第 5 章　物联网安全

随着物联网建设的加快，物联网的安全问题必然成为制约物联网全面发展的重要因素。在物联网发展的高级阶段，由于物联网场景中的实体均具有一定的感知、计算和执行能力，广泛存在的这些感知设备将会对国家基础设施、社会和个人信息安全构成新的威胁。一方面，由于物联网具有网络技术种类上的兼容性以及业务范围无限扩展性等特点，因此当大到国家电网数据，小到个人病例情况都接到看似无边界的物联网时，将可能导致更多的公众个人信息在任何时候、任何地方被非法获取；另一方面，随着国家重要的基础行业和社会关键服务领域如电力、医疗等，都依赖于物联网和感知业务，国家基础领域的动态信息将可能被窃取。所有的这些问题使得物联网安全上升到国家战略层面，成为影响国家发展和社会稳定的重要因素。

5.1　物联网安全问题分析

对于无法保证隐私信息以及不能提供完善安全措施的新技术，用户是不会在他们的生活中应用的。如果物联网的安全问题不能得到很好的解决，或者说没有很好的解决办法，将会在很大程度上制约物联网的发展。从物联网的概念中可以得知，物联网是一种虚拟网络与现实世界实时交互的新型系统，其核心和基础仍然是互联网，是在互联网基础上的延伸和扩展，其特点是无处不在的数据感知、以无线为主的信息传输、智能化的信息处理，用户端可以延伸和扩展到任何物品与物品之间，进行信息交换和通信。因为与物联网相结合的互联网本身就早已存在许多安全问题，传感网和无线网络与一般网络相比存在着特殊的安全问题，而物联网又以传感网、无线网络为核心技术，这更是给各种针对物联网的攻击提供了广阔的土壤，使物联网所面临的安全问题更加严峻。

5.1.1　物联网安全特点

物联网安全的相关技术特点有可跟踪性、可监控性、可连接性。

1. 可跟踪性

可跟踪性说明人们在任何时候都能知道物品的精确位置和周围环境参数。物联网的可跟踪性在航空业与公安部门应用很广，部分航空公司采用 RFID 技术，跟踪查找乘客失踪的行李。公安机关利用跟踪定位查找失踪人口的下落，既节省了人力物力，也提高了工作效率。物联网结合移动通信技术，使用无线网络对物品进行兼容与控制。假若物联网结合手机的 3G 网络，那将使人们的生产和生活发生极大变化，使之更加便捷和安全。例如在外地

的子女给老人戴上智能传感手表，利用手机随时了解父母的血压等身体症状。又如嵌入传感器的智能住宅，能在主人离家时自动关闭门窗和水电气，并定时发送安全情况信息给主人。再如在物流领域中，通过使用射频识别技术，在途中运输的货物和车辆都嵌入电子标签，利用路边的定点读写器读取信息，再通过通信卫星将信息传送给调度中心，动态跟踪整个运输过程，这样就可以防止运输货物的丢失，保证运输安全。

2. 可监控性

物联网可以通过物品来实现对人的监控与保护。以医疗系统中的健康监测为例，健康监测用于人体的监护、生理参数的测量等，可以对人体的各种状况进行监控，将数据传送到各种通信终端上，这样医生可以随时了解被监护病人的病情，以进行及时处理。另外，在射频自动识别不停车收费系统（ETC）中，通过安装在车辆挡风玻璃上的电子标签与在收费站ETC车道上的微波天线之间的专用短程通信，利用计算机联网技术与银行进行后台结算处理，从而达到车辆通过路桥收费站不需停车就能缴纳费用的目的，可以对经过的车辆进行监测，记录车辆的收费情况，并最终将数据传送至收费中心，进行自动化的收费处理，大大提高了车辆的通行效率。

