无线传感器（WSN）的安全

安全技术介绍

一、传感器网络安全防护主要手段

信息加密	对通信信息进行加密，即对传感器网络中节点与节点之间的通信链路上的通信数据进行加密，不以明文数据进行传输，即使攻击者窃听或截取到数据，也不会得到真实信息
数据校验	数据接收端对接收到的数据进行校验，检测接收到的数据包是否在传输过程中被篡改或丢失，确保数据的完整性。优秀的校验算法不仅能确保数据的完整性，也能够确保防止攻击者的重放攻击
身份认证	为确保通信一方或双方的真实性，要对数据的发起者或接收者进行认证。认证能够确保每个数据包来源的真实性，防止伪造，拒绝为来自伪造节点的信息服务

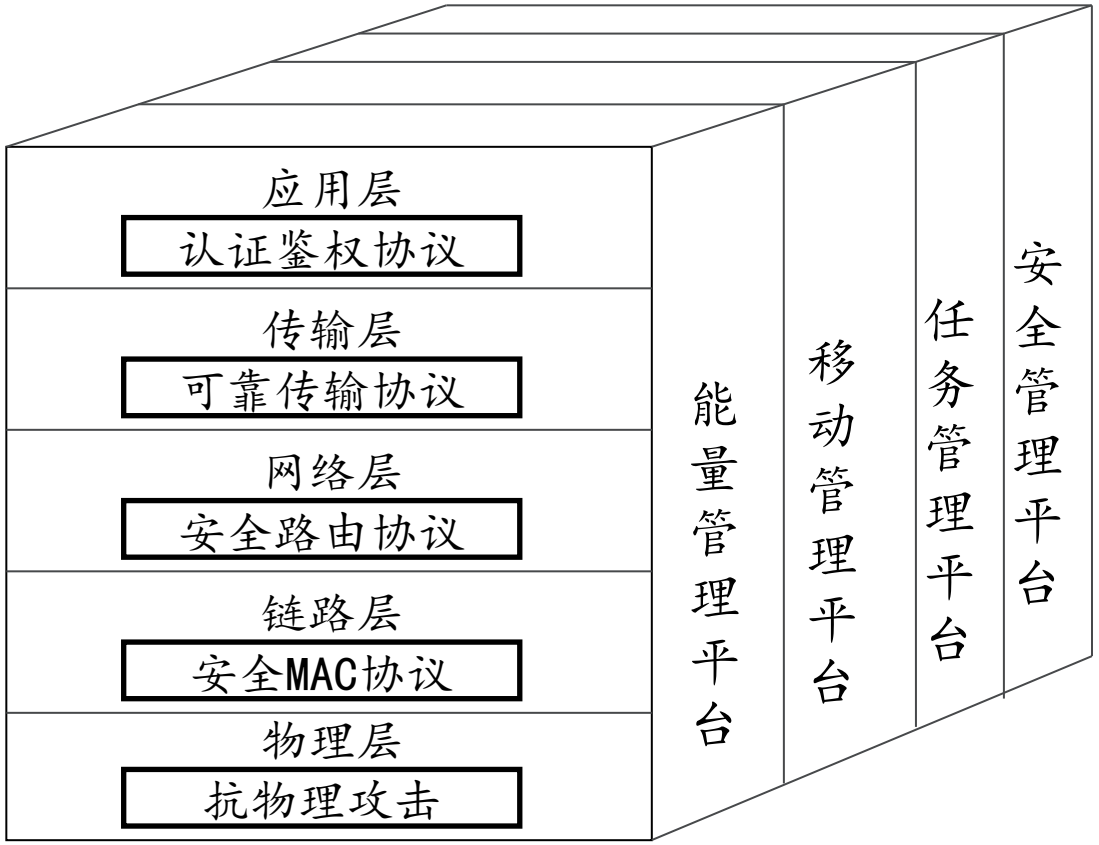
一、传感器网络安全防护主要手段

扩频与跳频	在无线通信中使用扩频或跳频，增加了通信信道，可以容纳更能多的节点进行同时通信，减少冲突和延迟，也可以防御攻击者对通信链路的窃听和截取
安全路由	在传感网络中要充分考虑路由安全、防止节点数据、基站数据泄露，同时不给恶意节点、基站发送数据，防止恶意数据入侵。 传统网络路由安全不是重点。
入侵检测	安全防护技术要能够实现传感器网络的入侵检测，防止出现由于一个节点的暴露而导致整个网络瘫痪的危险

二、传感器网络典型安全技术

1、传感器网络安全协议增强技术

WSN协议栈，包括物理层、数据链路层、网络层、传输层和应用层，与互联网的五层协议相对应。WSN协议还包括能量管理平台、移动管理平台和任务管理平台。设计并实现通信安全一体化的传感器网络协议栈，是实现安全传感器的关键。安全一体化网络协议栈能够整体上应对传感器网络面临的各种安全威胁，达到“1+1>2”的效果。



