传感器网络安全技术

物理层

物理层的攻击主要集中在物理破坏、节点捕获、信号干扰、窃听和篡改等。攻击者可以通过流量分析,发现重要节点如簇头、基站的位置,然后发动物理攻击。

- 信号干扰和窃听攻击：因为低成本的传感器网络很容易遭受信号扰和窃听攻击。其防御对策有**扩频通信**,如跳频如果干扰不是持续的,在非干扰间歇内可以发送优先级高的信息来降低干扰破坏程度另一种方法是切换到其他通信方式如红外线、光等。其缺点是成本比较高。而防止窃听攻击的有效方法是**对敏感通讯信息进行加密**。
- 篡改和物理破坏攻击：由于传感器节点分布,成本低,很容易物理损坏或被捕获,因此一些加密密钥和机密信息就一可能被破坏或泄漏,攻击者甚至可利用获得的信息对整个网络进行攻击,如篡改报文内容。而攻击者能够篡改路由报文的根本原因在于节点无法对路由报文**进行完整性检测**,因此对付篡改攻击的方法是对整个路由报文或其中的关键信息、**加入报文鉴别码**。节点在收到路由报文之后,先进行完整性检测,通过后能进行下一步处理,以防止报文被非法篡改。另外,还**需要结合入侵检测系统找到并清除这些被捕俘节点,更新加密密钥**。在实际应用中,对节点进行物理伪装和隐藏也是躲避物理破坏攻击的有效方法。
- 仿冒节点攻击：因为很多路由协议并不认证报文的地址,所以攻击者可以声称为某个合法节点而加入网络,甚至能够解蔽某些合法节点,替它们收发报文。造成这种攻击的根本原因是节点未能鉴别报文的来源。因此对付仿冒节点，攻击的有效方法是网络**各节点之间进行相互认证**。对于节点的行为首先要进行**身份认证,确定为合法节点才能接收和发送报文**。

链路层

链路层比较容易遭受攻击,攻击者可以通过分析流量来确定通信链路,发动相应攻击,如对主要通信节点如簇头发动资源消耗攻击。

- 链路层冲突攻击：攻击者通过花费很小的代价可实行链路层冲突攻击。例如发送一个字节的报文破坏正在传送的正常数据包,从而引起接受方校验和出错,进而在一些协议中认为链路层冲突,引发指数退避机制,造成网络延迟,甚至瘫痪。校错码虽然具有一定的纠错能力,但是如果攻击者恶意破坏数据包的较多数据位,校错码将无法纠正这些数据位而失效,并且校错码本身也会产生额外的处理和通信开销,造成网络负荷过重。冲突检测机制虽然能检测出冲突节点,但难以判断冲突节点是否为恶意节点,因此,关于链路层攻击的防御机制仍需进一步的研究。
- 资源消耗攻击：攻击者发送大量的无用报文消耗网络和节点资源,如带宽、内存、CPU、电池等。例如剥夺睡

眠攻击,攻击者不停发送报文,使得一节点的电源很快耗尽,从而达到DoS攻击效果。这种攻击的防御方法之一是在MAC层**限制节点发送数据报的速度**,使得攻击者不能发送大量的无用报文。另外**邻居节点也可以监视节点的反常行为,降低频繁发送报文节点的发送优先级**。

网络层

路由信息的欺骗、篡改或回放攻击主要是通过改变两个节点之间的路由信息进行攻击。攻击者可以伪造并广播假的路由信息。例如广播某条存在的路山已中断,或编造一条并不存在的路由。这类攻击可造成路由回路、分割网络、孤立节点、增长和缩短路由路径、增加端到端的延迟、吸引或排斥通信流鼠造成网络流量不均衡等后果。其根本原因在于节点无法验证报文的内容。因为要随时一掌握整个网络的连通情况,刁`能辨别某个节点所发出信息的真假,因此防比伪造路山攻击比较困难,防御方法主要是通过入侵检测系统来检测和清除这些入俊二竹点。