3. 可连接性

物联网通过与移动通信技术结合，实现物品通过无线网络的控制与兼容。例如在汽车及其钥匙上都植入微型感应器，醉酒驾车的现象就可能被杜绝。当喝了酒的司机拿出汽车钥匙时，钥匙能通过植入其中的气味感应器察觉到酒气，并通过发射无线信号让汽车“不要发动”，汽车就会自动罢工，并能够“指挥”司机的手机给他的亲友发送短消息，通知他们司机的位置，让亲友们来处理。又如商场超市里销售的禽肉蛋奶，在包装上嵌入微型感应器，顾客用手机扫描就能了解食品的产地和转运、加工的时间地点等各个环节，是否绿色安全等一目了然，甚至还能显示加工环境的照片。

5.1.2 物联网安全挑战

物联网安全的挑战可以分为传统技术安全的挑战以及特殊技术的挑战。

1. 物联网传统技术安全挑战

（1）移动通信的安全问题

随着3G手机在我国得到迅速的应用和推广，由3G手机带来的安全隐患也随之而来。3G（3rd-generation，第三代移动通信技术），是指支持高速数据传输的蜂窝移动通信技术。若将3G手机与物联网智能结合，会使得人们的生活更加方便，进而改变人们的生活方式。但是，3G手机是否安全将直接影响物联网的安全。其一，3G手机与计算机同样存在多种多样的漏洞，漏洞病毒会影响物联网的安全；其二，手机虽然简便易携带但是也极易丢失，这样就可能会对用户造成一定损害。

（2）信号干扰

若物联网的相关信号被干扰，那么对个人或国家的信息安全会有一定威胁。个人利用

物联网高效地管理自身的生活，智能化处理紧急事件。然而，若个人传感设备的信号遭到恶意干扰，就极易给个人带来损失。对于国家来说也一样，若国家的重要机构使用物联网，其重要信息也有被篡改和丢失的危险。例如，银行等重要的金融机构涉及大量个人和国家的重要经济信息。通常这些机构中配置了 RFID 等物联网技术，一方面有利于监控信息，另一方面成为了不法分子窃取信息的主要途径。

（3）恶意入侵与物联网相整合的互联网

物联网建立在互联网的基础上，高度依赖于互联网，存在于互联网中的安全隐患在不同程度上会对物联网有影响。目前，互联网遭受的病毒、恶意软件、黑客攻击层出不穷，同样，在物联网环境中互联网上传播的病毒、恶意软件，黑客如果绕过了相关安全技术的防范，就可以恶意操作物联网的授权管理，控制和损害用户的物品，甚至侵犯用户的隐私权。让人忧心忡忡的，像银行卡、身份证等涉及个人隐私和财产的敏感物品，若被他人控制，后果会不堪设想，不但会造成个人财产的损失，还会威胁到社会的稳定和安全。

2. 物联网特殊技术安全挑战

物联网除了传统网络安全威胁之外，还存在着一些特殊安全问题。这是由于物联网是由大量机器构成的，缺少人对设备的有效监控，并且数量庞大、设备集群度高，物联网特有的安全威胁主要存在于以下几个方面。

（1）节点安全

由于物联网的应用可以取代人来完成一些复杂、危险和机械的工作，所以物联网感知节点多数部署在无人监控的场景中。那么，攻击者就可以轻易地接触到这些设备，甚至通过本地操作更换机器的软硬件，从而对它们造成破坏；另一方面，攻击者可以冒充合法节点或者越权享受服务，因此，物联网中有可能存在大量的损坏节点和恶意节点。

（2）假冒攻击

在物联网标签体系中无法证明此信息已传递给阅读器，攻击者可以在获得已认证的身份后，再次获得相应服务。智能物品感知信息和传递信息基本上都是通过无线传输实现的，智能传感终端、RFID 电子标签相对于传统的互联网是“裸露”在攻击者的眼皮底下的，传输平台也是在一定范围之内“暴露”在空中的，在传感器领域的“窜扰”就显得非常频繁和容易。在传感器网络中的假冒攻击是一种主动攻击形式，极大地威胁着传感器节点之间的协同工作。