（传感器网络通信安全一体化协议栈）

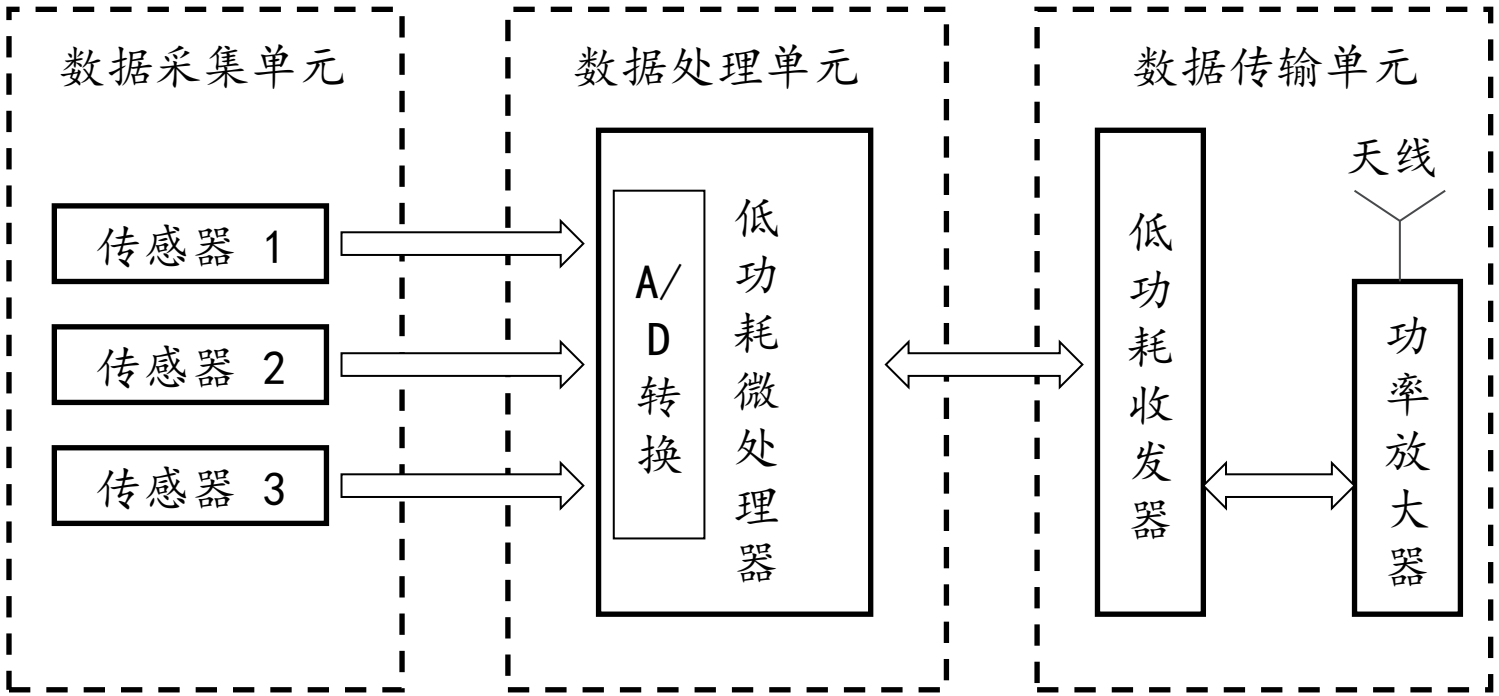
二、传感器网络典型安全技术

1） 物理层安全设计

物理层主要指传感器节点电路和天线部分：

(1) 节点设计

安全WSN节点主要由数据采集单元、数据处理单元及数据传输单元三部分组成，如下图所示：



二、传感器网络典型安全技术

节点设计应该考虑的因素

安全WSN 节点软硬件结构设计	硬件设计主要设计原则是：低功耗。在软件方面，可以关闭数据采集单元和数据传输单元，并将数据处理单元转入休眠状态。在硬件方面，可以采用太阳能补充能量。
微处理器和射频芯片的选择	通过对国际上安全WSN节点性能的分析，根据节点的总体设计需求，选择最合适的节点射频芯片和处理器。
微处理器与射频芯片之间的连接	主要是实现微处理器与射频芯片之间的低功耗全双工高速通信。
射频电路的设计	节点在信号发送和接收时功耗最大。通过合适的电路设计，还可以增大节点的通信距离，增强传感器网络的功能。
数据采集单元的设计	采集单元主要包括各种传感器，传感器的选择应以低功耗为原则，同时要求传输体积尽量小，信号的输出形式为数字量，转换精度能够满足需求。

