术在收集信息的过程中将每一个用户的信息都进行了划分，每个人只能通过自己设置的密码获取信息，而不能获取一些涉及他人隐私或者单位的机密信息。

3.3 进行安全的认证

安全认证是指用户在信息的传输过程中通过原来设置密码所涉及的信息或者第三方所发出的验证消息进行验证，获取信息的方式。通过验证，可以有效提高信息的安全性。例如，在存储信息的过程中要设置密码，而密码的设置可能包括电话号码等一些基本信息，再次查找信息的过程中计算机代理方会给手机发送验证码，而这个验证码就代表了用户的身份，在建立计算机实验室网络安全的过程中应该对每个进入工作系统的人员设置相应的身份验证，例如人脸识别等。

3.4 做好安全的防护工作

计算机实验室网络安全防护工作主要包括病毒的防护技术与防火墙技术。

（1）病毒的防护工作

通常情况下，面对病毒的入侵一般采用主动分析病毒的手段，从而对病毒进行拦截，对于云计算技术下常见的木马病毒要利用软件对网络故障进行检测，针对木马病毒破坏区域网的特点要及时检查主机的 IP 地址与 MAC 地址是否在同一种状态下，当发现网络无法运行时就需要对计算机实验室网络整体环境进行分析，并利用相关的软件进行杀毒。

（2）防火墙技术

在计算机网络系统里最主要的防护工作都是由防火墙担任的，当前的防火墙技术主要有两点：第一，检测技术，利用检测技术的时候要选择相应的参照标准，检测技术主要检测数据链路层和网络层；第二，Web 智能技术，这种技术被广泛应用在网络安全的维护中，通过与防火墙进行快速的对接，检测数据的进出以保证系统的安全。

4 结束语

建立安全的计算机实验室网络系统不仅仅是某个行业的工作，应该要利用社会各个阶层的优势。在维护计算机实验室网络安全的过程中要对计算机网络系统进行全面的布控，要将主要矛盾和次要矛盾进行充分的结合。最后，也是最为重要的一点要加强宣传，让越来越多的人了解计算机网络安全的知识。

参考文献：

[1]胡章君.基于云计算的计算机实验室网络安全技术探究[J].电脑知识与技术，2018，14（01）：63-64.

[2]杨巍.云计算下的计算机实验室网络安全技术分析[J].网络安全技术与应用，2017（12）：91+96.

[3]笪奇.计算机实验室的网络优化与维护探析[J].时代农机，2017，44（10）：207.

[4]胡江伟.基于云计算的计算机实验室网络安全技术探究[J].电脑编程技巧与维护，2017（20）：92-94.

[5]邱慕涛.基于云计算的计算机实验室网络安全技术应用探讨[J].中国管理信息化，2017，20（18）：148-149.

无线传感器网络中的安全和信任感知路由

◆施裕琴

（江苏省徐州医药高等职业学校　江苏　221116）

摘要：无线传感器网络（WSNs）在通信、计算和延迟方面的诸多限制，容易受到许多安全威胁的困扰，但传统的安全机制并不适用于无线传感器网络。因此，过去的十年间，有学者提出了许多安全路由方法，并建议将信任管理模型和相应的路由协议作为无线传感器网络（WSNs）的一个更为有效的安全机制。本文根据这类路由协议的基本特征进行适当的分类，并展开详细的调查，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。本文通过对许多重要协议间的比较，作出综合分析，并得出相应的结论，本文重点强调各协议的创新性，其基本理论和所面临的攻击和协议复杂性。

关键词：无线传感器网络；安全路由；基于信任路由；信任模型；多路径路由

无线传感器网络（WSNs）与现实世界的各种应用相比是一门快速发展的技术[1]，但无线传感器网络由于无线传播和资源受限的特点，使得它成为攻击者进行各种恶意攻击的理想媒介，因此，对于验收和部署 WSNs，安全性成为 WSNs 的一个主要需求，但是，因为 WSNs 在资源和带宽方面都受限制，要达到一个可以接受的安全性是一件很困难的事情。学者们提出各种安全机制（授权、机密性、信息完整性、密码技术等）以避免如窃听、信息重放和伪造信息等安全威胁。可是，这些方法虽然对外部攻击有效，但不能充分防御网络内部攻击，为了在 WSNs 内建立安全通信和保证关键数据的安全交换，必须确保 WSNs 内所有的通信节点是可信的。