（3）拒绝服务

一方面，物联网 ONS 以 DNS 技术为基础，ONS 同样也继承了 DNS 的安全隐患，例如 ONS 漏洞导致的拒绝服务攻击、利用 ONS 服务作为中间的攻击放大器去攻击其他节点或主机 ；另一方面，由于物联网中节点数量庞大，且以集群方式存在，因此会导致在数据传播时，由于大量机器的数据发送使网络拥塞，产生拒绝服务攻击。攻击者利用广播 Hello 信息，并利用通信机制中的优先级策略、虚假路由等协议漏洞同样可以产生拒绝服务攻击。

（4）篡改或泄漏标识数据

攻击者一方面可以通过破坏标签数据，使得物品服务不可使用；另一方面可以窃取或者

伪造标识数据，获得相关服务或者为进一步攻击做准备。通过向某个程序或者应用发送数据，产生非预期结果的攻击，通常为攻击者提供访问目标系统的权限。可以分为缓冲区溢出攻击、格式化字符串攻击、输入验证攻击等。一般情况下，向传感网络中的汇聚节点实施缓冲区的溢出攻击是非常容易的。

（5）权限提升攻击

攻击者通过协议漏洞或其他脆弱性使得某物品获取高级别服务，甚至控制物联网其他节点的运行。其中包括恶意代码的入侵，当恶意代码入侵成功之后，通过网络传播就变得很容易。它的传播性、隐蔽性、破坏性等和 TCP/IP 网络相比来说更难以防范，类似于蠕虫这样的恶意代码，本身也不需要有寄生文件，在这样的环境中检测和清除这样的恶意代码将非常困难。

（6）业务认证

传统的认证是区分不同层次的，网络层的认证就负责网络层的身份鉴别，业务层的认证就负责业务层的身份鉴别，两者独立存在。但是在物联网中，大多数情况下，机器都拥有专门的用途，因此，其业务应用与网络通信紧紧地绑在一起。由于网络层的认证是不可缺少的，那么其业务层的认证机制就不再是必需的，而是可以根据业务由谁来提供和业务的安全敏感程度来设计。例如，当物联网的业务由运营商提供时，那么就可以充分利用网络层认证的结果而不需要进行业务层的认证；当物联网的业务由第三方提供也无法从网络运营商处获得密钥等安全参数时，它就可以发起独立的业务认证而不用考虑网络层的认证；或者当业务是敏感业务时，一般业务提供者会不信任网络层的安全级别，而使用更高级别的安全保护，那么这个时候就需要做业务层的认证；而当业务是普通业务时，如气温采集业务等，业务提供者认为网络认证已经足够，那么就不再需要业务层的认证。

（7）隐私安全

在未来的物联网中，每个人及每件物品都将随时随地连接在这个网络上，随时随地被感知，在这种环境中如何确保信息的安全性和隐私性，防止个人信息、业务信息和财产丢失或被他人盗用，将是物联网推进过程中需要突破的重大障碍之一。如射频识别技术被应用于物联网时，RFID 标签嵌入在日常的生活用品中，用品的使用者在没有察觉的状态下，会不受控制地被扫描、定位和跟踪，这不仅涉及技术的问题，还会涉及相关的法律的问题。

3. 物联网的安全结构

物联网的层次结构决定了物联网安全机制的设计应当建立在各层技术特点和面临的安全挑战基础之上。物联网中，感知层实现监测物体标识和感知，网络层实现数据的处理和传输，应用层实现对网络层发送的信息的存储、挖掘、处理和应用。考虑到物联网安全的总体需求是物理安全、信息采集安全、信息传输安全和信息处理安全的综合，安全的最终目标是确保信息的机密性、完整性、真实性和网络的容错性，因此结合物联网分布式连接和管理（DCM）模式，物联网的安全层次应包括物理安全、信息采集安全、网络与信息系统安全、信息处理安全几个层次。物联网的安全层次结构如图 5-1 所示。

