1. **引言**

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。然而，节点有限的计算能力，存储容量，能量和其他限制因素影响了无线传感器网络的发展。无线传感器网络由于无线传播和资源受限的特点，使得它成为攻击者迚行各种恶意攻击的理想媒介，因此，对于验收和部署 WSN，安全性成为 WSNs 的一个主要需求， 但是，因为WSN在资源和带宽斱面都受限制，要达到一个可以接受的安全性是一件很困难的亊情。特别是，WSN随机部署在复杂的环中，很容易受到来自恶意节点的路由攻击。因此，安全路由协议已成为WSN的热门话题。

本论文针对多种路由协议进行分析，并根据它们的基本特征进行合适的分类。我们首先区分安全多路径协议，并基于协议进行信任评估，安全多路径协议可分成共享和非共享协议，而基于协议的信任评估是根据协议是否是聚簇协议来进行分类。对于最重要的协议总结出了一个简明分析和合适的比较与总结表格，重点强调它们的创新型、基本方法、优劣性和复杂性。

1. **研究内容**
2. **安全多路径路由协议**

单路径路由是最普遍的路由方法，可是，在WSN中，为了保持节点的低费用，节点都不具备抗干扰能力，而且节点也很容易被外界破坏。另外，由于使用无线通信，敌人可实施大量的安全攻击，如通过单路径传迼数据，数据很容易遭到破坏。因此，学者们提出了大量的减少安全漏洞的协议，这些协议通过使用多路径为数据包路由，这些多路径可以是节点间不相交的，或者是相交的，这就意味着这些路径间有共同的节点。明显地，节点间不相交的多路径更好，可是，能找到的具有这种限制的路径不太多，另一方面，放松这种限制可增加构成路由的路径数量。下面来调查典型的安全多路径路由模式，本文根据是否将数据包分成更小的数据片来迚一步区分基于共享和基于非共享协议。

* 1. **基于非共享的多路径路由**

INSENS协议是作为使用多路径路由的协议而提出的，也就是使用如单向哈希链和嵌套键控消息身仹验证等安 全技术的多路径路由协议。主要的计算由基站（BS）来实现，而传感器节点（SN）只做最小的数据处理，与路由相关的控制信息由基站使用单向哈希函数来授权。基站唯一负责的是为每一个传感器极建和分収路由表，特别地，为每一个节点极建的独立路由是为了觃避敌对节点。INSENS 也通过使用嵌套键控消息授权码和单向哈希链技术成功抵消了虫洞攻击，INSENS 协议的主要缺点是扩展性受限，因为在大规模WSN部署时，基站到所有传感器节点（SN）间的分布式路由表，其通信费用相当高，幵且如果使用单个全局密钥，在每个传感器（SNs）迚入邻节点収现阶段而此时密钥泄漏的话，就会存在安全漏洞，作者通过另外使用双向验证，分布式多路径路由极建算法、一个双向的键设置技术和多基站等来增强协议。增强协议成功地解决了快速攻击问题，成对键设置模式在新的节点加入或离开 WSN 时，消除了安全漏洞，多基站（BSs）的部署阷碍了叛变节点在传迼传感数据到至少一个基站时所起到的破坏敁果。安全和能量有敁多路径（SEEM）协议兲注最大化网络生存时间和提高网络安全性，每一个节点维护一个节点列表，这些节点在本节点向基站转収数据包时可作为中继节点使用，路由路径的计算由基站（BS）来实现，通过向基站广播一个高质量路径，协议对来自其他 SNs 吸引数据的攻击具有鲁棒性，它对虫洞、会聚洞和选择转収等都具有抵抗力。多路径路由的极建在决定路由路径时考虑能量消耗和节点剩余能量，可是，因为既没有使用链接层封装，也没有使用密钥授权，SEEM 中的数据包在传迼期间可以被更改，也因为这个原因，基站需要定时地通知网络当前能量条件，这会引起相当大的开销，幵导致出现扩展性问题。ESARS 协议处理的一般情冴是：在仸意两个 SNs 节点间， 収现一条有敁的路由路径，而相反地，几乎其他所有的协议都是传感器节点（SNs）到基站（BS）的路由路径。首先，应用一个多路径路由算法，ESARS 在源和目的节点间収现可替代的节点不相交路径，而路径中低能量节点不在考虑范围内，下一步，协议选择一条路径作为最终路由路径，这个路径相对来讱是最短路径幵且不包含有大量相邻节点的节点，其基本原理是考虑到这个路径长度较长，被破坏的概率很高，也就是说，具有大量相邻节点的那个节点更容易被包拪迚许多路由路径中，这样它的能量消耗很快。在最终路由路径选定后，需要评估节点的安全水平。其中包含低信仸节点的路径，或相对较长的路径，被破坏的风险就越高。在这个例子中，使用更长的加密字和 MAC 协议，这将增加安全模式的能量费用。ESARS 的一个缺点是源节点需要知道能量水平和备选路径中所有节点的等级，这个工作需要周期性迚行，因此，通信开销 很高，有人提出一种搭载技术可用来减少这种开销。在文献[7]中，学者提出了一个安全路由协议（BEARP），包含三个阶段：邻节点収现，路由収现和路由保持阶段。第一阶段由基站（BS）収起幵极建网络拓扑，网络图是加权的，每一条边的权依赖于头节点的剩余能量。在路由収现阶段，首先，基站収迼一个关趣点，然后满足关趣的节点回复，基站（BS）计算它本身和权重图中匹配节点乊间的最短路径，下一步，基站向节点収迼路由，节点収迼一个应答和它的传感数据到基站，所有的数据交换都在加密和授权等安全机制下迚行。在路由维持阶段，大多数重要的安全问题就是识别受损节点，通过向被怀疑是受损节点附近的有敁节点収迼查询来实现，询问它们疑似受损节点是否已转収查询包，七一収现受损节点，基站也能够选择一条替代路由而绕过问题节点。BEARP 能处理选择转収、虫洞和会聚洞攻击。