二、传感器网络典型安全技术

(2) 天线设计

由于WSN的设备大多要求体积小、功耗低，因此在设计该类无线通信系统时大多采用**微带天线。**

- **微带天线优点：**具有体积小、质量小、电性能多样化、易集成、能与有源电路集成为统一的组件等众多优点。
- **微带天线缺点：**受其结构和体积限制，存在频带窄、损耗较大、 增益较低、大多数微带天线只向半空间辐射、功率容量较低等缺陷。

倒F天线：适用于IEEE802.15.4标准，该标准是针对低速无线个人区域网络制定的，其把低能量消耗、低速率传输、低成本作为重点目标，为个人或者家庭范围内不同设备之间低速互连提供统一标准。

倒F天线优点：满足结构紧凑、价格低廉、易于加工、通信效果良好的无线传感器网络节点的典型要求。

二、传感器网络典型安全技术

2） 链路层安全协议

媒体访问控制协议（MAC）处于WSN的底层，是保证WSN高效通信的关键网络协议之一。

S-MAC：在802.11协议基础上针对传感网网络的节省能量需求而提出的传感器网络MAC协议。

SSMAC协议（Secure Sensor MAC)是在S-MAC发展起来的。针对S-MAC协议的安全缺陷，SSMAC基于NTRUsign数字签名算法，实现了数据完整性、来源真实性和抵御重放攻击的安全目标。

二、传感器网络典型安全技术

NTRU公钥密码体制简介

1996年 3位美国数学家发明了 NTRU (Number Theory Research Unit)公钥密码体制,经过几年的迅速发展与完善 ,该算法在密码学领域中受到了高度的重视并在实际应用中取得了很好的效果.由于NTRUsign公钥机制只使用简单的模乘法和模求逆运算，因此加/解密速度很快，密钥生成也很快。

NTRU算法的安全性是基于数论中在一个非常大的维数格中寻找一个很短向量的数学难题. 就目前来说 ， NTRU的安全性和目前最有影响的 RSA算法、椭圆曲线加密体制 ECC等算法是一样安全的。 在相同安全级的前提下 ， NTRU算法的速度要比其它公开密钥体制的算法快 ,用 Tumbler(tm)软件工具包执行 NTRU时的速度比 RSA 快 100多倍。用 NTRU 算法产生密钥的速度也很快 ， NTRU密钥的 bit数也较小。NTRU算法的优点意味着可以降低对带宽、处理器、存储器的性能要求 ,这也扩大了 NTRU公开密钥体制的应用范围。