根据物联网的安全层次结构，下面结合每层安全特点对安全技术进行系统阐述。

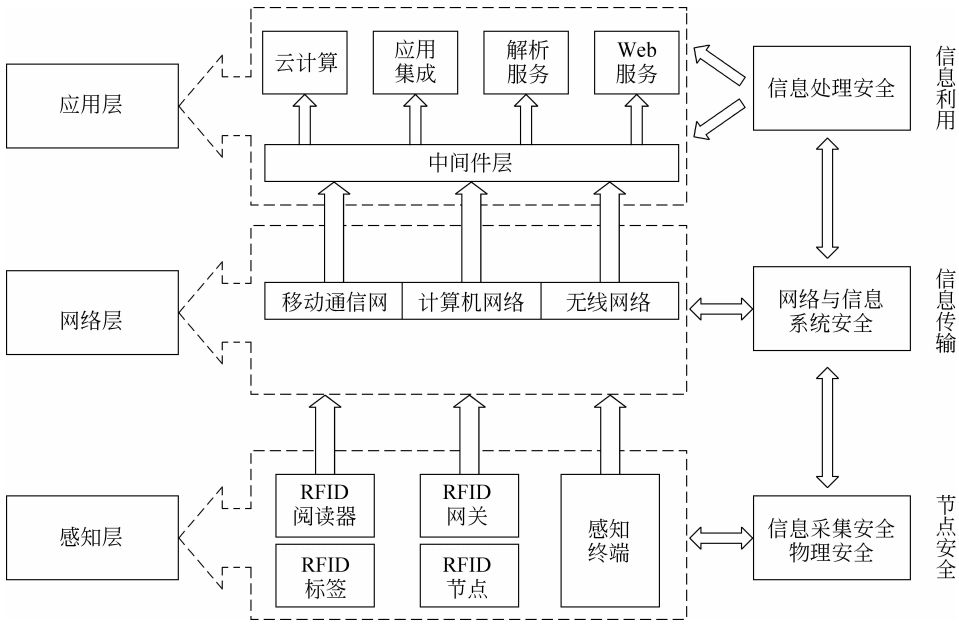

图 5-1　物联网安全层次结构

5.2　物联网感知层安全机制

物联网感知层的任务是实现智能感知外界信息，包括信息采集、捕获和物体识别，该层的典型设备包括 RFID 装置、各类传感器（如红外、超声、温度、湿度、速度等）、图像捕捉装置（摄像头）、全球定位系统（GPS）、激光扫描仪等，其涉及的关键技术包括传感器、RFID、自组织网络、短距离无线通信、低功耗路由等。

5.2.1　无线传感器网络安全机制

作为物联网的基础单元，传感器在物联网信息采集层面能否如愿以偿完成它的使命，成为物联网感知任务成败的关键。传感器技术是物联网技术的支撑、应用的支撑和未来泛在网的支撑。传感器感知了物体的信息，RFID 赋予它电子编码。传感网到物联网的演变是信息技术发展的阶段表征。传感技术利用传感器和多跳自组织网，协作地感知、采集网络覆盖区域中感知对象的信息，并发布给上层。由于传感网络是无线链路，具有比较脆弱，网络拓扑动态变化，节点计算能力、存储能力和能源有限，无线通信过程中易受到干扰等特点，使得传统的安全机制无法应用到传感网络中。传感技术的安全问题和防御方法如表 5-1 所示。

目前传感器网络安全技术主要包括基本安全框架、密钥分配、安全路由和入侵检测以及加密技术等。安全框架主要有 SPIN（包含 SNEP 和 uTESLA 两个安全协议）、Tiny Sec、参数化跳频、Lisp、LEAP 协议等。传感器网络的密钥分配主要倾向于采用随机预分配模型的密钥分配方案，安全路由技术常采用的是加入容侵策略等方法。

表 5-1　传感网络安全问题及防御方法

层　次	受到的攻击	防 御 方 法
物理层	物理破坏拥塞	物理防篡改、隐藏消息优先权、低占空比、区域映射
链路层	制造碰撞攻击、反馈伪造攻击、耗尽攻击链路层阻塞	纠错编码　MAC 请求速率限制(门限)
网络层	路由攻击、虫洞攻击、陷洞攻击、Hello 洪泛攻击	加密、使用冗余、探测机制出口过滤、认证监视
应用层	去同步　拒绝服务流等	客户端谜题、认证

