# 无线传感器网络安全路由研究综述*

李 挺，冯 勇†
（昆明理工大学 信息工程与自动化学院 云南省计算机技术应用重点实验室，昆明 650500）

**摘 要**：首先总结了无线传感器网络路由面临的主要安全威胁及其应对机制；然后根据协议所采用的核心安全策略对现有的安全路由协议进行了归纳、分类和比较，并着重对国内外重要的安全路由协议进行了介绍和分析。最后提出了几个无线传感器网络安全路由中需要进一步研究的问题。

**关键词**：无线传感器网络；网络安全；路由攻击；安全策略；安全路由协议
**中图分类号**：TP393 **文献标志码**：A **文章编号**：1001-3695(2012)12-4412-08
doi:10.3969/j.issn.1001-3695.2012.12.003

# Survey on secure routing research in wireless sensor networks

LI Ting, FENG Yong†
(*Yunnan Key Laboratory of Computer Technology Applications*, *Faculty of Information Engineering & Automation*, *Kunming University of Science & Technology*, *Kunming* 650500, *China*)

**Abstract**: This paper firstly sumed up the main secure threats and coping mechanisms in the network layer of WSN, and then summarized, classified and compared the existing secure routing protocols according to the core secure schemes used by them, and emphatically introduced and analyzed the important and typical ones among them. Lastly this paper proposed some problems which were worth further studying in secure routing area in WSN.

**Key words**: wireless sensor networks(WSN); networks security; routing attacks; secure schemes; secure routing protocols

在无线传感器网络的许多应用领域中，如安保防范、战场环境监控等，传感器节点采集和传输的数据非常敏感，确保数据在采集和传递过程中的安全显得尤为重要。由于采用多跳转发的数据传输机制和自组织的组网机制，无线传感器网络中每一个节点都需要参与路由的发现、建立和维护。这些特性使无线传感器网络的路由协议容易受到各种各样的攻击，如伪造路由信息、女巫攻击、虫洞攻击、污水池攻击、Hello 泛洪攻击等。这些攻击轻则影响网络的性能，缩短网络的生存时间；重则丢弃、窃取或窜改网络信息，破坏整个网络，给用户造成无法挽回的损失[1~3]。

同时，为减少数据消息的传输以节约能量，无线传感器网络中感知数据在传递给汇聚节点的过程中通常需要进行数据融合、冗余消息删除和数据压缩等网内(in-network)处理。数据消息传输过程中所经过的中间节点需要读取、修改和压缩消息的内容，而且无线传感器网络中很可能存在恶意的内部攻击者和被捕获的节点。因此，传统无线网络和 Ad hoc 网络中端到端的加密方式并不能保证无线传感器网络中传输数据的安全，需要在其网络层引入新的安全机制，即采用安全路由协议。安全路由协议不仅要以节约传感器节点能量的方式完成数据消息传输过程中的有效路由决策，而且要保证数据消息从源节点到汇聚节点的传输过程中，在每一个中间节点进行数据融合和冗余消除处理时的安全。

由于实现无线传感器网络的安全存在诸多方面的限制，主要包括无线信道开放传输的脆弱性，廉价传感器节点防护薄弱容易被攻击者捕获的脆弱性，部署环境无人看管存在着物理防护的脆弱性，节点计算、存储和能量受限不适合采用安全等级高但计算强度大的公钥密码算法等。这些因素使得无线传感器网络的安全路由成为一个具有挑战性的研究课题，吸引了国内外众多学者对无线传感器网络路由安全进行大量研究，并取得了丰富成果。

## 1 典型攻击及其防范

### 1.1 典型攻击

许多路由协议在最初设计时，只针对无线传感器网络的特点，将提高数据递交成功率、减少传输延迟、节约节点电池能量和延长网络的生存时间等方面作为设计重点，但是并没有考虑安全方面，因而这些协议存在着严重的安全问题。利用路由协议中安全缺陷所发起的攻击，主要可以分为以下几类[1,4,5]：

a)伪造路由信息，此类攻击是最简单的。攻击者参与到整个网络中，如数据的传递，在传递过程中攻击者可以传递自己伪造的路由信息给其他节点。由此，攻击者可能造成路由环路，吸引或阻塞网络流量，产生虚假信息，增加端到端的延迟，消耗相邻节点的能量，缩短整个网络的生存时间。

b)污水池攻击。如果攻击者只想破坏网络的性能，如增加合法用户收到信息的延迟、减少网络的生存时间等，它可以通过声称自己有充足的能量、路径最优来吸引部分或全部邻居节点将信息传给它，再由它传送出去。借此，攻击者可以将所

**收稿日期**：2012-04-22；**修回日期**：2012-05-30 **基金项目**：国家自然科学基金资助项目(71161015)；云南省自然科学基金资助项目(KKSY201203027)

**作者简介**：李挺(1988-)，男，重庆人，硕士研究生，主要研究方向为无线传感器网络安全；冯勇(1975-)，男(通信作者)，云南楚雄人，副教授，博士，主要研究方向为无线传感器网络和自组织网络(fybraver@163.com).

有信息全部丢弃或传递虚假信息等。

c)选择性传递,此类攻击是对污水池攻击的改进。若攻击者将自己接收到的信息全部丢弃,只要利用网络的冗余性,很快就能发现攻击者,并将其隔离。但如果攻击者采用选择性转发,因为无线传感器网络的拓扑结构存在很强的动态性,部分消息丢失是很正常的,这样就能降低邻居节点对攻击者的怀疑,而攻击者可以继续对网络造成破坏。

d)女巫攻击。在大多数路由攻击中,攻击者首先都要融入网络,得到邻居节点的信任,使自己成为路由路径上的一个中间节点。女巫攻击让攻击者在网络中拥有多重身份,让普通节点以为存在着更多节点并且可以通过这些节点将信息传递给汇聚节点或基站,然而这些信息却全都转发给了攻击者。此类攻击针对地理路由协议特别有效。

e)Hello 泛洪。某些路由协议需要广播 Hello 数据包来声称自己是其邻居节点,收到数据包的节点会认为发送者在自己的通信范围内。所以攻击者只要发送足够大功率的数据包给普通节点,并广播自己是其邻居节点即可。在以后的信息传递过程中,普通节点可能会选择包含该攻击者的路径,但由于普通节点与攻击者的实际距离太远,信息根本无法到达攻击者,从而导致网络混乱。

f)虫洞攻击。针对多跳路由协议,虫洞攻击是一种很好的攻击方法。首先两个节点相互串通(也可以不串通,可以一个攻击者和一个普通节点),一个位于基站附近,一个相离较远,在它们之间有一条“隧道”,相距较远的节点对外声称自己与基站附近的节点可以建立低延迟、高带宽的信道,让其邻居节点相信它,将信息转发给它。

g)确认欺骗。由于无线传感器网络的节点是电池供电,而且一般运行的环境比较恶劣,所以有些节点存在“死亡”或功率不足的问题,从而达不到传递消息的能力。但有些协议需要先通过链路层的确认,再通过得到回复确认的节点转发数据包。攻击者通过监听邻居节点的数据传输,替“死亡”或功率不足的节点发送伪造的链路层确认,让邻居节点以为这些节点还能运行,可以通过这些节点传递信息,从而导致网络失效,或者攻击者以这种诱导方式形成一条它期待的路径。

h)拒绝服务攻击。由于攻击者一般拥有足够多的能量,它可以在网络中大量占用网络带宽等资源,或者大量消耗普通节点的能量,从而阻碍普通节点正常的数据传输,甚至导致网络瘫痪。