- RUSHING攻击：在按需路由协议中,节点路由查询时经常采用泛洪查询,能会导致个节点收到多个相同的路由查询报文,这时节点只会处理第一个到达的路由查询报文,而将其他相同的路由查询报文抛弃。攻击就利用这个弱点,攻击者比其他节点更快地转发路由查询报文,使得其他节点首先收到它转发的报文。这将导致两个问题,其一,攻击者短时间内发送大量的路由查询,令其遍布整个网络,从而使得其它节点正常的路由查询由于无法提交处理而被抛弃其二,所有建立的路由都要通过攻击者。提出了通过随机转发的方法防御攻击。其方法是将节点只处理第一个收到的路由查询报文并抛弃随后到达的相同路由查询报文,改变为**节点收集一定数量的相同路由查询报文,然后选择其中任意一个进行处理**,以阻止攻击。
- 选择性转发攻击：恶意节点拒绝转发包,但是为了防止被发现,可能会选择性地发些包或将一些报文修改后再转发。多路径路由能有效减少由于这种攻击所造成的信息丢失。另外,**邻居节点和基站能监视这种行为,降低向这种容易丢包的节点转发包的优先级**。
- 黑洞攻击：攻击者引诱其他节点向它发包,从而创造以攻击者为中心的一个黑洞。**比较典型的攻击方法是攻击者让其他节点根据路由算法相信它是最好的转发选择,从而吸引其他节点向它发包**。例如,一个攻击者可以通过伪造或回放一个广告,以示它有十分高质量的路由到基站。等到吸引到其他节点向它发包后,再进行其他攻击,如进行选择性转发攻击。**该类攻击可采用随机密钥预分配机制和基站入侵检测与响应系统进行防御**。
- 巫师攻击：是指**一个攻击节点假冒多个合法节点的身份**。巫师攻击能有效地降低容错机制性能如分布存储,多路径路由和拓扑维护。巫师攻击对基于位置的路由协议的安全也能产生很大的威胁。因为基于位置的路由需要交换彼此的位置信息,一个巫师攻击节点可以使得其他节点相信很多位置上有它存在,从而导致路由混乱。建立对密钥能使得任意两个邻居节点相互验证,即使节点被捕获,巫师攻击也不能对其他邻居节点进行攻击。建议通过资源测试来确认一个物理节点的唯一身份。分析了这种攻击的多种攻击形式和防御方法,如通过无线波资源测试的方法、随机密钥预分配机制、节点注册、节点位置验证、代码验证即通过检查节点内存里面运行代码来验证节点是否为合法节点等方法。
- 蠕虫洞攻击：是攻击者把收到的包通过延迟很小的隧道发送到隧道另一端,在隧道的另端进行回放攻击。定义两个攻击者之间的隧道为蠕虫洞。图一所示是一个攻击者在基站附件产生一个黑洞,配合另一个攻击节点在离基站比较远的地方进行回放攻击。蠕虫洞攻击能破坏路由竞争条件,路由竞争条件是指当一个节点收到一个消息报以后,对随后干同的包进行简单的丢弃。另外,蠕虫洞攻击还可导致路山拓扑混乱,通过端虫洞转发包,可

以使得两个远距离的节点认为是相邻的。蠕虫洞攻击也可以和其他攻击,夕选择性转发攻击相结合,检测这种攻击十分困难。文献专门提出一种报文约束方法来抵抗蠕虫洞攻击,原理是基于精确的时间或位置信息来发现并阻止蠕虫洞攻击。基于时间约束的方法是给每个发出的报文打时间戳,接收时对比一下时间,将报文发送与接收控制在一定时间内。基于空间约束的方法是利用信息,报文发送时带上位置信息,接收时可查看其发送趾离,防止传送过远,将报文发送与接收控制在一定空间范围之内。