1. 物理攻击防护

无线传感器网络(WSN)对抗物理攻击的一种方法是当它感觉到一个可能的攻击时实施自销毁,包括破坏所有的数据和密钥,这在拥有足够冗余信息的传感器网络中是一个切实可行的解决方案。关键在于发现物理攻击,一个简单的解决方案是定期进行邻居核查(对于静态分布的 WSN 有效)。LEAP 定义了一种有效的方法来剔除被敌方捕获的存储特定信息(如密钥)的传感器节点。

物理攻击可能通过手动微探针探测、激光切割、聚焦离子束操纵、短时脉冲波形干扰、能量分析等方法实现,相应的防护手段包括在任何可观察的反应和关键操作间加入随机时间延迟、设计多线程处理器在两个以上的执行线程间随机地执行指令、建立传感器自测试功能使得任何拆开传感器的企图都将导致整个器件功能的损坏、测试电路的结构破坏或失效。

2. 密钥管理

密码技术是提供机密性、完整性和真实性等安全服务的基本技术,但传感器网络有限的资源和无线通信特征决定了密钥管理的困难性。目前针对 WSN 提出的密钥管理机制主要有如下几点。

(1) 预置全局密钥,所有节点共享同一个密钥,这种方案简单、代价小,但安全性差。

(2) 预置节点对密钥,即网络中每对节点间共享一个不同的密钥,随着网络规模的扩大全网密钥总量将快速上升,且为新插入的节点分配共享密钥困难。

(3) 随机密钥预分配,每个节点的通信代价与网络的规模无关,但密钥存储量将随网络规模增大而线性增加。

(4) 基于密钥分发中心(KDC)的密钥分配,基站作为 KDC,每个节点与基站间共享一个不同的密钥,其他节点间的密钥基于基站来建立。但通信量较大,适用于小规模网络,并且 KDC 易受到威胁。

(5) 公钥密码体制,一般将消耗较多的存储空间和能量,实用性差。

LEAP 密钥管理协议支持为每个传感器节点建立 4 类密钥,包括基站共享的单个密钥、其他节点共享的对密钥、多个邻居节点共享的簇密钥及由网络中所有节点共享的群密钥。不同类型密钥的选用取决于节点与谁通信。传感器先装载一个初始密钥,基于该初始密钥生成其他密钥;为了防止传感器节点在受到攻击后威胁其他节点,初始密钥用完后将被删除。该协议是通信和能量高效的,且密钥管理过程最小化了基站的参与程度。

3. 节点攻击防护

认证是解决这类问题的有效方法。链路层安全体系结构 Tiny Sec 能够发现注入网络的非授权的数据包，提供消息认证和完整性、消息机密性、语义安全和重放保护等基本安全属性。Tiny Sec 支持认证加密和唯认证，前者加密数据载荷并用 MAC 认证数据包，对加密数据和数据包头一起计算 MAC；后者仅基于 MAC 认证数据包，并不加密数据载荷。

另外，认证和加密是阻止来源于传感器网络外部的 Sybil 攻击的有效方法，但对网络内部入侵者是无效的；对于内部攻击而言，可使每一个节点都和可信基站间共享一个不同的对称密钥，两个节点间可以基于它实现身份认证并建立其他的共享密钥。

4. 安全路由

WSN 的安全路由需要解决以下问题：建立低计算、低通信开销的认证机制以阻止攻击者基于泛洪节点执行 DoS 攻击、安全路由发现、路由维护、避免路由误操作和防止泛洪攻击。

SPIN 协议提供广播认证，基本思路是先广播一个通过对称密钥 K 生成的数据包，在一个确定的时间后发送方公布该密钥，接收方负责缓存这个数据包直到相应的密钥被公开，这使得在密钥被公布之前，没有人能够得到认证密钥的任何消息，也就没有办法在广播数据包正确认证之前伪造出正确的广播数据包；在密钥公开后，接收方能够认证该数据包，即通过延迟对称密钥的公开来取得与非对称密钥近似的效果。SPIN 适用于静态拓扑，且未解决网络流量分析等问题，一个改进的方案是用广播密钥链代替单播以减弱流量分析攻击，并提供了一种发现和去除有不正常行为节点的机制。