通常针对具体的路由协议可以发动某一种特定类型的攻击,也可以将上述攻击方式组合起来形成新的更有威胁的攻击。而且,随着研究的不断深入,针对无线传感器网络路由攻击的方式也在不断出现,如 Ramaswami 等人[2]提出了一种谋串的黑洞攻击,Deng 等人[3]提出孤立基站的攻击方法,以及 Qi 等人[6]提出的目标定向的攻击模式等。

### 1.2　应对攻击的防范方法

为了应对无线传感器网络面临的各种攻击,提高网络的安全性,在研究人员的努力下已提出许多应对攻击的方法。根据所防范种类的不同,这些方法可以作如下分类:

a)针对外部攻击的防范方法。大部分无线传感器网络路由协议的外部攻击可以通过简单的链路层加密和认证来防范。因为节点不接受没有通过认证的节点,所以女巫攻击难以实施;又由于阻止了攻击者加入网络,同时也避免了选择性转发攻击和污水池攻击。

b)针对女巫攻击的防范方法。对于那些已经通过认证、融入网络但却被攻击者捕获的节点,可以采用让每个节点与可信的基站使用对称密钥。对于一组邻居节点可以用所得的密钥来实现它们之间的认证和加密连接。由于攻击者可以在网络中移动,与别的节点建立共享密钥,基站则可以限制每个节点可拥有的最多节点数。若邻居节点数目过多,则说明此节点有问题,从而阻止攻击者拥有过多身份。

c)针对 Hello 泛洪的防范方法。可以采用双向确认认证,在双方确定通信前进行双向的确认认证。由于普通节点发送功率小,无法将确认消息发送给攻击者,则认为链路失败。有时攻击者可能采用高功率的接收器达到确认的目的。对此,基站仍然可以采用限制邻居节点数目来防止此类攻击。

d)针对选择性转发的防范方法。最好的方式是多路径路由。因为无线传感器网络节点密度较高,具有冗余性,当一个消息从源节点到目的节点有 $M$ 条路径,而且这些路径完全独立时,能够完全防范多达 $M$ 个攻击者的攻击。

e)针对广播认证和泛洪的防范方法。由于所有节点都信任基站,不能够让攻击者随意伪造基站的信息,因此普通节点必须能够验证消息是否来自基站,可以采用数字签名或在信息中加入认证信息的方式。泛洪防范主要是防止一个消息传播到网络的每个节点,可以要求内部攻击节点在网络基础拓扑结构中形成顶点切割。

f)针对虫洞和污水池攻击的防范方法。这两类攻击是最难防范的,特别是当两类攻击相结合时。虫洞攻击很难被检测出来,因为攻击者之间使用私用频率;污水池攻击很难防范是因为普通节点无法辨别攻击者发送消息的真伪。所以最好的防范方法是在设计路由协议时,重点考虑这两种攻击。

设计安全路由协议时,就是在考虑怎么避免这些攻击,让无线传感器网络能在一个安全的环境中运行。但因为攻击的多样性和无线传感器网络自身的缺陷,导致想要设计出全面的防范方法是困难的。

## 2　安全路由协议

2002 年 Perrig 等人[7]较早提出了无线传感器网络的安全路由问题;次年 Karlof 等人[1]对传感器网络路由机制面临的攻击和相应的防范方法进行了讨论,阐述了安全路由问题的重要性。该问题从提出至今一直受到人们的广泛关注,经过研究人员多年的努力,已经取得了丰富的研究成果,提出了许多安全路由协议。根据这些路由协议所采用的核心安全策略,可以将它们分为基于反馈信息的安全路由、基于地理位置的安全路由、基于密码算法的安全路由、基于多路径传输的安全路由、针对层次结构的安全路由和应对特定攻击的安全路由等几类。

### 2.1　基于反馈信息的安全路由协议

在某些路由协议中,节点通过反馈信息,如延迟、信任度、地理位置、剩余能力等,作出一系列决策以提高安全性改善网络性能。这些决策主要包括安全路径选择、低耗能路径的选择、信任邻居节点的选择等。

Cao 等人[8]提出的 FBSR 重点考虑了网络的动态行为、安全路由和能量效应。节点从邻居节点获得当前动态网络信息作为反馈信息,使节点以安全和能量为要求来转发信息。反馈

信息包含在MAC层的应答帧中,以避免网络拥塞;以关键的单向hash链认证,避免虚假反馈;使用基站的统计检查,发现可能受到影响的节点。虽然协议没有采用任何加密机制,但针对常见的攻击,如虚假路由信息、污水池攻击和虫洞攻击等,都设计了相应的防范策略。

根据反馈信息计算出信任度,然后根据信任度作出一系列决定,是一种有效的安全措施。AE-ARAN[9]是在ARAN[10]基础上提出的匿名、高效的安全路由协议,还引入了D-S证据理论[11],同时处理信任评估中的随机性和主观性。协议根据信任评估模型计算节点的信任度,选择可信节点参与路由,在路由建立过程中各节点的路由表中都存储一个关于节点匿名身份的hash路由登记表,在需要建立路由时只需计算目的节点的hash身份是否在自己的路由表中,有效保证了网络匿名性和避免了重复发起路由,从而建立安全的路由。节点$A$评估节点$B$时,主要考虑$A$关于$B$的直接信任($D$)和间接信任($I$),然后根据Dempster组合规则对$D$和$I$进行合成以得出综合信任。协议可以有效地检测和隔离恶意节点,抵制修改、黑洞等攻击,可以提高整个网络的可靠性、鲁棒性和安全性,特别在恶意节点较多时,这种优势更明显。ATSR[12]的完全信任信息也包括直接信任和间接信任。直接信任是节点自己检测邻居节点的邻居节点所得,主要包括数据包的转发、网络层的确认、剩余能量等;间接信任是节点额外地向邻居节点要求的信任信息,加快信任积累的过程。针对获得间接信任的缺陷,协议设计了应对方法;协议对网络的动态变化和新节点加入的信任信息也作了考虑。由于信息量大,节点内存受到限制。

王潮等人[13]提出的安全路由算法将可信度概念与群体智能优化算法相结合。协议中,节点可信度是节点安全的度量研究基础,该协议可信性的度量指标只包含了延迟、丢包率、剩余能量。可信度作为信息素的一个分配策略,类似于MPLS的一个可信安全标签,建立可信安全路由,将恶意节点排除网络,提供安全可信的网络环境。该算法避免了密码认证算法的高计算量的复杂度,具有计算量小、收敛速度快、能跳出局域最优解、全局能量均衡、延长网络生存时间的优点,还针对虫洞攻击的防范进行了研究。