单路径路由是一个简单路由协议，但很容易被攻击者阻塞，因此，最自然的方法是经多路径路由[2-3]，在各种情况下，即使多条路由中有一些路由受到攻击，数据仍然可以安全地到达目的地[4-11]。安全多路径路由根据数据包是否分成多个共享来进一步区分各类路由。

另一种避免攻击和提高路由成功率的常用方法是信任路由。每一个节点主要根据该节点的转发历史维持一个信任值，只有那些具有高信任值的节点才被选中参与路由。目前已经存在的主要为专用网络和点对点网络设计的信任管理技术，因为需要 WSNs 具有更高的节点资源消耗如存储器和功率消耗，而不适合 WSNs，因此，最近几年学者们为 WSNs 提出了许多新的信任管理技术和相关路由协议[12-28]，而且，为了节约能量和提高安全性，现在大多数的 WSNs 组织成簇，因此，为了比较安全性能和效率，需要分别研究基于簇的和不基于簇（平面的）的信任路由协议，在文献[1]中可找到基于信任协议的比较早期的调查。

本论文提出一个有关安全/信任感知路由协议调查，也就是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，也就是相关的讨论和结论。重点强调它们的创新性、基本方法、优劣性和复杂性。而且，本文的工作也可以看作是文献[1]调查的更新。

1 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 WSNs 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[2]。另外，由于使用无线通信，敌人可实施大量的安全攻击，如通过单路径传送数据，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[3]。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进一步区分基于共享和基于非共享协议。

1.1 基于非共享的多路径路由

在文献[4]中，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份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（SNs）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构建和分发路由表，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 WSNs 部署时，基站到所有传感器节点（SNs）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（SNs）进入邻节点发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[5]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 SNs 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。多路径路由的构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，并导致出现扩展性问题。

ESARS 协议[6]处理的一般情况是：在任意两个 SNs 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（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。

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：邻节点发现，路由发现和路由保持阶段。第一阶段由基站（BS）发起并构建网络拓扑，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。

1.2 基于共享的多路径路由

在文献[8]中，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 SNs 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 SNs 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。

文献[9]的作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。文献提出的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，可以从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，由文献[10]提出。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，每一个共享从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。

在文献[11]中，提出了一个增强的 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），从每个节点到基站（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，但作者作出有效的假设，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。然后提出 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。

2 基于信任的路由协议

在文献中最早有信任感知的路由协议（如 T-RGR 和 EMPIRE[12-13]），是基于以前已存在的协议，以适当的方式处理信任因素，其他几个基于信誉的信任路由模式（如 ERRM，TCLM，TARF 和 SETM[14-18]）以更综合的方式开发合并多个属性。这些更早的协议在文献[1]中有很好的概述。下面，本文关注该领域中最近的工作，强调它们的创新性和优缺点。

2.1 非聚簇信任感知路由

在文献[19]中，作者提出了一个基于主动信任的能量有效安全路由模型（主动信任），这个模型在侦测黑洞攻击中表现良好。主动信任是第一个路由模式，使用主动侦测路由防止黑洞攻击。通过充分使用远端会聚区域的能量，启动探查多条高信任路由。相应地，在数据实际路由前，节点当前的信任值可以得到，也可以避免黑洞。主要的性能指标如：主动信任值，能量效率，网络生存时间，路由成功率和有效性，证明都比以前已存在的那些策略要强。可是，模型在信任评估过程中只考虑了黑洞攻击，并没有防御其他攻击，它也只能用于节点和会聚节点之间的路由，并不能应用于传感器节点之间的通信。

在文献[20]中，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（WSNs）。在文献[21]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[22]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，但在路由决策时并没有考虑节点的能量。