入侵容忍路由协议 INSENS 是为 WSN 安全路由提出的一个新方案，它的一个重要特点是允许恶意节点（包括误操作节点）威胁它周围的少量节点，但威胁被限制在一定范围内，用冗余机制的方法来解决。

5. 数据融合安全

有众多节点的无线传感器网络会产生大量原始冗余信息，数据融合是节省网络通信资源、减轻网络负荷的有效方法。一旦融合节点受到攻击，其最终得出的数据将是无效的，甚至是有害的，安全的数据融合十分必要。

融合—承诺—证实是一种安全数据融合方案，它由三个阶段组成。首先，融合节点从传感器节点收集原始数据并用特定的融合函数在本地生成融合结果，每一个传感器节点都和融合节点共享一个密钥，以便融合节点证实收到的数据是真实的。其次，融合节点对融合数据做出承诺，生成承诺标识（如基于 Merkle HASH 树结构），确保融合器提交数据后就不能再改变它，否则将被发现。融合节点向主服务器提交融合结果和承诺标识。最后，主服务器与融合节点基于交互式证明协议来证实结果的正确性。目前，安全数据融合方面的研究还不多，尚有大量的工作需要完成。

5.2.2　RFID 系统安全机制

如果说传感技术用来标识物体的动态属性，那么物联网中采用 RFID 标签则是对物体静态属性的标识，即构成物体感知的前提。RFID 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，识别工作无须人工干预。RFID 也是一种简单的无线系统，该系统用于控制、检测和跟踪物体，由一个询问器（或阅读器）和很多标签（或应答器）组成。

根据 RFID 的系统结构，RFID 的安全问题可以分为两类：一类是针对物联网系统中实体的威胁，主要是针对标签层、阅读器层和应用系统层的攻击，如表 5-2 所示；另一类是针对物联网中通信过程的威胁，包括射频通信层以及互联网层的通信威胁，如表 5-3 所示。

表 5-2　实体的主要威胁

对　象	攻击方式	描　　述
标签层	克隆攻击	复制或者伪造一个相同的 RFID 标签
	欺骗攻击	利用特殊硬件设施假冒合法的 RFID 标签获得访问权限
	非授权访问	攻击者在未授权的状态下读取 RFID 标签信息而不留痕迹
	拒绝服务攻击	给电子标签发送恶意请求信息，使标签无法响应合法请求
阅读器层	假冒攻击	攻击者假冒成合法的阅读器窃取或更改 RFID 标签的信息
应用系统层	隐私破坏	通过应用系统查询标签相关信息，实现对标签的主体跟踪
	拒绝服务攻击	伪造大量恶意请求，使得应用系统无法响应合法的请求

表 5-3　通信的主要威胁

通信信道	攻击方式	描　　述
射频通信层	窃听攻击	攻击者窃听阅读器到标签及标签到阅读器的通信信息
	重放攻击	充当中间人的角色，在合法阅读器及标签间重放通信信息
	篡改攻击	在合法的阅读器和标签间拦截或者修改正常的通信信息
互联网层	假冒攻击	这类攻击与传统意义上的互联网中的攻击基本一致，可以用现有的成熟的安全技术和密码机制来解决

目前，实现 RFID 安全性机制所采用的解决策略主要可以分为两大类：物理完全机制和安全认证机制。

1. 物理安全机制

使用物理方法来保护 RFID 系统安全性的方法主要有如下 5 类：封杀标签法（Kill Tag）、裁剪标签法（Sclipped Tag）、法拉第罩法（Faraday Cage）、主动干扰法（Active Interference）和阻塞标签法（Block Tag）。这些方法主要用于一些低成本的标签中，因为这类标签有严格的成本限制，因此难以采用复杂的密码机制来实现标签与读写器之间的通信安全。