CBSRP是在多级分簇路由结构上,根据确定度动态调整数据传输密钥的安全路由协议[14],每一轮数据传输都是使用根据确定度生成的新的随机密钥。簇的建立是由基站定时发起,其目的是最终建立一个由多级簇头组成的分层网络;数据传输阶段采用64 bit的AES算法进行加密认证。由于在这个过程中簇头不存储随机密钥和随机函数,只能转发数据,不能解密和认证,所以防止了污水池攻击、虫洞攻击、女巫攻击。采用动态密钥算法和分散式密钥管理,即使某个节点被捕获也不能提供其他节点的密钥,只能导致单个节点失效,中转节点没有解密和认证的能力,使得伪装为簇头的恶意节点无法获得有意义的信息。而且通过动态调整数据的传输密钥,也能够调节消耗在数据传输安全保证上的计算能耗和通信能耗,有利于节约能量。

TPSRP是在链路状态路由协议OLSR的基础上提出的基于信任保留的安全路由协议[15]。协议采用信任保留的方法对节点进行认证,而且采用关联规则的信任评估手段,使得节点可以通过综合的信任信息,自我识别并限制内部叛变节点的恶意行为。身份认证时,在使用SOLST认证方法的基础上增加了DH单跳密钥协商机制,能够有效抵抗重放攻击。保留信任的基本思想是对每个报文的接收状态进行记录,保留认证步骤中收到的最后一个报文的验证结果。认证采用主动和被动模式。TPSRP还提供报文完整性校验以及接收者验证发布者的机制来抵抗恶意节点广播虚假消息、窜改正常节点的报文等。安全路由的形成一般是从两个节点作为种子节点开始的,这两个节点进行身份认证,通过后形成可信节点,然后再递归地扩大网络范围。此协议对抵抗虫洞攻击特别有效。

Galuba等人[16]提出的Castor安全路由协议可以同时解决安全性、可计算性和适应性问题。该协议只使用一些简单的确认数据包,不需要使用任何控制信息,每个节点在局部领域里由自己作路由决定。在数据传递过程中,中间节点直到收到目的节点的确认信息才停止传递该信息。该协议对各种常见的攻击和针对该协议的特定攻击都有很好的防范能力。

### 2.2 基于地理位置的安全路由协议

地理位置信息可以作为重要的路由决策依据以改善数据传输性能,目前已提出了许多基于地理位置的路由协议。此类协议通常需要在邻居节点间进行坐标位置信息的交换,而这一特性使其容易受到包括女巫等类型的攻击,需要采用有针对性的安全机制来提高路由协议的安全性。

GPSR路由协议是典型的基于地理位置的路由协议。TRANS是建立在GPSR基础上的安全路由协议[17],还对能量限制作了特别的考虑。协议主要包括信任路由和不安全避免,其主要思想是使用信任概念来选择安全路径和避免不安全位置。信任路由设置在汇聚节点和感知节点,包括加密确认、信任表处理和黑名单处理等。不安全位置避免设置在汇聚节点,包括不安全位置探测、黑名单传播和不安全位置集合。数据包由可信中间节点传递给目的节点。协议增加网络的吞吐量来提高能源效率;采用恶意节点位置识别机制,所使用的传输量比传统有关计划的传输量小。在包头嵌入黑名单,以此引导数据包绕过恶意节点。

要得到地理位置信息,首先需要计算出地理位置。传统的定位方法主要有基于测距定位和无须测距定位。Abu-Ghazaleh等人[18]介绍了一种确认地理位置的算法,并且通过对路由认证和基于可信路径选择的建立来抵抗攻击。针对基于地理位置转发的两个缺陷,协议分别设计了应对方法。该协议通过认证和加密保证了合法节点加入网络和数据的机密性,但不能阻止由于恶意节点或普通节点被捕获而使得地理路由被中断。

Wood等人[19]提出的SIGF是基于IGF协议的一组可进行配置的安全协议簇,通过修改配置达到不同的安全级别,为不同的需要提供必需的安全强度。此协议可以防范常见的一些攻击,如污水池攻击、选择性转发和部分拒绝服务攻击等。SIGF包括了三个协议:SIGF-0不保存状态信息,但可以以一定的概率提供防范;SIGF-1保存历史记录和节点信誉信息,可以防范一些攻击;SIGF-2使用邻居节点状态共享信息,可以提供更强大的安全保证。同时该协议在安全提供和状态的保存与维护方面制定了明确的协商制度,而且SIGF为了节约能量,大多数采用被动的安全机制,当没有攻击时节约能量。

H-SPREAD是基于一个分布式的$N-1$多路径发现协议[20],协议使传感器节点感知自己的局部信息。协议扩展了SPREAD[21]。H-SPREAD使用了两个步骤来发现最优路径。首先使用分支意识(branch-aware)泛洪协议寻找一组节点不相交的路径;根据分支节点的位置标记邻居节点的关系,不同树

枝上的传感器形成一种不相交的路径。在第一阶段无须引入任何额外的路由信息。针对第一阶段的一些限制,为最大限度地发现不相交的路径,在第二阶段作了调整。该协议还采用了活跃的数据包来提高每个路径的可靠性。但是该协议同样遭受很多攻击,如 DoS 攻击,攻击者通过俘获的节点发动虫洞攻击、污水池攻击和 rushing 攻击,由于没有认证,攻击者甚至可以伪装为 sink 节点,成为网络所有流量的目的地。

匿名的方式有很多,如源节点、目的节点信息的匿名,路由路径的匿名等。Li 等人[22]提出了三种方式可以达到对源节点地理位置信息的匿名,三种方式分别是以最小距离、角度、象限为基础来选择中间节点。通过删除上一跳节点信息,使得攻击者不能回溯找到上一跳节点,从而无法确定源节点信息。该协议要求每个节点知道其他节点的地理位置信息,而且每个节点都将自己的信息单方面传递给 sink 节点。对每种不同的方式都有较好的节能效果。

Prism 路由协议[23]实现了安全和隐私保护。协议对节点进行认证时采用组签名机制,设计反跟踪机制来防止内部和外部攻击者的跟踪,还要求确保路由信息的完整性。整个网络中,节点没有唯一的 ID 标志,但必须知道节点的地理位置信息,节点间通信时是基于当时的拓扑结构或一些最新的条件,当不能满足此条件时,采用 hit-and-miss 方式进行弥补。

### 2.3　基于密码算法的安全路由协议

通过加密机制可以保护信息不被攻击者窃取;通过认证机制可以防止攻击者加入网络。上述这些安全机制的应用能够有效增强无线传感器网络的安全性。

基于密码算法的安全路由协议中最经典是 SPINS[7],它主要包括 SNEP 和 μTESLA 两个安全模块。SNEP 提供数据的机密性、点到点的数据认证、数据的新鲜性;μTESLA 在 TESLA 的基础上进行改进提供广播认证。SNEP 用于交换消息的报文小,虽然加密的时候使用计数器,但是计数器的值只是在最后的报文中使用,SNEP 达到语义上的安全,能避免重放攻击;节点通过改变发送的计算器的值和需要发送的每个加密信息来避免 DoS 攻击。μTESLA 使用对称加密机制对原始数据进行认证,每隔一段时间才更新一次密钥,并且对认证请求发送者的数目进行限制,以此来降低节点的能耗。为了代替高能的 TESLA 数字签名,该协议使用节点到基站的认证通道,辅助程序的广播认证。但 SNEP 的各种安全机制都是通过信任基站完成的,所以基站就成为瓶颈。由于节点新加入网络是点对点的单播过程,对于一个大规模的网络来说,源端认证的广播协议初始化需要消耗很多的资源。