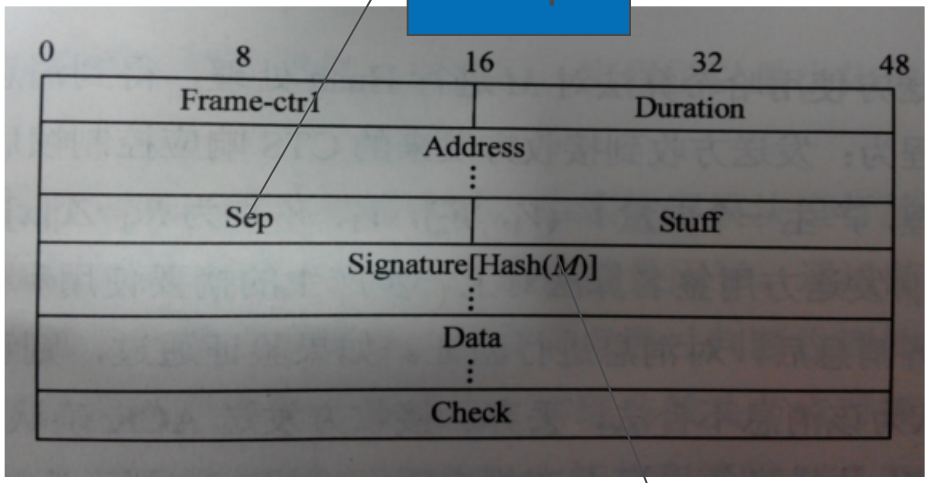
二、传感器网络典型安全技术

S-MAC是在802.11基础上根据节省能量的要求提出的传感器网络MAC协议。

（1）帧格式设计

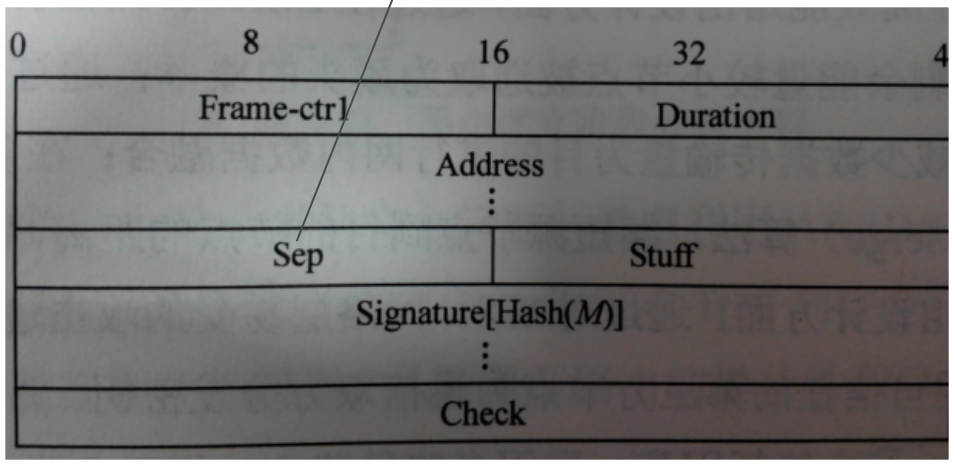
MAC层帧结构设计的目标是用最低复杂度实现S-MAC的可靠传输，帧结构设计的好坏直接影响整个协议的性能。**每个MAC子层的帧都由帧头、负载和帧尾三部分构成。**

seq



SSMAC数据帧格式

ACKID



ACK确认帧格式

M表示{Seq,Address,Frame-Ctrl}；
Hash（M）：用SHA-1对M进行运算
Signature[Hash(M)]:签名

二、传感器网络典型安全技术

（2）协议流程

针对碰撞重传、串音、空闲侦听和控制消息等可能造成传感器网络消耗更多能量的主要因素，S-MAC协议采用以下机制：

① 采用周期性侦听/睡眠的低占空比工作方式，控制节点尽可能处于睡眠状态来降低节点能力的消耗；

② 邻居节点通过协商的一致性睡眠调度机制形成虚拟簇，减少节点的空闲侦听时间；

③ 通过流量自适应的侦听机制，减少消息在网络中的传输延迟；

④ 采用带内信令来减少重传和避免监听不必要的数据等

二、传感器网络典型安全技术

SSMAC协议流程：

①A → B:RTS;//发送方发送RTS帧(请求)给B

②B → A:CTS;//接收方发送CTS响应（空闲响应）控制帧给A

③A:H(M);//发送方对M进行Hash处理

④A:Eska[H(M)];//发送方对摘要私钥进行数字签名

⑤目的节点B收齐消息后，对消息进行验证。如果验证通过，则认为该信息合法；否则不合法，丢弃。B向A发送确认帧ACK及其签名给A。若A在规定时间内没有接收到确认帧ACK，就必须重传消息，直到接收到确认，或者经过若干次重传失败后放弃。