（1）封杀标签法

封杀标签的方法是在物品被购买后，利用协议中的 kill 指令使标签失效，这是由标准化组织 Auto-ID Center 提出的方案。它可以完全杜绝物品的 ID 号被非法读取，但是该方法以牺牲 RFID 的性能为代价换取了隐私的保护，使得 RFID 的标签功能尽失，是不可逆的操作，如顾客需要退换商品时，则无法再次验证商品的信息。

（2）裁剪标签法

IBM 公司针对 RFID 的隐私问题，开发了一种“裁剪标签”技术，消费者能够将 RFID 天线扯掉或者刮除，大大缩短了标签的可读取范围，使标签不能被远端的阅读器随意读取。IBM 的裁剪标签法弥补了封杀标签法的短处，使得标签的读取距离缩短到 1～2 英寸，可以

防止攻击者在远处非法监听和跟踪标签。

（3）法拉第罩法

法拉第罩法根据电磁波屏蔽原理，采用金属丝网制成电磁波不能穿透的容器，用以放置带有 RFID 标签的物品。根据电磁场的理论，无线电波可以被由传导材料构成的容器所屏蔽。当我们将标签放入法拉第网罩内，可以阻止标签被扫描，被动标签接收不到信号不能获得能量，而主动标签不能将信号发射出去。利用法拉第网罩同时可以阻止隐私侵犯者的扫描。例如，当货币嵌入 RFID 标签以后，可以利用法拉第网罩原理，在钱包的周围裹上金属箔片，防止他人扫描得知身上所带的现金数量。此方法是一种初级的物理方法，比较适用于体积小的 RFID 物品的隐私保护。但如果此方法被滥用，还有可能成为商场盗窃的另一种手段。

这种方法的缺点是：在使用标签时又需要将标签从法拉第网罩中取出，这样就无法便利地使用标签；另外，如果要提供广泛的物联网服务，不能把标签一直屏蔽起来，更多时候需要让标签能够和阅读器自由通信。

（4）主动干扰法

主动干扰法使用某些特殊装置干扰 RFID 阅读器的扫描，破坏和抵制非法的读取过程。主动干扰无线电信号是另一种屏蔽标签的方法。标签用户可以通过一个设备主动广播无线电信号，用于阻止或破坏附近的 RFID 阅读器的操作。主动干扰法使用起来比较麻烦，需要特定的无线电信号发射装置，此方法可以用于装载货物的货车，在途中可以避免攻击者非法读取车中的信息。但主动干扰实现成本比较高，不便于操作，如果其使用频率与周围的通信系统相冲突，或者干扰功率没有严格的限制，则可能影响正常的无线电通信及相关通信设备的使用。

（5）阻塞标签法

阻塞标签法也称作 RSA 软阻塞器，内置在购物袋中的标签，在物品被购买之后，禁止阅读器去读取袋中所购货物上的标签。EPCglobal 第二代标准具有这项功能。阻塞标签法基于二进制数查询算法，它通过模拟标签 ID 的方式干扰算法的查询过程。阻塞标签可以模拟 RFID 标签中所有可能的 ID 集合，从而避免标签的真实 ID 被查询到。该方法也可以将模拟 ID 的范围定为二进制树的某子树，子树内的标签有固定的前缀，当阅读器查询 ID 的固定前缀时，阻塞标签不起作用。当查询到固定前缀的后面几位时，阻塞标签将阻碍查询过程。通过这种方式——选择性阻塞标签可以用于阻止阅读器查询具有任意固定前缀的标签。阻塞标签法可以有效地防止非法扫描，其最大的优点是 RFID 标签基本上不需用修改，也不用执行加解密运算，减少了标签的成本，而且阻塞标签的价格可以做到和普通标签价格相当，这使得阻塞标签可以作为一种有效的隐私保护工具。但是缺点是阻塞标签可以模拟多个标签存在的情况，攻击者可利用数量有限的阻塞标签向阅读器发动拒绝服务攻击。另外阻塞标签有其保护范围，超出隐私保护范围的标签是不能得到保护的。