Misra 等人[24]提出了一种端到端的安全通信协议算法 ETESC。该算法的核心思想是给每个节点预配置不同的密钥,从而加强某些环节的弹性,算法中还采用杠杆原理。协议由不同的密钥管理和有弹力意识的路由两部分组成。算法与现在经典的地理位置路由协议和以数据为中心的路由协议结合,都体现出了很好的安全性。

国内周贤伟等人[25]提出的安全路由算法把优化能量、提高路由的安全性和缩短传输延迟同时作为设计目标,采用多目标决策。在安全性方面,节点在部署前通过预置公私密钥对方案有效提高了路由的安全性;在路由选择时,以最少转发跳数为依据,减小了数据延迟,让能量储备较多的节点承担较多的数据转发任务,可获得最优路由和延长网络生存时间。该算法设计简单、针对性强、安全性高,但是在触发路由发现时,引入阈值来与有效路径比较,以判断路由发现时机,使得精确性不够。

Anderegg 等人[26]在路由协议中引入了博弈论中"贪婪、自私的"代理,代理在自己的能力范围内接受报酬为其他代理转发信息,通过代理形成一种可信任的路由协议。该协议改进了 VCG 机制,而且属于被动类型的路由协议,只有当网络节点初始化会话时才运行和计算路由路径,不需要节点拥有关于网络的所有信息。在路由发现过程中寻找节能的路径。协议保证找到一条成本最低且最可信的路径,但协议的预算不平衡,特别是对不在路径中的中间媒介节点。

BEARP 协议[27]保证了信息安全性的四个特点:信息的机密性、完整性、新鲜性和有效的认证。协议由邻居发现和路由发现组成。通过邻居发现过程使得节点可以知道自己的真正邻居并且保存它们的信息。协议的重点是采用加密和认证,加密所有的数据包,在源节点与基站间实行认证,确保路由的安全。

IBRP 协议[28]主要引入节点的身份认证来保证网络路由的安全性。在路由发现过程中采用椭圆曲线加密算法,确保在此过程中发现的节点都是可信的;协议还采用能量阈值来确保节点不会过度消耗能量。该协议重点对女巫攻击和虫洞攻击作了分析。Guo 等人[29]也是采用了椭圆曲线的加密算法来保证节点间通信的安全性,通过使用时间驱动分簇的协议和节点一般情况下处于睡眠的方式节能。

Directed Diffusion 是经典路由协议,SDDRP[30]在其基础上增加了 μTESLA 机制,认证从汇聚节点发送给源节点的确认信息,提高协议的安全性。该协议有效地抵抗了虫洞攻击和确认欺骗攻击,但同时消耗更多的能量,增加了平均延迟。

无线传感器网络的隐蔽性包括信息、目的节点位置和源节点位置的隐蔽性。STsR 协议[31]通过引入汇聚节点的环形区域路由(STaR)来保护源节点位置的隐蔽性。该协议假设攻击者没有能力监视整个汇聚节点的环形区域。协议由两部分组成:a)源节点在节点区域随机选择一个媒介节点,然后把消息发送给媒介节点;b)媒介节点通过单路径将转发信息给汇聚节点。但是该协议存在很多假设情况,而且对环形区域的大小选择存在问题,不能选择一个合适的范围,使得攻击者不能监视整个区域。

Al-Karaki 等人[32]提出的 ASSP 协议,通过限制密钥长度的阈值和新创建密钥的长度来权衡安全等级与能量的消耗。协议由确立会话密钥、获得密钥池、分配密钥三个部分组成。协议的一个特点就是密钥长度对网络的安全性与能量之间的一个转换,长密钥保证了网络的高安全性但缩短了网络的生存时间。

Ariadne 是一个按需的安全路由协议[33],该协议能够抵抗各种主动攻击,而且还能非常有效地降低节点被攻击者捕获所带来的损失。为了达到这些安全性,该协议只依靠高效的对称密钥加密操作。Ariadne 在 DSR 路由协议的基础上添加 TESLA 机制,但该协议需要时间同步和及时认证。

### 2.4　基于多路径传输的安全路由协议

多路径路由能够有效提高数据消息的递交成功率,平衡节点能量消耗以延长节点的生存时间。同时,多路径路由也是针对选择性转发攻击的一种有效防范方法。

Ouadjaout 等人提出一种新的多路径路由 SMRP,在此基础上设计出了 SEIF[34]。此协议与一般的容侵类路由协议的区别在于分布式和联网核查计划,而且不需要向基站提交路由建

立和安全检查,还运用新的多路径选择计划,加强网络的带宽,节约节点的能源。SEIF 依靠单向的 hash 链建立一个多路径、多到一的传播树,还提供路由初始化的确认和父节点的认证;单向 hash 链提供交换控制信息的认证;为了抵御 Hello 泛洪攻击,使用怀疑机制。但协议没有解决大量的攻击,如果攻击者捕获了普通节点,它可以找到有关加密数据存储的信息,并用它来破坏网络的机密性。

PRSA[35]是一种路径冗余的安全算法。PRSA 要找到从源节点到目的节点的安全多路径路由且成本还要低。为了加强网络的可靠性,在被确定的路径上允许节点的数据包以多种模式发送,如循环赛模式、冗余模式、选择模式,协议的安全性主要源于入侵检测设计的支持;而且该协议能减少网络延迟、丢包率、能量消耗,增强数据包的生产能力。

匿名路由协议 MPRASRP[36]可以有效地防止攻击者获得源节点和目的节点的身份,以阻止攻击者进一步跟踪两个节点间的信息处理。针对传统的匿名路由协议都是单路径的问题,该协议提出了多路径的想法。保证节点匿名的原因是:源节点和目的节点的身份用目的节点的公共密钥加密,而只有目的节点可以解密数据包。该协议能有效防止中间人攻击,而且在条件恶劣的环境下也很有效,但是该协议不能防止重放攻击。MASK[37]也是通过匿名性达到安全性,在该协议中物理层和网络层交换信息都不要公开 ID,提供发送者和接收者及两者之间关系的匿名,而且在通信过程中由于使用了动态匿名,能够抵抗偷听和重放攻击,也有很好的节能效果。

MSR[38]协议的基本思想是将一个原始信息通过取消编码分成子数据包,然后将这些子数据包通过独立的多重路径发送出去,最后由目的节点将这些信息再组合起来。该协议主要包括随机的多路径、加强被动确认和取消编码。只有需要的时候才建立随机多路径。被动确认是基于被动地监听流量,分析邻居节点的安全行为,减少路由的报头,对常见攻击有很好的防范,保证了路由的安全。

