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，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发路由表，特别地，为每一个节点构建的独立路由是为了规避敌对节点。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，并且如果使用单个全局密钥，在每个传感器（SN）进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，分布式多路径路由构建算法、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）的部署阻碍了叛变节点在传送传感数据到至少一个基站时所起到的破坏效果。

安全和能量有效多路径（SEEM）协议关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发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SN吸引数据的攻击具有鲁棒性，它对虫洞、会聚洞和选择转发等都具有抵抗力。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中的数据包在传送期间可以被更改，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 协议处理的一般情况是：在任意两个SN节点间， 发现一条有效的路由路径，而相反地，几乎其他所有的协议都是传感器节点（SN）到基站（BS）的路由路径。首先，应用一个多路径路由算法，ESARS在源和目的节点间发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，这个路径相对来讲是最短路径并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括进许多路由路径中，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。其中包含低信任节点的路径，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进行，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。安全路由协议BEARP，包含三个阶段：邻节点发现，路由发现和路由保持阶段。第一阶段由基站（BS）収起并构建网络拓扑，网络图是加权的，每一条边的权依赖于头节点的剩余能量。在路由发现阶段，首先，基站发送一个兴趣点，然后满足兴趣的节点回复，基站（BS）计算它本身和权重图中匹配节点之间的最短路径，下一步，基站向节点发送路由，节点发送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进行。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效节点发送查询来实现，询问它们疑似受损节点是否已转发查询包，万一发现受损节点，基站也能够选择一条替代路由而绕过问题节点。BEARP能处理选择转发、虫洞和会聚洞攻击。

* 1. **基于共享的多路径路由**

H-SPREAD协议提出了安全性和可靠性问题。H-SPREAD协议使用一个分布式的N到1多路径发现协议，这个协议能发现从传感节点SN到基站BS之间的多条节点不相交路径，这个多路径数据分散技术与一个秘密共享方案相结合，这样，当 WSN中只有少量的受损传感器节点时，H-SPREAD协议能成功地将传感器SN的数据交付给基站BS。特别地，在一个秘密共享方案中，使用一个（T，M）阈值秘密共享机制；每一个数据包被分成 M 份共享数据，然后，这些共享数据都被独立地发送到基站（BS），只要至少T份共享数据到达基站（BS），原数据包就可以被恢复。多路径发现协议由两个阶段组成，第一阶段，根据网络密度，发现一定数量的节点不相交路径，第二阶段，由第一阶段中决定的节点不相交路径在节点中相互交换，这些节点是属于到根节点基站（BS）的不同分支，这样，在第二阶段后，每一个节点比第一阶段学习到更多节点不相交路径，但是，在信息交换中费用也更高。

有研究者提出了一个基于秘密共享和一个分散路由协议模式，每一个共享路由由每一跳的飞行决定，利用随机选择的下一个节点转发数据包，这样，虽然路由路径并不是不相交的， 但在这条路径中随机选择转发节点，用这种方法，在共享路径上实现了较好的空间抑制性。多播辅助树随机传播路由方法，多播树根是建在基站BS上，然后这棵树用于指示转发共享数据。这个随机转发用到若干次，然后共享数据通过一条最短路径路由，可以仍最后访问的节点发送至基站BS，利用随机协议的主要好处是，对手不可能事先知道共享数据所跟随的路由路径，这样它也不可能通过叛变的特殊节点来安排它的攻击。

另一个组合了一个秘密共享方案的随机分散路由协议是SEDR协议。SEDR协议的主要目标是最大化网络生存时间，同时能成功地抵御黑洞攻击。它包含三个阶段，首先，源数据包的共享被发送到源节点周边地区随机选中的传感器节点，在第二阶段，每一个共享仍第一阶段中选出来的节点发送至另外一个具有目的地限制的节点，也就是选择路由的所有中间节点都和路由中的开始节点一样，与基站间有相同的跳数，然后，在第三阶段，每一个共享跟随指向基站的最短路径发送至基站。通过在网络上分散数据包，协议实现了更好的节点剩余能量利用，在网络中避免了热点，协议成功地解决了黑洞攻击问题。

对于增强的H-SPREAD协议，提供了更多的备用路由路径和确保路由构建的设置阶段，提出的子分支多路由协议SMRP，仍每个节点到基站（BS）都构建了备用路由，要求这些路由中的每一条必须通过路由到基站的路由树中的不同分支，根在这些节点的子树被称作分支。本质上，生成的路由允许通过根相同的子节点，与基站（BS）相邻的节点都被很好地监控，这些节点叛变的风险相对较低。而对于SEIF协议，这是 SMRP协议的安全版本，SEIF是基于单向哈希链技术，提供发送者对所有交换控制信息的授权，这样，对手就不能模仿路由树中节点的父节点或通过模仿基站重新开始构建新一轮数据，不能让入侵者代表基站伪造有效的子分支标记，但 SEIF不能侦测虫洞攻击，也没有考虑如何评估不同路由路径的费用问题。

