可能避免出现漏洞。可以采用源代码静态分析软件对代码进行分析，也可以对代码进行充分的白盒测试、模块测试，保证测试结果至少达到语句覆盖和条件组合覆盖，还可以考虑使用支持契约编程等高级特性的编程语言，使用测试驱动开发方式等多管齐下的方式，保证软件质量。

### 5.4.4 物联网终端的安全机制

**1. 使用可信的数据网络**

对于物联网终端来说，可信的网络包括无线服务提供商的数据网络以及公司、居家和可信地点提供的 Wi-Fi 连接。这样就可以确保用于进行数据传输的网络没有安全威胁，也无法被攻击者用来获取所传输的敏感数据。实现设置和管理假冒的 Wi-Fi 连接点比实现假冒的蜂窝数据连接容易得多。因此，使用由无线服务提供商提供的蜂窝数据连接能够有效降低遭受攻击的风险。

**2. 使用可靠方式获取应用程序**

对于我们使用的移动终端，终端的操作系统都会带有系统自身的应用商店，如苹果系操作系统平台会带有 App 商店；安卓操作系统平台一般会配有谷歌商店或一些设备提供厂商自己开发的应用商店，比如华为手机会带有华为应用市场。使用设备提供厂商自带的应用商店下载应用程序，会大大增强应用程序的源安全性。

**3. 赋予应用程序最少的访问权限**

当从应用市场下载和安装应用程序时，确保只给予应用程序运行所需的最少权限。如果一个应用的权限要求过度，用户可以选择不安装该应用或者将该应用标记为可疑，不要轻易确认应用程序提及的访问权限。

**4. 物联网终端的安全设计**

目前，很多物联网终端设备制造商并没有很强的安全背景，也缺乏标准来说明一个产品是否是安全的。很多安全问题来自于不安全的设计。因此，物联网终端设备制造商可以从以下三方面加强物联网终端的安全设计：一是提供安全的开发规范，进行安全开发培训，指导物联网领域的开发人员进行安全开发，提高产品的安全性；二是将安全模块内置于物联网产品中，比如工控领域对于实时性的要求很高，而且一旦部署可能很多年都不会对其进行替换，这使得安全可能更偏重安全评估和检测，如果将安全模块融入设备的制造过程，将能显著降低安全模块的开销，为设备提供更好的安全防护；三是对出厂设备进行安全检测，及时发现设备中的漏洞并协助厂商进行修复。

## 本章小结

本章分析了物联网感知层面临的安全问题，探讨了物联网感知层的安全机制；重点分析了物联网的 RFID 安全问题和无线传感器网络安全问题，探讨了 RFID 安全的解决方案，重点介绍了基于物理和基于哈希函数的安全解决方法。最后，简要地讨论了物联网智能终端安全。

## 思考与练习

1. 为什么说物联网感知层安全极端重要？
2. 现在许多小轿车使用了基于 RFID 的汽车钥匙，你知道它们是如何保证车辆安全的

吗？媒体曾曝出针对车辆的遥控解码器(干扰器)导致车主损失的报道，从攻击的角度这属于哪一种情形？技术上如何实现的？我们该如何防范？

3. 以保护我国疆域安全为例，试针对某一海洋区域，设计基于无线传感器网络的监测防护体系，对敌方潜艇等活动情况进行侦测。

4. 面对无线传感器网络的特点和安全需求，你能想到的安全方案是什么？

5. 试设计一个以 RFID 应用为基础的营区门禁系统，突出体现其安全控制方案的实现和方案中的非技术要素。

6. 请列举几个威胁 RFID 应用系统安全的例子。

7. 简述 RFID 的基本工作原理和 RFID 的安全技术。

8. 物联网的感知层存在哪些安全危险？

9. 物联网的感知层在安全技术上包含哪些内容？

10. 物联网的终端安全措施有哪些？