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。

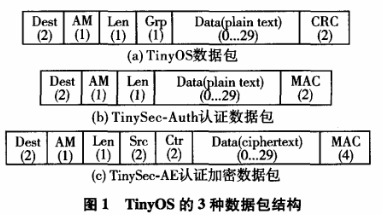
该协议采用的是对称分组密码，加密算法可以是RC5或是Skipjack算法。其加密算法的工作模式为CBC模式，是一种拥有反馈机制的工作模式。每组密文不仅依赖于其明文，也依赖于上一密文分组(第1组密文依赖于初始向量IV)。

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，是一种非常适合WSN的链路层加密协议。

1. WSN中的密钥管理技术

密钥管理是传感器网络安全的基础。近年来，无线传感器网络的密钥管理研究已经取得了很大的进步，目前应用最多的密钥管理方案有：

1. 共享密钥预分配

为了为无线传感器网络中邻居节点之间通信的安全，可在网络节点上预先储存 所有节点之间的会话密钥，如网络规模为 n 的，则需要的密钥总数为 C2 n，每个节点 需要储存（n-1）个密钥。两个节点之间可以直接使用预共享的密钥进行加密通信。显然这种方案不需要依赖基站，计算复杂度较低，因为任何两个节点间共享的密钥是独有的，所以当某一节点被俘获后也不会其他节点的密钥信息。但是这种方法对于节点存储能力要求比较高，对网络的扩展性也不好，已部署的网络已分配了密钥，使得新增节点难以加入网络。无线传感器网络中，普通节点也可与基站共享一对主密钥，这样每个节点对储存空间的要求就比较小，使密钥计算和储存全在基站中进行。这种密钥管理方案对于收集型网络非常有效，因为所有节点都是跟汇聚节点进行通信。但其对于多跳网络并没有防御DoS攻击的能力，另外如果基站被俘获整个网络的安全信息都会受到破坏。

1. 随机密钥预分配

基本的随机密钥分配方案目的是在保证任意节点间通信安全的前提下，尽可能的减少对节点资源的要求。其基本思想是在节点部署前，所有节点随机从一个很大的对称密钥池中选取n个密钥作为节点的密钥环，并预先储存在节点上。密钥环的大小要保证两个都拥有n个密钥的节点有相同的密钥的概率大于预先设定的概率p，节点间相同的密钥称之为共享密钥。在节点部署后，邻居节点之间要通信就通过广播自己密钥环中所有密钥的ID，寻找和自己有相同密钥的节点，利用其共享密钥进行会话加密，保障其通信安全。这种方案也可能存在一个或多个和它周围的节点之间没有共享密钥，使其成为了孤立节点。为了解决随机密钥分配中孤立节点问题可以增加网络节点部署密度，也可增加节点通信信号传输功率，从而增大其通信半径，使其能找到更多的邻居节点。基于密钥池预分配的特点是使得节点能够与邻居建立安全链路，很大程度的降低了节点需要的存储量，但是由于节点可能存在相同的共享密钥，单个节点被攻击可能网络中其他节点的不安全。

1. 基于q-composite随机密钥预分配

在随机密钥预分配基本模型中，任何两个邻居节点的密钥环中至少有一个共享密钥，为了提高网络的抵抗力，要求传感器节点之间共享至少q个密钥。此时网络被攻击的难度与共享密钥个数q就成指数关系。从而增加了网络的安全性。 q-composite随机密钥预分配方案中要想使网络中任意两个节点间的安全连通 度超过q，就必须要缩小密钥池的大小，增加节点间共享密钥的重复度，这种情况带来缺点是，密钥池减小，节点间共享密钥的个数增加，就会是攻击在俘获少量节 点后就能获得很大的密钥空间，所以寻找一个最佳的密钥次规模是保证安全值得关键。

q-composite随机密钥预分配和随机密钥基本分配模型的过程类似，只是要求邻居节点共享密钥数大于q，如果两个相邻节点间共享密钥数超过q, 则利用所有超过q的密钥生成一个密钥K，K=hash(K1||K2||…||Kq), 作为两个节点之间的共享密钥。这样两个节点就会计算出相同的通信密钥。

1. 基于EBS随机密钥预分配

EBS(exclusion basis systems)主要用于密钥动态管理,其有两种密钥：管理密钥和会话密钥。管理密钥又称为密钥生成密钥，但并不直接用于通信数据的加密，而是用于EBS内部的密钥事件，包括密钥系统的建立和更新、生成会话密钥、驱逐节点等。会话密钥称为通信密钥，当EBS系统建立后，会在线的生成会话密钥，用于组内或某些特殊节点的通信数据加密。

EBS为一个三元组（n，k,m）表示的集合，n表示节点数，k为分配给每个节点的管理密钥个数，m为密钥更新的信息数。对于任意一用户，做多有k个密钥，m个密钥子集。

在 EBS中最多广播m个数据包，就可以取消并更新任意节点拥有的全部管理密钥，从而把该节点驱逐出网络。

1. WSN中路由安全

无线传感器网络路由面临各种特殊威胁，安全路由技术成为无线传感器网络的重点研究方向。无线传感器网络技术中有许多路由协议，但这些路由协议主要考虑的能耗和效率的问题，并没有涉及到安全的问题。敌人很容易对网络路由协议进行攻击，如伪造路由信息等，这就使得网络无法正确、可靠的将信息传送到目的节点。另一方面，无线传感器网络路由设计的重要目标是降低节点能源损耗，提高网络生命周期。路由信息被篡改会使节点能量消耗增大，从而缩短网络寿命。而且，增加安全机制也将增大节点能量消耗，使得安全路由协议的设计更为复杂。因此，研究一种高效的安全路由技术，不但能够防御各种攻击和威胁，而且适用于无线传感器网络的特点，是一项十分具有挑战性的任务。

增加路由协议的安全性主要采用消息加密、身份认证、路由信息广播认证、入侵检测等机制来保证信息的完整和准确性。针对确认欺骗、虚假路由信息等攻击，复旦大学的Yin Changqing等人设计了关于直径的路由协议并增加安全机制，提出了关于直径的启发式安全路由SRD。该协议设计思想是首先以源节点A为中心，以r跳数为半径做圆，寻找最小距离的节点B，然后再以B为圆心做圆，以此下去，最终寻找到目的节点D。在此基础上，考虑能量有限问题，将To2kens代替公钥而采取认证和加密机制。该协议以数字签名和密钥管理作为路由安全机制的方法，把计算复杂的能量消耗来代替通信复杂的能量消耗，在尽量保证网络生命期不减弱的情况下，增加了安全机制。但是计算量大，同时，所有节点都在直径范围内进行广播自己的路由信息，使得能量浪费。

其他的一些路由协议一般采用链路层加密和认证、多路径路由、身份认证、双向连接认证和认证广播等机制来有效抵御虚假路由信息、Sybil攻击和Hello flood攻击。无论哪种路由协议，都在复杂性、能量损耗和安全性等方面难以平衡，一般都侧重于强化某些性能，而以牺牲其他性能为代价。一些安全路由协议是在现有的路由协议基础上增加了安全机制，使得在设计上增加了成本。

1. 总结