1. **安全多路径路由协议**
   1. **基于共享的多路径路由**

有研究者提出了一个带有摘要信息验证的信任感知路由模式TAIV，可以提供传感器节点间的安全路由，TAIV和以前模式之间的主要差别是TAIV模式的特征是两条不相交的路由路径：骨干路由路径和辅助路由路径，第一条是用于发送数据包，第二条用于传送验证信息。在上面的情境中，应用了一种典型的基于信任路由方法，这种方法与一个连接控制集结构相结合，不仅提高了在低费用时的网络路由安全性，而且也可以判断恶意节点的位置，可是提出的解决方案只能处理黑洞攻击，对其他攻击不能防御，也由于它的内部结构（主干路由路径，连接控制集），它很难适应基于簇的无线传感器网络（WSN）。在文献《A trust aware routing protocol for energy constrained wireless sensor network》中，提出了一个新的信任感知路由（TERP），TERP协议将能量意识特征并入路由设置阶段，在信任评估阶段就能够动态地侦测和隔离行为异常节点，这可以更好地帮助信任节点之间进行负载均衡。TERP使用组合路由函数，决策是基于信任，能量和跳数计算。一个改进的路由维护机制是基于监控到的拥塞程度，智能地评估链接状态，可是，提出的协议假设恶意节点之间没有勾结，也就是在网络建立之后不允许添加或移除节点。这种假设是不现实的，并且限制了TERP协议应用的扩展。为了建立一个能处理各种敌对攻击的信任模型，文献《A trust-aware secure routing framework in wireless sensor networks》的作者提出了一个称作为 TSRF（信任感知安全路由框架）的集成框架。他们首先分析了在信任感知路由协议中的攻击，提出了特殊的信任计算和信任引出模型来处理这些攻击，而且进一步设计了一个优化路由算法，这个算法不仅考虑信任度量标准的特征，而且考虑路径选择的服务质量（QoS）要求，同时总路由开销很低。尽管以上各步在安全增强上是有效的，但在路由决策时幵没有考虑节点的能量。

* 1. **基于簇的信任感知路由**

在基于簇的 WSN中，将一个敌对节点或叛变节点选为簇头（CH）是对网络最重大的破坏。在文献《Trust based LEACH protocol for wireless sensor networks，Proceedings of the 2nd International Conference on Future Generation Communication and Networking》中提出了基于信任的LEACH（TLEACH）协议，目的是增强 LEACH 协议的安全性。TLEACH 关注的是阻止叛变节点成为簇头（CHs），它包括信任管理模块，利用直接的观察也就是一个信任信息交换机制来构建和维护相邻传感器节点间的信任信息，而基于信任的路由模块是原 LEACH协议的修改版本，组合了一个基于信任的决策模块，虽然协议对敌对节点的攻击具有鲁棒性，但它对串谋攻击也是脆弱的。

研究者提出了RATCT、TEESR、TROM协议。

RATCT是一个基于信任值核心树的路由算法，目的是构建一个安全簇结构，并延长WSN的生存时间，具有更高信任水平的节点和更多剩余能量的节点被选作簇头（CHs），所有的簇头组织成一棵信任值核心树，会聚sink 节点是根节点，然后核心树扩展覆盖所有节点，一个信任模型用于评估节点的信任水平并侦测节点的敌对行为，每一个节点保持一对公共和私有的密钥来加密和签署需传送的数据包，会聚节点通过分析加密和数据包标签来侦测敌对行为，信仸模型能有敁地侦测敌对行为，但它使用了一个要求额外能量的集中方法来构建核心树和计算信任值。

TEESR是一个基于信任的能量有效安全路由协议，它使用合适的授权和泛洪机制来限制邻近的敌对节点，基于节点信任值的使用，建立一个覆盖区域的网络和多路径安全路由，簇头（CHs）和会聚（sink）节点选择安全路由，虽然协议能应对会聚洞和虫洞攻击，但对内部攻击无能为力。

多属性信任感知路由协议（TRPM），协议的信任管理模型合并通信、数据、能量，并包含信任评估属性和一个具有测量攻击频率功能的滑动时间窗，TRPM在处理各类路由目标和信任目标攻击时表现出很好的性能，协议并不合并一个信任感知簇头（CH）选择模式。

1. **总结**

本文针对多种安全路由协议进行调查，根据它们的基本特征进行合适的分类。最初大量的研究工作只考虑安全多路径协议，可是，由于WSN在资源分配中的限制（有限的硬件资源和更高的通信费用，增加的能量消耗等）导致最近十几年都评估基于信任的路由协议，而且，最近五年研究者的工作主要向着下面两个基本方向来提高效果：（1）现代WSN基于簇的结构合并基于信任的路由协议的效率；（2）合适的组合模式等，如何提高效率和有效地组合（简单的限制多路径逻辑的基于信任路由方案）。