为避免通过恶意节点传输数据,Zhao 等人[39]提出了一种多路径路由协议,实现了可靠的数据传输却不执行任何安全机制。但攻击者可以发动大量的攻击,如窃听、虫洞攻击等;而且,以拒绝服务攻击为基础的路径可以减少该协议的有效性,如果源节点没有收到通知数据包,它不会切换到新的替代路径,而会继续使用受损的路径。

基于恶意节点检测的多路径安全路由协议[40]综合考虑了网络能耗和安全性之间的平衡问题,使用对称密钥和非对称密钥相结合的加密和认证过程。采用协商机制,有效识别恶意节点,防止节点将数据发向恶意节点;一旦恶意节点被确定,节点 ID 就会被加入黑名单。保证存在路由的情况下能够发现路由,且不暴露网络的拓扑结构,能够有效抵御针对路由安全的威胁;针对延迟问题,协议在节点处引入双队列模型,控制延迟。

连通性是多跳路由协议里一个重要的概念,SeMuRa[41]扩展了 *K*-connectivity,引入 *K*-*X*-connectivity 概念。协议还扩展了 DSR 算法,在交换数据包时,使用极限的数字签名认证。为了保证路由的安全性,协议要求在建立路由时,节点必须能够认证其他节点;伪造的数据包在到达基站前就必须被检测出来;节点还要监测邻居节点的行为;协议采用看门狗机制来检测节点不转发数据包的情况;协议能避免虫洞攻击。

### 2.5 针对层次结构的安全路由协议

传感器节点通常采用电池供电,能量难以补充,节能是无线传感器网络面临的重要挑战。层次式网络结构具有较好的节能特性,但是其中的簇头、树根等关键节点一旦因攻击而失效将会对网络的安全和性能造成严重影响,需要采用有针对性的安全保护机制。

LEACH 是一个经典的分簇类的路由协议,但是该协议并没有很好地考虑安全问题。AC[42]协议是在其基础上增加了安全考虑的分簇路由协议,协议有三层路由,其中一层用来选择簇头,一层用来身份认证和保密,另一层用于路由。该协议要求每个传感器节点通过唯一的 ID 标志,集群和簇头的形成由 LEACH 协议完成,部署前就确认基站。

SHSMRP[43]协议将分层网络结构和纳树相结合,节点能够获得自己的地理位置信息,而且此信息作为加入网络的重要条件。协议由五部分组成:节点信息聚集、纳树的构造、纳子树的构造、数据传递、纳树的维护。协议根据 LKHW[44]设计出了自己的本地密钥等级。该协议通过使用 HMAC 保证了数据的秘密性、完整性,能有效地避免虫洞攻击和女巫攻击。

SCMRP[45]是一个主动类型的协议。在初始化时就已经部署好需要的信息,如节点唯一的 ID 号、节点与基站共享的密钥对等。通过使用基站的数字签名证书,避免恶意节点伪造 ID;又因为节点与基站有唯一的密钥对,保证了信息的机密性。协议还充分考虑了网络动态变化问题和分簇协议中常见的孤立节点的问题,对常见的攻击也有有效的防范能力,如伪造路由信息、污水池攻击等,但是该协议过分依赖基站。

INSENS[46]协议安全有效地设计了树型结构的路由路径。在协议中的攻击者可以捕获传感器节点,可以注入、修改和阻止数据包,但是协议必须能够容忍这些攻击,而且还要将损失控制在一定的范围内,不能影响整个网络的工作状态。通过每个节点交换管理信息达到路由发现,确定传感器网络的拓扑结构,构建适当的传播表。路由发现由基站领导完成。数据传播使用一个三元组来匹配。INSENS 有基本版本和加强版本两种。基本版本适合于中等规模的传感器网络,如数百个节点;加强版本适合于大型传感器网络,如上千个节点。加强版本是针对基本版本不足之处进行改进,使用双向认证来防范攻击;使用多个基站多跳路径来增加 INSENS 的可扩展性,以适应大规模网络;增加一组动态安全维护机制,能管理节点的加入和离开带来的更新问题。

网络拓扑结构是一种树型结构,基站为树根,并且认为是可信的,每个节点在树型结构中都有多个父节点,协议中基站和每一节点共享一个密钥;通过节点间唯一的密钥,每对邻居节点建立安全的通信信道。这是 SeRINS 路由协议[47]的一个特点,该协议是一种安全交替的路由协议。为了在建立交替路由中避免恶意节点,线路根据跳数更新单向的 hash 链。邻居报告系统是最重要的一部分,通过节点周围的邻居节点,确认节点的路由广播,将怀疑节点报告给基站,当基站确认恶意节点以后,它向整个网络广播此消息,以此排除恶意节点。节点的路由广播使用 ARMS 认证 ,避免了伪造路由信息;使用交替路由计划防范了选择性转发;邻居报告系统排除了恶意节点也排除了污水池攻击;因为每对邻居节点通过唯一的密钥建立通信信道,同时可以避免 Hello 泛洪攻击和确认欺骗攻击。

### 2.6　应对特定攻击的安全路由协议

由于具体的路由协议通常情况下只是面临几种特定类型的攻击,因此可以根据不同攻击的特点,在设计路由协议时有针对性地采用相应的安全措施来抵御这些攻击,以提高路由协议的安全性。

Ramaswami 等人[2]提出一种针对谋串的黑洞攻击的安全路由协议,该协议在经典协议 AODV 的基础上进行改进。协议使用轻量级确认体制和多跳路由协议保证协议的安全,而且可以鉴别和孤立谋串的黑洞攻击。协议采用 AODV 协议的路由发现过程,转发数据包时,源节点发出爆裂(burst)的特殊数据包沿路径传播;当目的节点收到特殊数据包,其使用多跳路径来传递特殊的爆裂数据包的确认信息。其根据收到 ACK 报文的数量来判断是否存在黑洞。

DoS 攻击可以分为被动和主动两类。S_LEACH[48]是一种针对被动的 DoS 攻击的安全路由协议,而且还能加强节点间的相互合作能力。该协议是在 LEACH 路由协议的基础上引入贝叶斯博弈方法。贝叶斯博弈可以使恶意节点更加活跃,而且在恶意节点活跃时间内使入侵检测系统能够更好地运行。

通常根据网络的规模动态调整路由协议。SPR[49]便是一种主动减缓虫洞攻击和污水池攻击引起的安全影响的路由协议簇。协议簇使用预计的路径风险作为协议的参数,由于能量消耗和安全性成反比,该协议也将能量消耗作为协议的一个参数。协议簇分为 SPR1 和 SPR2,SPR1 主要是假设网络中所有节点的量化风险值存储在安全的基站,由基站帮助源节点验证完整的路径风险,当节点数目过大的时候,对于基站要求就会很高;SPR2 就是针对这种情况设计的,根据风险值和路由节点到源节点的跳数作为参数。对于虫洞攻击,通过减少容易受到损害的通信量节点数减少虫洞的通信量;对于污水池攻击,采用多路径和随机路由防范。