表 1 非聚簇信任感知路由协议

协议	方法	信任值	优点	局限性	攻击
ACTIVE TRUST[19]	多条探测路径被初始化（在实际数据路由前可获得行为的知识）	基于邻居节点的推荐和节点最近的历史来计算信任值	高性能指标（能量效率、网络生存时间、路由成功等）	只关注黑洞攻击，只考虑到会聚节点的路由（并不是所有节点/目的节点）	黑洞攻击；篡改攻击
TAIV[20]	使用两条不相交的路由路径（主干路径发送数据包，而辅助路由路径传送验证信息）	路由路径中的所有节点信任值的增加或减少是基于传送的成功与否	增加路由成功率，有效地确定敌对节点的位置	只关注黑洞攻击/灰洞攻击，很难调整到基于簇的 WSNs	黑洞攻击；灰洞攻击；篡改攻击
TERP[21]	加权路由函数，其中的决策是基于信任、能量和跳数	直接/间接信任值的加权组合和未来行为评估	高能量效率 改进的路由维护机制	只关注黑洞攻击， 不允许添加和移除节点	黑洞攻击；篡改攻击
TSRF[22]	数学方法（通过利用一个多属性路由度量标准，在加权图上找到优化路径）	直接和间接信任值的加权组合（基于转发率）	能应对攻击，对于信任管理攻击表现鲁棒	不考虑节点能量，增加了通信开销	黑洞、灰洞、篡改、会聚洞攻击和能量枯竭攻击
TRS[23]	初始化路由发现（多路由）最后选择满足信任需求的最短路由	通过未来行为估计增强直接信任值（基于模糊逻辑预测模型）	对于各种攻击表现很好，低通信开销	不考虑推荐信任，不考虑节点能量	黑洞、灰洞、篡改、会聚洞和能量枯竭攻击

在文献[23]中，作者提出了一个有效的基于信任单播路由协议（TSR），将包准确率作为评估标准，并使用模糊逻辑规则预测方法评估节点信任度，一个源节点可以建立多条到目的节点的无环路由，每一条路由都有一个由跳数和路由信任值组合而成的评估向量，目的节点将质量好的路由作为候选路由，这条路由满足传送数据包的信任要求，最短路由可能被选作传送路由，与大多数基于信任路由协议相比，TSR 完全忽略了来自第三方节点对于信任值计算过程的评价，而且，选择最优路由的任务由会聚（sink）节点执行，这可能导致它更快的能量消耗。

最后，文献[24]作者提出了一个组合了地理路由的周围环境信任感知路由解决方案（ATSR），首先，一个地理路由方法适合于有效处理大型网络，第二，一个分布式信任管理系统合并直接和间接的信任信息，用于侦测和避免敌对节点实施路由攻击，以及攻击威胁到交换过程的声誉，能量感知也依赖于扩展网络生命周期。在提出的模式中，路由决策是基于一个权重费用函数，这个函数合并了信任、能量和位置属性。提出的协议考虑有效地评估信任的多个因素，它能应对各种攻击，从这个意义上看，这是

一个相当有效的解决方案。

表 2 基于簇的信任感知路由协议

协议	方法	信任值	优点	局限性	攻击
TLEACH[27]	信任管理模块维护节点间的信任信息	组合直接和间接信任值	对敌对节点表现鲁棒	无法应对串谋攻击	黑洞、灰洞、篡改攻击
RATCT[28]	建立一棵信任值树和一个信任模型，使用树结构来检测敌对行为	基于加密和数据包标签分析来评估信任水平	有效地侦测敌对行为	构建核心树需要消耗额外的能量	黑洞、灰洞、篡改攻击
TEESR[29]	基于节点信任值的多路径安全路由	会聚节点进行信任参数计算	可抵抗会聚洞和虫洞攻击	没有机制应对内部攻击	会聚洞、西比尔选择转发攻击
ECTMRA[30]	组合了信任感知和多路径路由的聚簇方法，路由只考虑那些达到一个期望信任值的路由	信任计算是基于转发率，包一致性和后备电池等因素	提高了路由处理质量，延长了网络生存时间并减少了端到端延迟	容易受到串谋攻击，没有阻止内部攻击的机制	黑洞、灰洞、篡改攻击
TRPM[31]	基于通信、数据、能量和推荐信任评估建立可靠路由	信任模型由通信、数据、能量、推荐信任评估属性组成	在处理各种路由和受信任目标攻击时表现很好	不包含信任感知簇头选择模式	黑洞、灰洞、篡改攻击，能量枯竭攻击、会聚洞、西比尔、串谋攻击