2. 安全认证机制

由于各种物理安全机制存在着这样和那样的缺陷与不足，因此基于密码技术的安全机制更受到人们关注。严格的 RFID 安全机制应该能同时包括认证和加密两种功能。针对低端 RFID 系统，设计切实可行的阅读器与标签相互认证方案，是实现低成本 RFID 系统信息安全的重要途径。低成本 RFID 安全认证协议为了防止标签的伪造和标签内容的滥用，实

现 RFID 系统安全目标，必须在通信之前进行阅读器与标签之间的相互认证。由于低成本 RFID 标签中的硬件资源有限，一些高强度的对称加密（AES、DES 和 3DES）和公钥加密算法（RSA 和 ECC）难以在标签中实现。目前，国内外学者已经提出了许多针对低成本 RFID 的安全认证协议，但现有的大多数协议都存在着这样或那样的缺陷，未能在协议设计的复杂度和安全性上实现完美的结合。

一般来说，根据不同的安全性需求，考虑协议的复杂性和实现成本，将 RFID 系统中的安全认证协议分为三类，分别是重量级、中量级和轻量级协议。

重量级安全认证协议，一般被称为完善（Full-fledged）的安全认证协议。它基本使用完善和安全的加密方法，例如 DES、3DES、AES，甚至包括公钥加密方法 RSA 和 ECC。具有代表性的是用于电子护照且基于 ICAO（International Civil Aviation Organization）标准的 ICAO 认证协议，它采用 64 位密钥的双密钥 3DES 算法和消息认证码，具有很高的安全强度。但由于该类算法采用比较成熟的加密手段，标签的成本很难降低，所以往往只使用在对安全性要求较高的军事、安全和金融领域，低成本的 RFID 系统不适宜采用重量级的安全认证协议。

轻量级安全认证协议采用简单的位运算代替复杂的加密算法和杂凑运算。这些位运算包括或（OR）、异或（XOR）、与（AND）、非（NOT）和移位（Rot(x,y)）等。具有代表性的轻量级安全认证协议有轻量级强认证强完整性协议（Strong Authentication and Strong Integrity，SASI）和两消息互认证协议（Two-Message Mutual Authentication Protocol，T2MAP）。其中，T2MAP 协议仅需要两条消息，是所有 RFID 协议中使用消息数最小的认证协议。该协议规定在标签和读写器的内存中，保存相对应的标签 ID 和密钥。它几乎不需要加密电路，所以安全性也最差。由于轻量级协议主要考虑系统的成本，安全性能较差，因此主要应用于商品零售和物流跟踪等低端 RFID 系统中。

中量级认证协议使用具有一定安全强度和复杂度的杂凑运算，其安全性和复杂性介于重量级和轻量级协议之间。由于其兼顾了安全性和成本需求，已成为 RFID 领域研究的重点和热点。

下面介绍几种具有代表性的协议。

（1）哈希锁协议

哈希锁（Hash-Lock）是一个抵制标签未授权访问的隐私增强协议，2003 年由麻省理工学院和 Auto-ID Center 提出。整个协议只需要采用单向密码学哈希函数，实现简单的访问控制，因此可以保证较低的标签成本。

首先阅读器为标识号为 ID 的标签产生一个密钥 key，并计算 metaID＝Hash(key)，将 metaID 发送给标签；标签将 metaID 存储下来进入锁定状态。同时阅读器把（metaID，key，ID）存储到后台数据库中。在阅读器想询问标签信息时，阅读器向标签发送询问信息，标签回复 metaID 给阅读器，阅读器通过查询后台数据库，找到对应的（metaID，key，ID）记录，然后将 key 值发给标签；标签收到 key 后就计算 Hash(key)，并对比计算的 Hash 值是否与 metaID 相等，若相等，则标签把自身的 ID 值发送给阅读器，此时标签处于解锁状态，并允许阅读器读取它的信息。

为了避免信息泄漏和被追踪，Hash-Lock 协议使用 metaID（通过对标签密钥的杂凑运算获得）来代替标签的真实 ID。但由于 Hash-Lock 协议中没有 ID 动态刷新机制，并且 metaID 也保持不变，ID 是以明文的形式通过不安全的信道传送，因此 Hash-Lock 协议非常