同样,RESIST[50]也是一个协议簇,主要针对树型拓扑结构的污水池攻击。根据复杂度和强度的不同,协议簇分为 RESIST-1 和 RESIST-0。RESIST-1 阻止恶意节点修改它到汇聚节点的距离,RESIST-0 则不允许这种谎言存在。为了防止污水池攻击,协议簇限制了离汇聚节点最近的攻击者勾结攻击的能力,而且恶意节点间的勾结交流也被限制。协议簇采用椭圆曲线加密算法减少节点加密的开销,使用单向 hash 函数减少报头节约能量。

Song 等人[51]提出的方法其主要思想是根据确定的统计发现路由,而且提高了对虫洞攻击的判断,甚至精确地找出攻击者的位置。但是如果恶意节点在路由过程中行为正常,这将很难检测出来,特别是黑洞攻击。

Zhang 等人[52]提出的路由协议采用了多路径网络的交叉认证想法,而且能够过滤恶意节点注入的虚假报告。在通信和传感器节点中提前识别虚假报告,这样可以节约能量,促进网络的生存时间。协议扩展了 IHA[53]设计,算法中的节点协助发现阶段、报文认可阶段和线路过滤阶段是最重要的。但攻击者可以发动 DoS 攻击,并禁止数据包到达目的节点和影响节点的关联过程;重放攻击可以消耗节点的资源,影响网络的生存能力;攻击者还可以捕获传感器节点,并选择性丢弃数据包,影响网络的运行。

针对可以使孤立基站或者使基站失效的两种攻击方法,Deng 等人[3]提出了相应的安全策略:a)安全多路径路由,提供了多条到达基站的路径从而提高入侵容忍来防范基站被孤立,采用单向 hash 链和反馈算法来阻止欺骗和 DoS 攻击、rushing 攻击;b)反流量分析策略,就像采用逐跳的群集密钥加/解密和数据发送控制来伪装基站的位置。

针对广播认证协议的 DDoS 攻击,Chen Jia-wei[54]设计了防范方法。该协议基于 DBP-MSP 和安全路由,引入广播状态表,基站根据节点信息来更新广播状态表,接收者由基站通过搜索表返回的信息,可以确定解决 DDoS 攻击的方案;还引入密钥链方案,每间隔一段时间,基站向发送者发送单向密钥链,减少发送者的存储和计算负担。

Claycomb 等人[55]提出了安全策略的概念。策略提供设计者和管理者访问节点资源的能力,安全策略主要是基于信任、任务和预组密钥,协议使用 IBC 对节点和组身份加密;而且这些策略可以自动适用网络条件和额外的刺激因素。对于女巫攻击、虫洞攻击等都设置了应对的策略。

针对两种较新的攻击方式,即网络成员间不合作和恶意节点隐藏丢包,Kong 等人[56]提出一种新的自愈社区机制来解决这两种攻击。其核心思想是通过分散对邻居节点社会的网络服务询问来缓解攻击者自私行为和恶意节点的行动。自愈社区是基于更多的中间节点对传输过程中对数据包实施观察,通过实验证明该协议有很强的安全性。

### 2.7　各类协议的比较

通过前面六个小节对现有主要安全路由协议进行的分类介绍和讨论,对每类协议的理论基础、工作机制和特点有了较为充分的了解。在此基础上,对本文中划分出的六类安全路由协议进行横向比较,以更为具体地了解不同协议之间的差异,更为全面地认识每类协议的特性。如表 1 所示,从每个类别所包含的典型协议、可抵御的攻击类型、主要缺陷和资源消耗这四个方面对本文所划分出的六类安全路由协议进行了综合比较。

表 1　各类协议的比较

| 协议类别 | 典型协议 | 可抵御攻击类型 | 主要缺陷 | 资源消耗 |
|---|---|---|---|---|
| 基于反馈信息的安全路由协议 | AE-ARAN[9]<br>Castor[16]<br>FBSR[8]<br>TPSRP[15] | 伪造路由信息;污水池攻击;虫洞攻击;重放攻击 | 反馈信息的新鲜性和真实性不易保证 | 较低 |
| 基于地理位置的安全路由协议 | TRANS[17]<br>Prism[23]<br>Li,*et al*[22]<br>Abu-Ghazaleh[18] | 伪造路由信息;污水池攻击;虫洞攻击 | 攻击者能够通过地理位置信息窃取网络拓扑等信息 | 较低 |
| 基于密码算法的安全路由协议 | SPINS[7]<br>ETESC[24]<br>Anderegg[26]<br>Ariadne[33] | 伪造路由信息;女巫攻击;虫洞攻击;污水池攻击;重放攻击 | 高强度的加密算法对资源的消耗较大 | 较高 |
| 基于多路径传输的安全路由协议 | SEIF[34]<br>SeMuRa[41]<br>MSR[38]<br>PRSA[35] | 选择性转发;重放攻击;污水池攻击;虫洞攻击;伪造路由信息 | 多路径上的节点失效会增加数据包延迟;对于 DoS 攻击敏感 | 较低 |
| 基于层次结构的安全路由协议 | INSENS[46]<br>AC[42]<br>SeRINS[47]<br>SHSMRP[43] | 伪造路由信息;虫洞攻击;女巫攻击;污水池攻击;Hello 泛洪;确认欺骗攻击 | 簇头节点成为攻击的重点,重新选择簇头耗能、耗时 | 较低 |
| 应对特定攻击的安全路由协议 | Song,*et al*[51]<br>Deng,*et al*[3]<br>Kong,*et al*[56]<br>S_LEACH[48] | 单个协议能够抵御一种或少数几种特定类型的攻击 | 同一协议能防范的攻击方式较为单一,协议难以移植、扩展 | 一般 |

## 3　WSN 安全路由研究展望

国内外的研究人员在无线传感器网络安全路由方面做了

大量工作,取得了丰富的研究成果,已提出许多有效的安全路由机制。但是现有研究工作中还存在以下问题需要进一步研究和解决:

a)由于无线传感器网络路由协议的安全缺陷被不断发掘,各种新的针对网络层的攻击方法不断出现并不断演化,必须研究这些新发现的安全缺陷以及路由机制可能面临的新类型攻击,提出新的安全有效的机制去应对和解决这些新出现的路由安全威胁。

b)目前对安全路由协议进行安全性、计算代价和通信代价等方面的分析评价时,往往是根据从特定网络设置中获得的模拟实验数据来进行。不同安全路由协议之间缺乏统一、有效的安全性分析和评估机制,迫切需要针对无线传感器网络路由安全的基础特性建立统一的评估模型,并开发相应的安全评估机制。

c)节点静止的无线传感器网络在一些现实的应用中存在着性能、成本等方面的局限性,因而出现了由人、动物或车辆等移动对象携带的传感器节点所组成的移动传感器网络。与节点静止的无线传感器网络相比,移动传感器网络中节点的移动性导致的网络间断连通、拓扑变化频繁的特性对其路由安全机制提出了新的要求和挑战。然而,现有的研究工作主要是针对节点静止的无线传感器网络,而对于移动传感器网络的路由安全研究较少。

d)目前的安全路由研究中大都假定网络中的传感器节点是同构的。但是在许多应用中,同构传感器节点单一的感知能力、计算能力、通信能力和能量水平难以满足用户对于监测精度、通信性能和降低节点能耗等方面的要求,需要采用多类型传感器节点组成的异构无线传感器网络。但是当前尚缺乏针对异构无线传感器网络安全路由机制的深入研究。

e)在资源受限的无线传感器网络中,路由机制的安全性与资源消耗之间的矛盾始终存在。如何以尽可能小的计算代价、存储代价、通信代价和能量消耗实现满足特定应用要求的安全路由机制将是研究人员持续探求的目标。对于这一问题的解决,无疑需要更具创新性的思想和研究工作。