2.2 基于簇的信任感知路由

在基于簇的 WSNs 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[25]中，提出了一个基于信任的框架和一个将值得信任的节点选作簇头（CHs）的机制。论文利用了一个简单的信任模式，并没有过多关注信任评估。论文[26]中在选择值得信任节点作为簇头时，也提出了一个基于信任机制，算法利用了一个簇头选择的概率值，当传感器节点（SNs）基于它的簇头信任值加入一个簇，这个过程一直持续到所有节点都加入一个簇，这个算法非常消耗能量。在文献[27]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。

在文献[28]中，作者提出了 RATCT 协议，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，信任模型能有效地侦测敌对行为，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。

文献[29]提出了一个基于信任的能量有效安全路由协议（TEESR），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。

在文献[30]中提出了能量保存信任值多路由算法（ECTMRA），它组合了聚簇、信任感知和多路径路由来最大化网络生存时间，簇头负责计算本簇中节点的信任值，而簇头的可信度是由基站或邻居簇头来计算。信任度的计算是基于转发率因子数据、包一致性因子和后备电池，路由算法只考虑路由满足一个期望的信任分数。

最近，文献[31]提出了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。

3 结论

本文提出了一个基于信任路由协议的详细调查，并根据它们的基本特征进行合适的分类，它从整体展示中脱颖而出，最初大量的研究工作只考虑安全多路径协议，可是，由于 WSNs 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 WSNs 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）。

参考文献：

[1]G. Han，J. Jiang，L. Shu，J. Niu，H.-C. Chao，Management and applications of trust in Wireless Sensor Networks：A survey，Journal of Computer and System Sciences，Volume 80，Issue 3，pp. 602-617，2014.

[2]Stavrou，E.，& Pitsillides，A.（2010）. A survey on secure multipath routing protocols in WSNs. Computer Networks，54（13），2215-2238.

[3]Zin，S. M.，Anuar，N. B.，Kiah，M. L. M.，& Ahmedy，I.（2015）. Survey of secure multipath routing protocols for WSNs. Journal of Network and Computer Applications，55，123-153.

[4]Deng，J.，Han，R.，& Mishra，S.（2006）. INSENS：Intrusion-tolerant routing for wireless sensor networks. Computer Communications，29（2），216-23.

[5]Nasser，N.，& Chen，Y.（2007）.SEEM：Secure and energy-efficient multipath routing protocol for wireless sensor networks. Computer communications，30（11-12），2401-2412.

[6]Hayajneh，T.，Doomun，R.，Al‐Mashaqbeh，G.，& Mohd， B. J.（2014）. An energy‐efficient and security aware route selection protocol for wireless sensor networks.Security and Communication Networks，7（11），2015-2038.

[7]Zhou，J.（2013）.Efficient and secure routing protocol based on encryption and authentication for wireless sensor

networks. International Journal of Distributed Sensor Networks，9（4），108968.

[8]Wenjing Lou and Younggoo Kwon，H-SPREAD：a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks，in IEEE Transactions on Vehicular Technology，vol. 55，no. 4，pp. 1320-1330，July 2006.

[9]Shu，T.，Krunz M.，& Liu，S.（2010）.Secure data collection in wireless sensor networks using randomized dispersive routes. IEEE transactions on mobile computing，9（7），941-954.

[10] Liu，A.，Zheng，Z.，Zhang，C.，Chen，Z.，& Shen，X.（2012）. Secure and energy-efficient disjoint multipath routing for WSNs. IEEE Transactions on Vehicular Technology，61（7），3255-3265.

[11] Challal，Y.，Ouadjaout，A.，Lasla，N.，Bagaa，M.，& Hadjidj，A.（2011）.Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks. J. of Network and Computer Applications，34（4），1380-1397.

[12]K. Liu，N.Abu-Ghazaleh，K.D. Kang，Location verification and trust management for resilient geographic routing，Journal of Parallel and Distributed Computing 67（2），215-228，2007.

[13]I. Maarouf，U.Baroudi，A.R.Naseer，Efficient monitoring approach for reputation system-based trust-aware routing in wireless sensor networks，IET Communications 3（5），846-858，2009.

[14]N. Lewis，N. Foukia，An efficient reputation-based routing mechanism for wireless sensor networks：Testing the impact of mobility and hostile nodes，in：Sixth Annual Conference on Privacy，Security and Trust，pp.151-155，2008.