本节的数据链路层的安全是通过SSMAC协议实现，是重点。SSMAC是在S-MAC的基础上，采用NTRU数字签名技术，实现数据的完整性、防抵赖性和防重放攻击。

二、传感器网络典型安全技术

3）网络层安全路由协议SEC-Tree

由于WSNs网络能量资源易受限，且易受外界干扰和攻击，设计高效且安全的WSNs网络路由协议成为研究热点

网络层安全核心问题：

1、簇管理

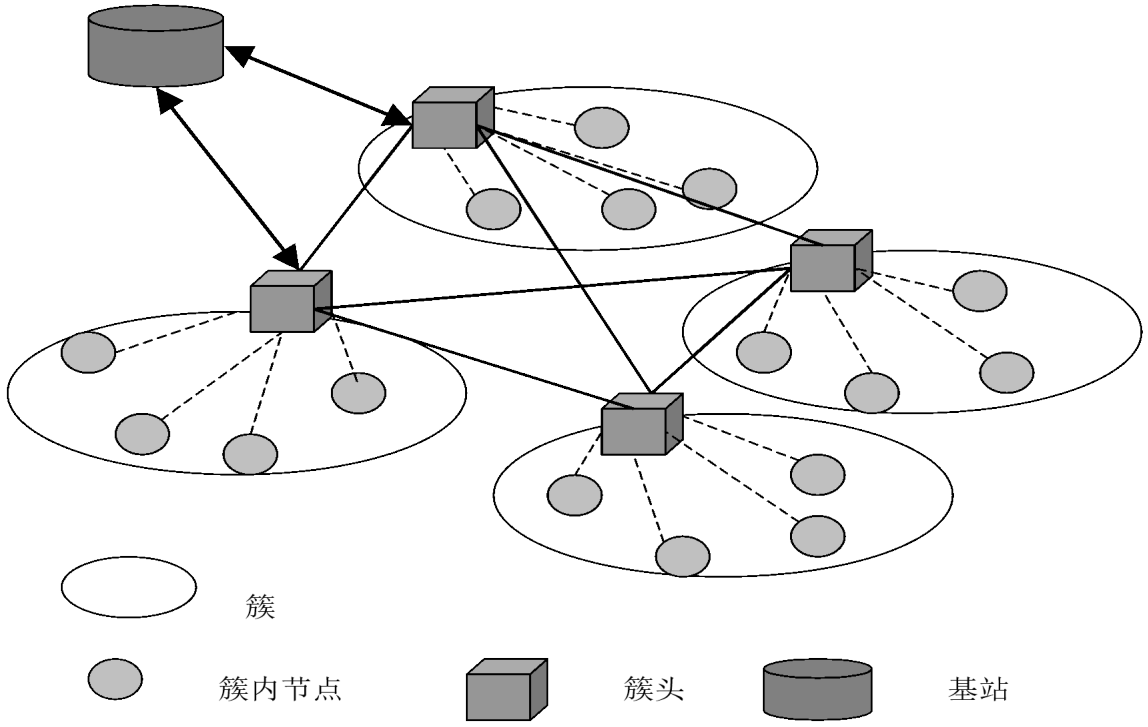
2、多跳路由

3、多路径路由

4、认证

5、密钥管理

6、数据融合机制



二、传感器网络典型安全技术

3）网络层安全路由协议SEC-Tree

目前WSNs路由协议大致分为基于层次的路由协议、以数据为中心的路由协议以及基于地理位置的路由协议。

SEC-Tree路由协议:一种在传统层次路由协议基础上设计的高效安全的路由机制。该协议克服了传统层次路由协议采用单跳通信、扩展性差、不适合大规模网络的缺点，并引入了身份鉴别机制，具有高效安全的特征。

二、传感器网络典型安全技术

(1) 总体框架

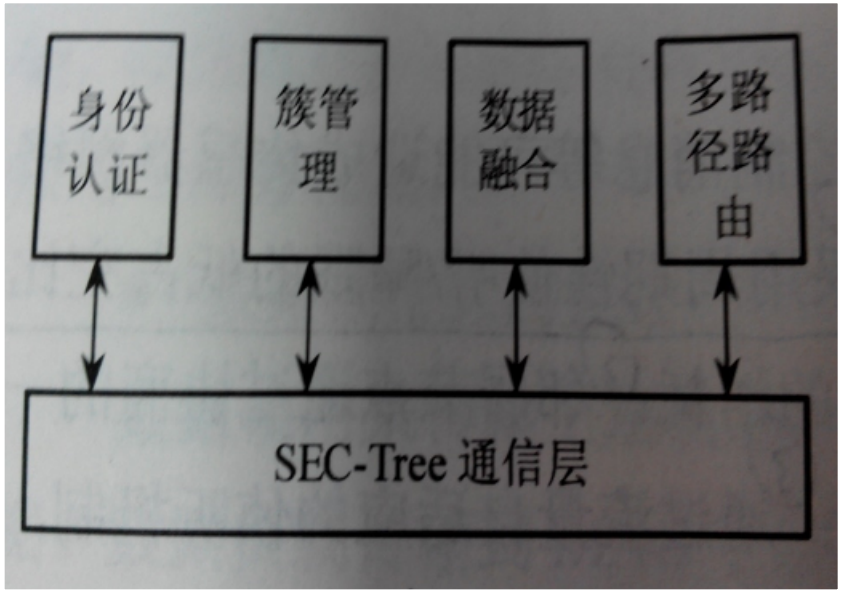
SEC-Tree协议在LEACH协议的基础上，引进**“剩余能量因子”**和**“数据特征码”**；在认证方面采用**改进的SNEP协议**，采用**可信第三方分发密钥**，采用**加随机数认证机制**；在多跳机制中采用ECM（Energy-Considering Merge）算法，**缩短通信节点的距离**，**减少数据传递能耗**，构建SEC-Tree路由机制。

SEC-Tree协议是一个**高效率、高安全和高可靠的WSN 路由协议**，它通过改进的**分簇机制、数据融合机制、多路径路由机制实现SEC-Tree路由协议的高效能**，通过密钥机制和多路径机制实现安全可靠的路由协议。

低功耗自适应分层性协议（(Low Energy Adaptive Clustering Hierarchy）：以循环的方式随机选择簇头节点，将整个网络的能量负载平均分配到每个传感器节点中，从而达到降低网络能源消耗、提高网络整体生存时间的目的。

二、传感器网络典型安全技术

1、身份认证模块：采用改进的SNEP（传感器网络加密协议），为簇管理、多跳路由、多路径路由、数据信息的传递与融合提供安全机制；
2、簇管理模块内置SEC-Tree簇形成算法ECM，实现基于剩余能量机制的簇头选择，周期性维护基于簇拓扑的结构；
3、多跳路由机制实现基于SEC-Tree的层次化路由算法，选择最短路径路由，自适应更改路由表，能够提高网络传播效率；