传输层攻击

- 泛洪攻击：攻击者**通过泛洪发送大量攻击报文**的方式,导致整个网络性能下降,不能正常通信。例如经典的TCP SYN Flooding攻击,攻击者通过发送大量假的连接到某个节点,导致单个节点不能正常工作。当然对于无连接的协议不存在这种攻击。一种解决方案是要求客户成功回答服务器的若干问题后再建立连接,它的缺点是要求合法节点进行更多的计算、通讯和消耗更多的能量。另一种方案是**引入入侵检测机制,基站限制这些泛洪攻击报文的发送**。如规定在一定时间内,节点发包数量不能超过某个阈值。
- 同步破坏攻击：传感器网络通常**采用同步机制进行通信,攻击者通过不断地伪造消息发给已经建立通信连接的节点**。这些伪造的消息可能包含序列号或控制标志以引起连接的两节点由于误认为帧丢失而要求重新传输。如果攻击者能控制同步时间机制,就能引起两个节点进行无休止的同步恢复协议。这种攻击可以通过**报文鉴别码对所有报文传输协议中包头的控制部分进行鉴别**,发现并防止攻击者通过伪造报文来破坏同步机制。

> “

安全技术			网络分层	安全威胁	
跨层安全协议	信任模型	密钥管理 加密技术	应用层		拒绝服务攻击
		传统网络 安全技术	传输层	针对传输 数据的攻击	
		同步和定位安全 安全路由 安全数据融合	网络层	针对传输 数据的攻击 伪装攻击	
		入侵检测 扩频技术 基于固定分配的 安全 MAC 协议	数据链路层	针对传输 数据的攻击	
		入侵检测	物理层	物理攻击	

1. 针对传输数据的攻击是最常见最普通的攻击方法，针对传输数据的攻击主要是针对信道中传输的数据进行攻击，攻击者利用监听设备窃听信道，窃取或修改数据。
2. **物理攻击是针对节点物理安全的攻击。由于节点部署在广阔的空间，并且对于特定的领域的应用，节点的物理安全无法保证。对手可以通过监听信道来确定发射源的位置，从而俘获节点，破解节点存储的数据和保存的密钥。对手可以将修改后的节点重新注入到网络中，如果缺少相应的安全策 略，网络误将被俘节点当作合法节点，整个网络的安全会受到威胁和破坏。**（防篡改与认证）
3. 伪装攻击是恶意节点伪装多个身份或复制多个相同身份来实现的，女巫攻击和复制攻击是典型的伪装攻击。女巫攻击能较大地降低容错方案的效率，如分布式储存、分散性、多路径和拓扑结构维护。可以用来区分节点的拷贝、存储划分或路由实际上都可以被一个攻击者利用而呈现多个身份。

4. 拒绝服务攻击（Dos）的目的是削弱或破坏网络的服务，破坏节点间的协同工作。拒绝服务攻击包括针对节点的攻击和针对信道的攻击，分别是针对节点和无线声信道的攻击。Dos攻击具有低成本、难发现、致命性等特点。相对于其它类型的攻击，由于信道特性和传感器网络的局限性，Dos攻击对传感器网络造成更大的威胁和破坏。

协议层	DoS 攻击	防御方法
传输层	泛洪攻击	基于固定分配的协议
	失步攻击	认证技术 安全时钟同步协议
网络层	丢弃贪婪攻击	减少路由跳数
	汇聚攻击	加密技术 认证技术
	方向误导攻击	出口过滤 认证技术 监测机制
	黑洞攻击	认证技术
	虫洞攻击	安全路由
数据链路层	冲突攻击	重传机制 冲突检测机制 安全 MAC 协议
	耗尽攻击	限制重传次数 安全 MAC 协议
	不公平性	短帧策略
物理层	拥塞攻击	睡眠-唤醒机制 扩频与多址接入技术
	物理破坏	防篡改机制 隐藏伪装节点