## 4 结束语

安全问题是无线传感器网络大规模推广和应用必须解决的关键问题之一,而安全路由是无线传感器网络安全研究的重要内容。本文以协议所依据的核心安全策略对现有无线传感器网络安全路由协议进行了划分和归纳,并分类对其中有代表性的重要安全路由协议进行了介绍、分析和讨论。在此基础上,对无线传感器网络安全路由领域需要进一步研究的问题和未来的发展趋势进行了展望。随着无线传感器网络不断进入到实际应用中,人们对其安全性的重视也不断增强,安全路由将会受到更多的关注,该领域的研究也将持续地发展和深入。

**参考文献:**


[1] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: attacks and countermeasures[C]//Proc of the 1st IEEE International Workshop on Sensor Network Protocols & Applications. 2003:113-127.

[2] RAMASWAMI S S, UPADHYAYA S. Smart handling of colluding black hole attacks in MANETs and wireless sensor networks using multipath routing[C]//Proc of Information Assurance Workshop. [S. l.]:IEEE Press, 2006:253-260.

[3] DENG Jing, HAN R, MISHRA S. Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks[C]//Proc of IEEE International Conference on Dependable Systems and Networks. Washington DC:IEEE Computer Society, 2004:637-646.

[4] DOUCEUR J R. The sybil attack[C]//Proc of the 1st International Workshop on Peer-to-Peer Systems. London: Springer-Verlag, 2002: 251-260.

[5] WOOD A D. Denial of service in sensor networks[J]. Computer, 2002, 35(10):54-62.

[6] QI Yue, PEI Qing-qi, ZENG Yong, *et al*. A security approach for WSN protocols based on object-oriented attack model[C]//Proc of the 7th International Conference on Computational Intelligence and Security. Washington DC:IEEE Computer Society, 2011:517-520.

[7] PERRIG A, SZEWCZYK R, TYGAR J D, *et al*. SPINS: security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5):521-534.

[8] CAO Zhen, HU Jian-bin, CHEN Zhang, *et al*. FBSR: feedback based secure routing protocol for wireless sensor networks[C]//Proc of the 20th IEEE International Conference of Advanced Networking and Applications. [S. l.]:IEEE Press, 2006:160-164.

[9] 李小青, 李晖, 杨凯, 等. 一种基于 D-S 证据理论的 Ad hoc 网络安全路由协议[J]. 计算机研究与发展, 2011, 48(8):1406-1413.

[10] SANZIGIRI K, DAHILL B, LEVINE B N, *et al*. Authenticated routing for Ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(3):598-610.

[11] DEMPSTER A P. Upper and lower probabilities induced by a multiblued mapping[J]. Annals of Mathematical Statistic, 1967, 38(2):325-339.

[12] ZAHARIADIS T, LELIGOU H, KARKAZIS P, *et al*. Design and implementation of a trust-aware routing protocol for large WSNs[J]. International Journal of Network Security & Its Applications, 2010, 2(3):52-68.

[13] 王潮, 贾翔宇, 林强. 基于可信度的无线传感器网络安全路由算法[J]. 通信学报, 2008, 29(11):105-112.

[14] 姚兰, 赵志滨, 于戈. 无线传感器网络中基于确定度的安全路由协议的研究[J]. 计算机研究与发展, 2006, 43(Z2):650-654.

[15] 付才, 洪帆, 洪亮, 等. 基于信任保留的移动 Ad hoc 网络安全路由协议 TPSRP[J]. 计算机学报, 2007, 30(10):1853-1864.

[16] GALUBA W, PAPADIMITRATOS P, POTURALSKI M, *et al*. Castor: scalable secure routing for Ad hoc networks[C]//Proc of IEEE INFOCOM. Washington DC:IEEE Computer Society, 2010:1-9.

[17] TANACHAIWIWAT S, DAVE P, BHINDWALE R, *et al*. Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks[C]//Proc of IEEE Workshop on Energy-Efficient Wireless Communications and Networks. [S. l.]:IEEE Press, 2004: 463-469.

[18] ABU-GHAZALEH N, KANG K, LIU Ke. Towards resilient geographic routing in WSNs[C]//Proc of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks. New York:ACM Press, 2005:71-78.

[19] WOOD A, FANG LEI, STANKOVIC J, *et al*. SIGF: a family of configurable, secure routing protocols for wireless sensor networks[C]// Proc of the 4th ACM Workshop on Security of Ad hoc and Sensor Networks. New York:ACM Press, 2006:35-48.

[20] LOU Wei-jing, KWON Y. H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks[J]. IEEE Trans on Vehicular Technology, 2006, 55(4):1320-1330.

[21] LOU Wei-jing. SPREAD: enhancing data confidentiality in mobile Ad hoc networks[C]//Proc of the 23rd Annual Joint Conference on IEEE Computer and Communications Societies. [S. l.]:IEEE Press, 2004: 2404-2413.

[22] LI Yun, REN Jian. Source-location privacy through dynamic routing in wireless sensor networks[C]//Proc of the 29th Conference on Information Communications. Piscataway:IEEE Press, 2010:1-9.

[23] DEFRAWY K E, TSUDIK G. Privacy-preserving location-based on-

demand routing in MANETs[J]. IEEE Journal on Selected Areas in Communications,2011,29(10):1926-1934.

[24] MISRA S,ROY S,OBAIDAT M D,*et al*. A fuzzy logic-based energy efficient packet loss preventive routing protocol[C]//Proc of the 12th International Symposium on Performance Evaluation of Computer & Telecommunication System. Piscataway:IEEE Press, 2009:185-192.

[25] 周贤伟,覃伯平. 基于能量优化的无线传感器网络安全路由算法[J]. 电子学报,2007,35(1):54-57.

[26] ANDEREGG L, EIDENBENZ S. Ad hoc-VCG:a truthful and cost-efficient routing protocol for mobile Ad hoc networks with selfish agents [C]//Proc of the 9th Annual International Conference on Mobile Computing and Networking. New York:ACM Press,2003:245-259.

[27] ZHOU Ji-liang. Efficient and secure routing protocol based on encryption and authentication for wireless sensor networks[C]//Proc of the International Conference on Artificial Intelligence and Education. [S. l.]:IEEE Press,2010:406-409.