4、多路径路由在路由的建立和维护阶段，建立冗余的数据通道，提高路由的安全性，包括容错自适应策略、时延能耗自适应策略和安全自适应策略三个策略子模块；
5、数据融合模块内置基于数据特征码的高效数据融合算法，提供在簇头节点进行数据融合的处理方法。

二、传感器网络典型安全技术

(2) 运行逻辑

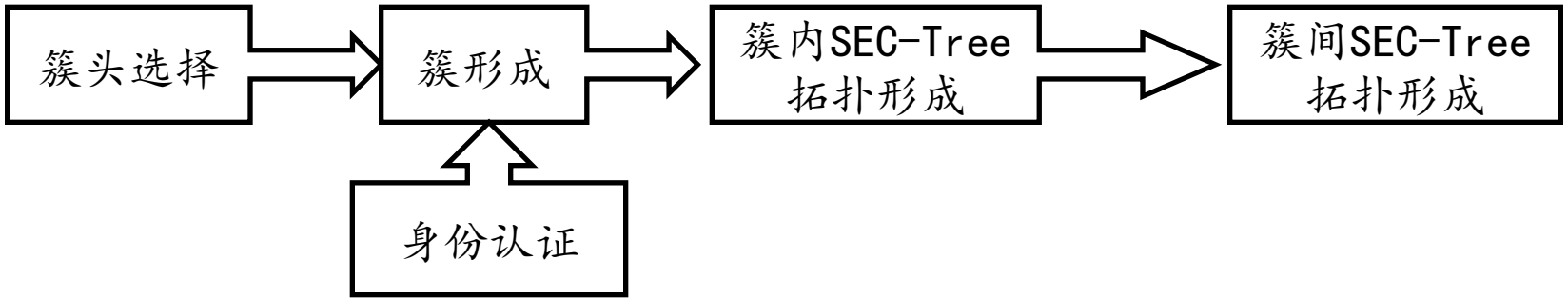
SEC-Tree协议包括拓扑建立和拓扑维护两个阶段，数据传输阶段包含在拓扑维护阶段内。SEC-Tree的簇管理、多跳路由、多路径路由、认证、数据融合(数据特征码)等各个模块在路由建立和路由维护阶段协同作用，实现了以最小化传感器网络能量损耗为目的的安全路由。

以循环的方式随机选择簇首节点，将整个网络的能量负载平均分配到每个传感器节点中，从而达到降低网络能源消耗、提高网络整体生存时间的目的。

(3)路由建立运行逻辑

节点初始化时，由簇管理模块进行簇头选择。簇管理内置SEC-Tree改进的LEACH路由算法，引入了剩余能量因子。通过随机选取簇头，进入簇形成阶段。该阶段由簇头广播请求信号，其余节点通过判断收到的信号强度决定自己所加入的簇。在簇形成阶段调用身份认证模块，实现非簇头节点对簇头节点的信息认证。一旦簇形成，根据ECM算法建立簇内SEC-Tree拓扑和簇间SEC-Tree拓扑，至此初始化路由表工作完成。路由建立阶段处理流程如下图所示：

二、传感器网络典型安全技术



（路由建立阶段处理流程）

路由协议利用ARRIVE路由协议的思想，对TREE-based路由算法进行安全扩充，提出了基于SEC-Tree的安全协议算法和基于优化BP神经网络的系统安全评价模型，从而保证路由的健壮性和可靠性。

ARRIVE路由协议：UC Berkeley 学者Karlof 等人设计的针对稠密的无线传感器网络的可靠的路由算法，适合恶劣环境中的可靠路由 。

无线传感器路由建立的运行逻辑

1、Tree-based路由算法是以Sink Node（网关节点）为树根，周期性的向它的邻居节点发送一个带有自身ID和距离（初始值为0）的消息，接收节点判断是否到目前为止所侦听的距离最近的节点，是则记录该源节点的ID作为它转发路由的父节点，并增加距离，然后将它自己的ID作为源节点的ID重新发送这个消息，由此构建一棵自组织的生成树。