主要针对于网络通信方面：

- 密码技术和密钥管理：目前主要使用是对称密码算法。但是在特定情况下，如访问控制等也使用低开销的非对称密码算法。在对称密码中，消息认证码(MAC)和 hash 被广泛使用，如消息/身份认证通过 MAC 来进行，而不是传统的数字签名方式。
- 入侵检测：入侵检测及响应能够及时发现入侵行为并采取应对措施，是保障网络安全的一个重要手段，作为一种积极主动的技术，它能在系统受到危害时及时告警。入侵检测通常使用两种基本的分析方法来检测入侵行为，即误用检测和异常检测。误用检测对不正常的行为进行建模，形成入侵和误用特征库，检查收集的数据中是否包含入侵特征。异常检测通过对正常行为建模，将所有偏离正常行为的事件定义为异常。传感器网络面临着多种多样的入侵，按照入侵者的类型可以分为内部和外部入侵。外部入侵中，入侵者不知道传感器网络内部信息，如传感器节点的密钥信息、各种参数等，不能直接入侵网络中的节点。内部入侵是指攻击者伪装成网络中的合法节点进行的入侵。入侵者既可以是网络中被攻击者攻陷的合法传感器节点，也可以是攻击者在获得合法节点信息后注入网络中的伪节点。简单的密码技术仅仅能够识别外来非法节点的入侵而无法识别那些被捕获节点的入侵，因为这些被捕获节点和正常节点一样具有加解密和认证身份所需的密钥。文献提出了一种基于安全协议的入侵检测系统，该系统把大量的监测任务交给功能更加强大的基站完成，选取针对网络层的安全协议作为入侵检测点，并利用路由拓扑信息资源。然而该系统是基于查询式无线传感器网络模型，假设网络中节点均匀分布、基站位于网络中心位置，基站具有足够的能量资源、较强的计算和存储能力；网络是不安全的，可能受到各种入侵攻击，但基站是安全的。然而这种假设在实际应用中很难满足，无法保证所有节点均匀分布也无法保证基站的绝对安全。

- 身份认证技术：身份认证技术是任何安全体系 中的不可或缺的重要组成部分．身份认证技术主要用来确定新加入节点的合法性，区别恶意侵入者，确定节点请求和服务的合法性．身份认证技术能有效防御大部分Dos攻击．因此，设计一种适合、健全的身份认证体系能有效保护网络的安全，保持网络的效能。
- 防篡改机制：当节点感知到自己 被恶意攻击者俘获、篡改，会自动清除所有程序和保 存的数据以及密钥，防御篡改攻击。
- 同步和定位安全
- 路由安全

认证与访问控制

认证指使用者采用某种方式来“证明”自己确实是自己宣称的某人, 网络中的认证主要包括身份认证和消息认证。身份认证可以**使通信双方确信对方的身份并交换会话密钥**。保密性和及时性是认证的密钥交换中两个重要的问题。为了防止假冒和会话密钥的泄密, 用户标识和会话密钥这样的重要信息必须以密文的形式传送, 这就需要事先已有能用于这一目的的主密钥或公钥。因为可能存在消息重放, 所以及时性非常重要, 在最坏的情况下, 攻击者可以利用重放攻击威胁会话密钥或者成功假冒另一方。

消息认证中主要是接收方希望能够**保证其接收的消息确实来自真正的发送方**。有时收发双方不同时在线, 例如在电子邮件系统中, 电子邮件消息发送到接收方的电子邮件中, 并一直存放在邮箱中直至接收方读取为止。广播认证是一种特殊的消息认证形式, 在广播认证中一方广播的消息被多方认证。

传统的认证是区分不同层次的, 网络层的认证就负责网络层的身份鉴别, 业务层的认证就负责业务层的身份鉴别, 两者独立存在。**但是在物联网中, 业务应用与网络通信紧紧地绑在一起, 认证有其特殊性。**例如, 当物联网的业务由运营商提供时, 那么就可以充分利用网络层认证的结果而不需要进行业务层的认证;或者当业务是敏感业务如金融类业务时, 一般业务提供者会不信任网络层的安全级别, 而使用更高级别的安全保护, 那么这个时候就需要做业务层的认证;而当业务是普通业务时, 如气温采集业务等, 业务提供者认为网络认证已经足够, 那么就不再需要业务层的认证。