[15]H. Deng，Y. Yang，G. Jin，R. Xu，W. Shi，Building a trust-aware dynamic routing solution for wireless sensor networks，in：IEEE Globecom 2010 Workshop on Heterogeneous，Multi-Hop Wireless and Mobile Networks，pp.153-157，2010.

[16] Zhan，W. Shi，and J.Deng，“Design and implementation of TARF：A trust-aware routing framework for WSNs，” IEEE Trans. Dependable Secure Comput.，vol. 9，no. 2，pp. 184–197，Mar./Apr. 2012.

[17]H.A. Rahhal，I.A. Ali，S. Shaheen，A novel trust-based cross-layer model for wireless sensor networks，in：28th National Radio Science Conference，NRSC，pp. 1-10，2011.

[18]N. Poolsappasit，S. Madria，A secure data aggregation based trust management approach for dealing with untrustworthy motes in sensor network，in：2011 International Conference on Parallel Processing，pp.138-147，2011.

[19]Y. Liu，M. Dong，K. Ota，and A. Liu，ActiveTrust：Secure and trustable routing in wireless sensor networks，IEEE Trans. Inf. Forensics Security，vol. 11，no. 9，pp. 2013-2027，2016.

[20]X. Liu，N. Xiong，N. Zhang，A. Liu，H. Shen，C. Huang，A Trust With Abstract Information Verified Routing Scheme for Cyber-Physical Network，Published in：IEEE Access（Volume：6），pp.3882-3898 2018.

[21]A. Ahmed，K. A. Bakar，M. I. Channa，K. Haseeb，and A.W. Khan，A trust aware routing protocol for energy constrained wireless sensor network，Telecommun. Syst.，vol. 61，no. 1，pp. 123-140，2016.

[22]J. Duan，D. Yang，H. Zhu，S. Zhang，and J. Zhao，TSRF：A trust-aware secure routing framework in wireless sensor networks，Int. J. Distrib. Sensor Netw.，2014（3）：1-14，2014.

[23]H. Xia，Z. Jia，X. Li，L. Ju，and E. H.-M. Sha，Trust prediction and trust based source routing in mobile adhoc networks，AdHoc Netw.，vol. 11，no. 7，pp.2096-2114，2013.

[24]T. Zahariadis，P. Trakadas，H. C. Leligou，S. Maniatis，and P. Karkazis，A novel trust-aware geographical routing scheme for wireless sensor networks，Wireless Pers. Commun.，vol. 69，no. 2，pp. 805-826，2013.

[25]Crosby，G. V.，Pissinou，N.，& Gadze，J.（2006）. A framework for trust-based cluster head election in wireless sensor networks. In Proceedings of the 2nd IEEE Workshop on dependability and security in sensor networks and systems，pp. 10-22，2006.

[26]Raje，R. A.，& Sakhare，A. V.（2014）.Routing in wireless sensor network using fuzzy based trust model. In Proceedings of 4th international conference on communication systems and network technologies（CSNT’14）（pp. 7-9）.

[27]F. Song，B. Zhao，Trust based LEACH protocol for wireless sensor networks，Proceedings of the 2nd International Conference on Future Generation Communication and Networking，2008，pp.202–207.

[28]J.Wang，L. Li，Z. Chen，A routing algorithm based on trust worthy core tree for WSN，Proceedings of the IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing，EUC，2010，pp.763-770.

[29]N. Durrani，N，Kafi，J. Shamsi，W. Haider，A. Abbsi，Secure Multi-hop Routing Protocols in Wireless Sensor Networks：Requirements，Challenges and Solutions，in Proc. 8th Int. Conf. Dig. Inf. Manag.，2013，pp. 41-48.

[30]T. Senthil and B. Kannapiran，ECTMRA：Energy Conserving Trustworthy Multipath Routing Algorithm Based on Cuckoo Search Algorithm，Wireless Pers. Commun.（2017）94：2239-2258.

[31]B. Sun and D. Li，A Comprehensive Trust-Aware Routing Protocol with Multi-Attributes for WSNs，IEEE Access，Vol. 6，2018，pp. 4725-4741.

基于频谱共享关键技术的 230MHz 电力无线网分析

◆梁倩云[1]　陈少磊[2]

（1.国网四川省电力公司遂宁供电公司　四川　629000；2.国网四川省电力公司　四川　610041）