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。WSN自身的特点决定了其安全问题将有别于传统网络，其不可靠的无线通信信道又使得安全防范变得更加困难，而且WSN节点还必须能够检测、鉴别不可信节点和入侵者来保护自身安全，抵御各种类型的攻击，以保持整个系统的安全性和完整性。所有这些都要求WSN具有更高、更强的安全机制，来克服WSN在安全方面的弱点，以保证WSN在各个领域的渗透式应用。

1. 研究内容
2. WSN的安全需求

WSN具有和应用密切相关的特点，不同的应用有不同的安全需求，WSN的安全需求是设计有效安全架构的根本依据。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。无线传感器网络的密钥管理系统的设计在很大程度上受到其自身特征的限制，因此在设计需求上与有线网络和传统的资源不受限制的无线网络有所不同，要特别充分考虑到无线传感器网络传感节点的限制和网络组网与路由的特征。它的安全需求主要体现在以下几个方面。

(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。

1. WSN的中的密码技术

WSN的链路层安全策略的轻量化研究适合于各种应用环境的WSN系统，结合序列密码和分组密码各自的优势，提出了一种新型轻量的WSN链路层加密算法——TinySBSec。

TinyOS是一个基于组件（component-based）的开源操作系统，由UC Berkeley（加州大学伯克利分校）开发，专为存储器受限制的WSN设计。TinySec则同样是UC Berkeley为WSN开发设计的一款可运行于TinyOS的WSN链路加密协议。

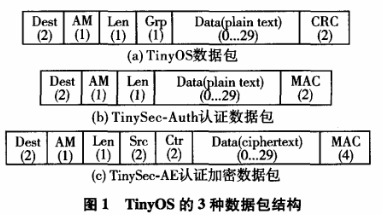
该协议采用的是对称分组密码，加密算法可以是RC5或是Skipjack算法。其加密算法的工作模式为CBC模式，是一种拥有反馈机制的工作模式。每组密文不仅依赖于其明文，也依赖于上一密文分组(第1组密文依赖于初始向量IV)。

CBC模式的数学语言表示如下：



CBC模式能增加攻击者篡改消息的难度，以尽可能简单的运算，达到一定的安全性能，而且并不会增加太多额外的能量损耗。正是基于这一优点，其他的一些WSN链路层加密协议，如WSNSec和Con-tikiSec也使用CBC工作模式。

TinyOS的链路层协议有3种数据包结构：Tiny．OS packet format、TinySec-Auth packet format和Ti-nySec.AE packet formato其中TinyOS packet format是TinyOS默认的数据包结构，没有加密和MAC(消息认证码)，只有CRC检验数据的完整性；TinySec-Auth是只带MAC认证的数据包结构，Data是未加密的明文；TinySec-AE则是既有MAC认证，同时Data也被加密保护的数据包结构。3种数据包结构如图l所示。



TinySec采用的RC5和Skipjack加密算法、CBG-MAC以及CBC密码工作模式都没有明显的漏洞，且对资源的占用也控制的较好，是专为WSN量身定做的最合适的链路层加密协议。