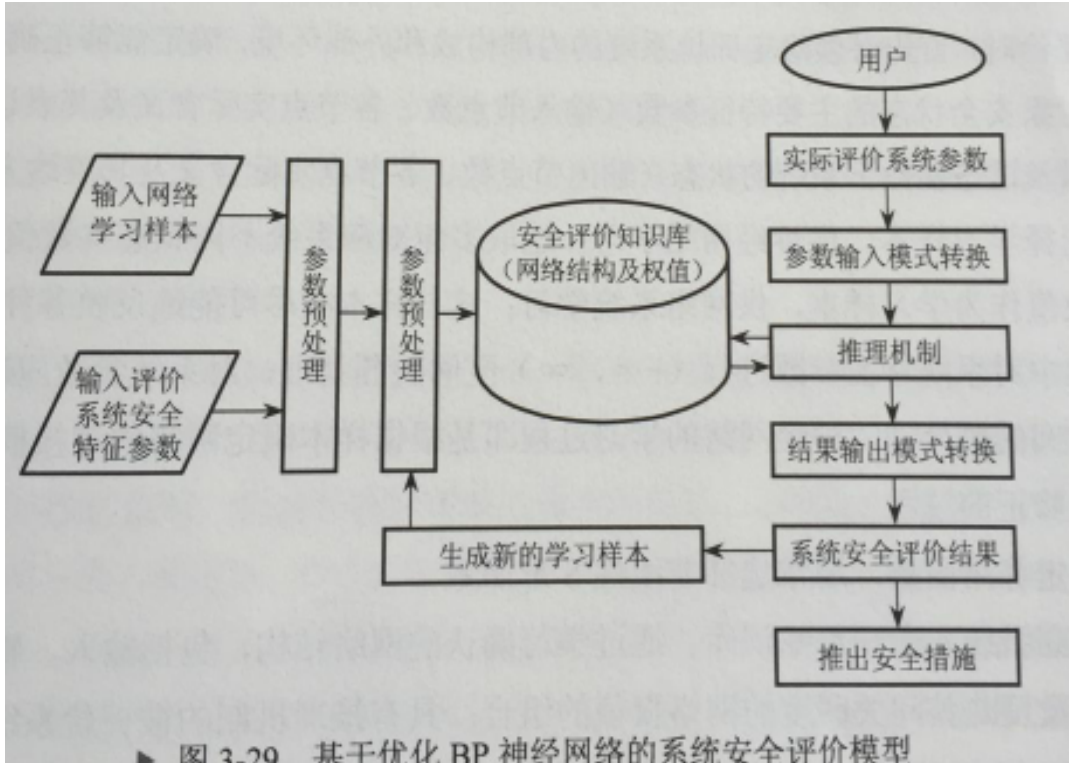
2、采用Tree-based路由算法，无线传感网络形成动态生成树。由于网络是自组织的，就可以形成多个并发的根节点，这样就可以形成一个生成森林。

3、动态网络生成树后，数据包的路由是根据节点中所记录的路由信息直接转发，但节点要传输一个数据包，它指明它的父节点是接收者。转发处理程序将数据包发送给他的临近节点，只有它的父节点会继续转发该数据包，其他临近节点将丢弃该数据包，这样数据包最终路由到根节点。

基于优化BP神经网络的系统安全评价模型

实现过程

1. 确定网络的拓扑结构，包括中间隐层的层数及输入层、输出层和隐层的节点数；
2. 确定被评价系统的指标体系，包括特征参数和状态参数；
3. 选择学习样板，供神经网络系统学习；
4. 确定作用函数；
5. 建立系统安全评价知识库。



▶ 图 3-29　基于优化 BP 神经网络的系统安全评价模型

4）传输层可靠传输协议

可靠传输协议的功能是：（1）在网络受到攻击时，传输层能够将数据安全、可靠地送达目的地；（2）能够抵御针对传输层的攻击。

传统的传输层实现数据的端到端的可靠传输，通过复杂的算法保证传输，降低网络核心层的负担，以此提高网络的整体性能。无线网络可靠的传输不能采用TCP协议，实现可靠传输是要考虑如下因素：

1、无线通信。链路的不可靠性，非对称链路、信号干扰、障碍物等影响信道质量的因素；

2、资源有限。TCP主要解决差错和拥塞控制上，而传感器网络的能量、内存、计算能力和通信能力有限，实现复杂的算法提高可靠性不可能，因此为增强可靠性，以**通信尽量小**来**延长网络的生存周期**；

3、下层的路由协议。无论有线和无线都是在不可靠的IP层上为应用层提供一个可靠的端到端的传输服务。无线网络是**通过若干个传感器节点为一个可靠传输提供努力，因此汇聚节点是发现多个源节点提供的信息，而不是单个节点的报告**，因此**端到端的可靠传输不能适用于无线传感器网络**。

4、恶意节点。可靠传输要有一定的容忍入侵能力，在发现入侵时调整传输策略，保证数据可靠送达。

5）应用层认证鉴权协议

针对资源有限和无线通信的特点，采用SPINS进行改进最优化协议栈。

SPINS安全协议框架**是**最早的**WSN安全框架之一**，**包括SNEP**(Secure Network Encryption Protocol）**和μTESLA**（micro TimedEfficient St reaming Loss2tolerant Authentication Protocol) **两个部分。**

