1. 研究背景

无线传感器网络(Wireless Sensor Networks, WSN)是一种分布式传感网络，它的末梢是可以感知和检查外部世界的传感器。WSN中的传感器通过无线方式通信，因此网络设置灵活，设备位置可以随时更改，还可以跟互联网进行有线或无线方式的连接。通过无线通信方式形成的一个[多跳](https://baike.baidu.com/item/%E5%A4%9A%E8%B7%B3/5932947)[自组织网络](https://baike.baidu.com/item/%E8%87%AA%E7%BB%84%E7%BB%87%E7%BD%91%E7%BB%9C)。微电子技术、计算技术和无线通信等技术的进步，推动了低功耗多功能传感器的快速发展，使其在微小体积内能够集成信息采集、数据处理和无线通信等多种功能，在此背景下，无线传感器网络（WSN）成了近年来的一个研究热点。

1. 研究内容
2. WSN的安全需求

由于WSN使用无线通信，其[通信链路](https://baike.baidu.com/item/%E9%80%9A%E4%BF%A1%E9%93%BE%E8%B7%AF)不像有线网络一样可以做到私密可控。所以在设计传感器网络时，更要充分考虑信息安全问题。手机[SIM卡](https://baike.baidu.com/item/SIM%E5%8D%A1)等[智能卡](https://baike.baidu.com/item/%E6%99%BA%E8%83%BD%E5%8D%A1)，利用[公钥基础设施](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5%E5%9F%BA%E7%A1%80%E8%AE%BE%E6%96%BD)(Public Key Infrastructure, PKI)机制，基本满足了电信等行业对信息安全的需求。同样，亦可使用PKI来满足WSN在信息安全方面的需求。

(1) 数据机密性

数据机密性是重要的网络安全需求，要求所有敏感信息在[存储](https://baike.baidu.com/item/%E5%AD%98%E5%82%A8)和传输过程中都要保证其机密性，不得向任何非授权用户泄露信息的内容。

(2) [数据完整性](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%AE%8C%E6%95%B4%E6%80%A7)

有了机密性保证，攻击者可能无法获取信息的真实内容，但接收者并不能保证其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过程。通过[数据完整性](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%AE%8C%E6%95%B4%E6%80%A7)鉴别，可以确保数据传输过程中没有任何改变。

(3) 数据新鲜性

数据新鲜性问题是强调每次接收的数据都是发送方最新发送的数据，以此杜绝接收重复的信息。保证数据新鲜性的主要目的是防止重放(Replay)攻击。

(4) 可用性

可用性要求传感器网络能够随时按预先设定的工作方式向系统的合法用户提供信息访问服务，但攻击者可以通过伪造和信号干扰等方式使传感器网络处于部分或全部瘫痪状态，破坏系统的可用性，如拒绝服务(Denial of Service, DoS)攻击。

(5) 鲁棒性

无线传感器网络具有很强的动态性和不确定性，包括网络拓扑的变化、节点的消失或加入、面临各种威胁等，因此，无线传感器网络对各种安全攻击应具有较强的适应性，即使某次攻击行为得逞，该性能也能保障其影响最小化。

(6) [访问控制](https://baike.baidu.com/item/%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6)

[访问控制](https://baike.baidu.com/item/%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6)要求能够对访问无线传感器网络的用户身份进行确认，确保其合法性。

根据计算机网络层次的不同，无线传感器网络主要受到以下几种安全威胁：

（1）物理层：主要的攻击方法为拥塞攻击和物理破坏。

（2）链路层：主要的攻击方法为碰撞攻击、耗尽攻击和非公平竞争。

（3）网络层：主要的攻击方法为丢弃和贪婪破坏、方向误导攻击、黑洞攻击和汇聚节点攻击。

（4）传输层：主要的攻击方法为泛洪攻击和同步破坏攻击。