在物联网的认证过程中, 传感网的认证机制是重要的研究部分, 无线传感器网络中的认证技术主要包括 基于轻量级公钥的认证技术、预共享密钥的认证技术、随机密钥预分布的认证技术、利用辅助信息的认证、基于单向散列函数的认证 等。

基于轻量级公钥算法的认证技术

基于公钥，算法更简单、安全性更高，是目前主要的身份认证方式。主流的公钥认证方式包括 椭圆曲线密码 和 双线性映射 等。

鉴于经典的公钥算法需要高计算量, 在资源有限的传感器网络中不具有可操作性, 当前有一些研究正致力于对公钥算法进行优化设计使其能适应于无线传感器网络, 但在能耗和资源方面还存在很大的改进空间, 如基于RSA公钥算法的TinyPK认证方案, 以及基于身份标识的认证算法等。

基于预共享密钥的认证技术

基于共享密钥的认证方式，由于对网络负担比较大，一般存在于密钥预分配中身份认证的方式，主要包括两方参与的身份认证和三方参与的身份认证。两方参与的身份认证主要是节点与节点之间的身份认证；三方参与的身份认证根据网络模式包括，节点、KDC（或者基站）和用户之间的身份认证，节点、簇头节点和用户之间的身份认证，以及节点、注册基站和非注册基站之间的身份认证等。

SNEP (Secure Network Encryption Protocol)方案中提出两种配置方法:一是节点之间的共享密钥, 二是每个节点和基站之间的共享密钥。这类方案使用每对节点之间共享一个主密钥, 可以在任何一对节点之间建立安全通信。缺点表现为扩展性和抗捕获能力较差, 任意一节点被俘获后就会暴露密钥信息, 进而导致全网络瘫痪。

表 3.1　SPINS 用到的参数

参数名称	参数意义
A, B	认证参与主体
N_A	由 A 生成的随机变量
X_{AB}	主体 A、B 共享的主密钥
K_{AB} 和 K_{BA}	主体 A、B 共享的加密密钥
K'_{AB} 和 K'_{BA}	主体 A、B 共享的 MAC 加密密钥
$[M]_{K_{AB}}$	用密钥 K_{AB} 加密过的信息 M
$[M]_{(K_{AB},IV)}$	用密钥 K_{AB} 和初始矢量 IV 加密过的信息 M，初始矢量 IV 这里代表一个序数。
$MAC(K'_{AB}, M)$	用 K'_{AB} 生成的信息 M 的 MAC。

$$A \rightarrow B : [D]_{(K_{AB}, C_A)}, MAC\left(K_{AB}, C_A \| [D]_{(K_{AB}, C_A)}\right)$$

BROSK 比起 SPINS 更加低能耗。而且，认证方式也更加简单。K 为所有节点共享的主密钥，IDi 为节点 i 的身份，Ni 为节点 i 生成的随机变量， MACk(M)为信息 M 经过密钥 K 加密后得到的 MAC。BROSK 过程如下：

1，A 广播信息 M_1： $ID_A \| N_A \| MAC_K\left(ID_A \| N_A\right)$；

2, B 接收到 A 广播的信息后，发送给 A 信息 M_2： $ID_B \| N_B \| MAC_K\left(ID_B \| N_B\right)$；

3, A 和 B 计算共享的会话密钥 $K_{AB} = MAC_K\left(N_A \| N_B\right)$。

基于单向散列函数的认证方法

该类方法主要用在广播认证中, 由单向散列函数生成一个密钥链, 利用单向散列函数的不可逆性, 保证密钥不可预测。通过某种方式依次公布密钥链中的密钥, 可以对消息进行认证。目前基于单向散列函数的广播认证方法主要是对μTESLA协议的改进。μTESLA协议以TESLA协议为基础, 对密钥更新过程, 初始认证过程进行了改进, 使其能够在无线传感器网络有效实施。

μTESLA 使用单向密钥链，通过对称密钥的延迟透露引入的非对称性进行广播认证，其由 4 个阶段组成：(1) 密钥建立(2) 广播密钥透露(3) 传感器节点自举(4) 认证广播数据包。