[28] LI Wei-chang,LI Hong-ning,XIE Min,*et al*. An identity-based secure routing protocol in WSNs [C]//Proc of the 7th International Conference on Computational Intelligence and Security. Washington DC:IEEE Computer Society,2011:703-706.

[29] GUO Xiao-wang,ZHU Jian-yong. Analysis and design of energy-oriented security protocols for wireless sensor networks[C]//Proc of International Conference on Electronic & Mechanical Engineering and Information Technology. [S. l.]:IEEE Press, 2011:2298-2301.

[30] EL-BENDARY N, SOLIMAN O S,GHALI N I,*et al*. A secure directed diffusion routing protocol for wireless sensor networks[C]//Proc of the 2nd International Conference on Next Generation Information Technology. [S. l.]:IEEE Press, 2011:149-152.

[31] LERON L,LI Yun,REN Jian. Preserving source-location privacy in wireless sensor network using STaR routing[C]//Proc of IEEE Global Telecommunications Conference. 2010:1-5.

[32] AL-KARAKI J N,ALROUSAN M,KHASAWNEH S. On the development of adaptive and self-dependent secure routing protocol(ASSP) for wireless sensor networks[C]//Proc of the 8th International Conference on Advances in Mobile Computing and Multimedia. New York:ACM Press, 2010:288-294.

[33] HU Y,PERRIG A,JOHNSON D B. Ariadne:a secure on-demand routing protocol for Ad hoc networks[J]. Wireless Networks,2005,11(1-2):21-38.

[34] OUADJAOUT A, CHALLAL Y, LASLA N. SEIF:secure and efficient intrusion-fault tolerant routing protocol for wireless sensor networks [C]//Proc of the 3rd International Conference on Availability, Reliability and Security. Washington DC:IEEE Computer Society,2008:503-508.

[35] SAMI D, AL-WAKEEL S,SAAD E,*et al*. PRSA:a path redundancy based security algorithm for wireless sensor networks[C]//Proc of IEEE Wireless Communications and Networking Conference. 2007:4156-4160.

[36] ZHANG Zhi-ming,JIANG Chang-gen,DENG Jian-gang. Multiple-path redundancy secret anonymous routing protocol for wireless sensor networks[C]//Proc of the 6th International Conference on Wireless Communications Networking and Mobile Computing. [S. l.]:IEEE Press,2010:1-4.

[37] ZHANG Yan-chao,LIU Wei,LOU Wen-jing. MASK:anonymous on-demand routing in mobile Ad hoc networks[J]. IEEE Trans on Wireless Communications,2006,5(9):2376-2385.

[38] MOUSTAFA M A,YOUSSEF M A,EL-DERINE M N. MSR:a multipath secure reliable routing protocol for WSNs[C]//Proc of the 9th IEEE/ACS International Conference on Computer Systems and Applications. [S. l.]:IEEE Press, 2011:54-59.

[39] ZHAO Li,DELGADO-FRIAS J G. Multipath routing based secure data transmission in Ad hoc networks[C]//Proc of International Conference on Wireless and Mobile Computing,Networking and Communications. [S. l.]:IEEE Press,2006:17-23.

[40] 姚兰,罗磊,高福祥. 基于恶意节点检测的多路径安全路由协议[C]//中国控制与决策会议论文集. 2009:4323-4328.

[41] TRIKI B, REKHIS S, BOUDRIGA N. A novel secure and multipath routing algorithm in wireless sensor networks[C]//Proc of the International Conference on Data Communication Networking. [S. l.]: IEEE Press, 2011:1-10.

[42] SRINATH R, REDDY A V, SRINIVASAN D R. AC:cluster based secure routing protocol for WSN[C]//Proc of the 3rd International Conference on Networking and Services. Washington DC:IEEE Computer Society,2007:45.

[43] FAN Rong,CHEN Jian,FU Jian-qing,*et al*. A striner-based secure multicast routing protocol for wireless sensor network [C]//Proc of the 2nd IEEE International Conference on Future Networks. Washington DC:IEEE Computer Society,2010:159-163.

[44] PIETRO R D, MANCINI L V, LAW Y W,*et al*. LKHW:a diretcted diffusion-based secure multicast scheme for wireless sensor networks [C]//Proc of International Conference on Parallel Processing. [S. l.]:IEEE Press,2003:397-406.

[45] KUMAR S,JENA S. SCMRP:secure cluster based multipath routing protocol for wireless sensor networks[C]//Proc of the 6th International Conference on Wireless Communication and Sensor Networks. [S. l]:IEEE Press, 2010:1-6.

[46] DENG Jing,HAN R,MISHRA S. INSENS:intrusion-tolerant routing for wireless sensor networks[J]. Computer Communications,2006,29(2):216-230.

[47] LEE S,CHOI Y. A secure alternate path routing in sensor networks [J]. Computer Communications,2006,30(1):153-165.

[48] MOHI M,MOVAGHAR A,ZADEH P. A Bayesian game approach for preventing DoS attacks in wireless sensor networks[C]//Proc of International Conference on Communications and Mobile Computing. [S. l.]:IEEE Press, 2009:507-511.

[49] NAHAS H A,DEOGUN J S,MANLEY E D. Proactive mitigation of impact of wormholes and sinkholes on routing security in energy-efficient wireless sensor networks [J]. Wireless Networks, 2009, 15(4): 431-441.

[50] PAPADIMITRIOU A,FESSANT F L,VIANA A C,*et al*. Cryptographic protocols to fight sinkhole attacks on tree-based routing in wireless sensor networks[C]//Proc of the 5th IEEE Workshop on Secure Network Protocols. [S. l.]:IEEE Press,2009:43-48.

[51] SONG Ning,QIAN Li-jun,LI Xian-fang. Wormhole attacks detection in wireless Ad hoc networks:a statistical analysis approach[C]//Proc of the 19th International IEEE Parallel and Distributed Processing Symposium. Washington DC:IEEE Computer Society,2005:289-296.

[52] ZHANG You-tao,YANG Jun,VU H T. The interleaved authentication for filtering false reports in multipath routing based sensor networks [C]//Proc of the 20th International IEEE Parallels and Distributed Processing Symposium. Washington DC: IEEE Computer Society, 2006:26.

[53] ZHU Sen-cun,SETIA S,JAJODIA S,*et al*. An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC:IEEE Computer Society,2004:259-271.

[54] CHEN Jia-wei. Broadcast authentication protocol scheme based on DBP-MSP and safe routing in WSN against DDoS attacks[C]//Proc of the 2nd International Conference on Networking and Distributed Computing. [S. l.]:IEEE Press, 2011:170-174.

[55] CLAYCOMB W,LOPES R,SHIN D. A group-based security policy for wireless sensor networks[C]//Proc of ACM Symposium on Applied Computing. New York:ACM Press,2010:778-785.

[56] KONG Jie-jun,HONG Xiao-yan, YI Yun-jung,*et al*. A secure Ad hoc routing approach using localized self-healing communities[C]//Proc of the 6th ACM International Symposium on Mobile Ad hoc Networking and Computing. New York:ACM Press,2005:254-265.