SNEP(网络安全加密协议)是一个低通讯开销的、**实现了数据机密性、通讯机密性、数据认证、完整性认证、新鲜性保护的简单高效的安全协议。**SNEP采用共享主密钥的安全引导模型，其各种安全机制通过信任基站完成。SNEP本身只描述安全实施的协议过程，并**不规定实际的使用算法，具体的算法在具体实现时考虑。**

特性：

① 数据认证，只要MAC校验正确，消息接收者就可以确认消息发送者的身份；

② 重放保护，MAC值计数阻止了重放消息；

③ 低的通信开销，计算器的状态保存在每一个节点，不需要在每个信息中发送。

问题：共享主密钥方案，虽然能够解决节点间的安全通信，但不能解决密钥管理问题，缺乏实用型。

5）应用层认证鉴权协议

μTESLA协议是基于时间的、高效的容忍丢包的流认证协议,用以**实现点到多点**的**广播认证** 该协议的主要思想是先广播一个通过密钥Kmac认证的数据包,然后公布密钥Kmac。这样就保证了在密钥Kmac公布之前,没有人能够得到认证密钥的任何信息,也就没有办法在广播包正确认证之前伪造出正确的广播数据包。这样的协议过程恰好满足流认证广播的安全条件。

问题： **μTESLA协议不能有效解决传感器节点身份认证和数据源认证。**

SPINS协议框架在数据机密性、完整性、新鲜性、可认证性等方面都作了充分的考虑。但是,SPINS协议只是一个框架协议,它并**没有指定实现各种安全机制的密码算法**,在SPINS的**具体应用**中,需要**考虑**很多**具体的实现问题。**

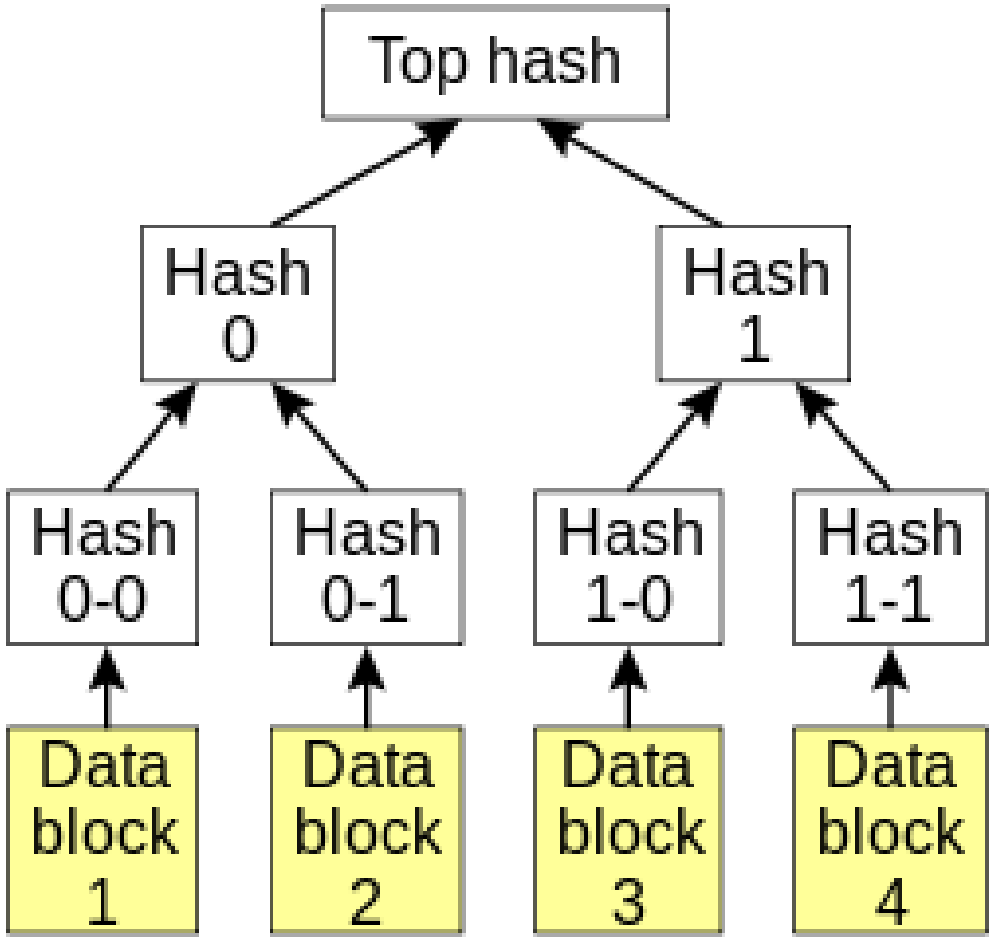
应用层的访问控制：基于Merkle哈希树的访问控制方式

基于Merkle哈希树的访问控制方式是一种多密钥链的访问控制方式。

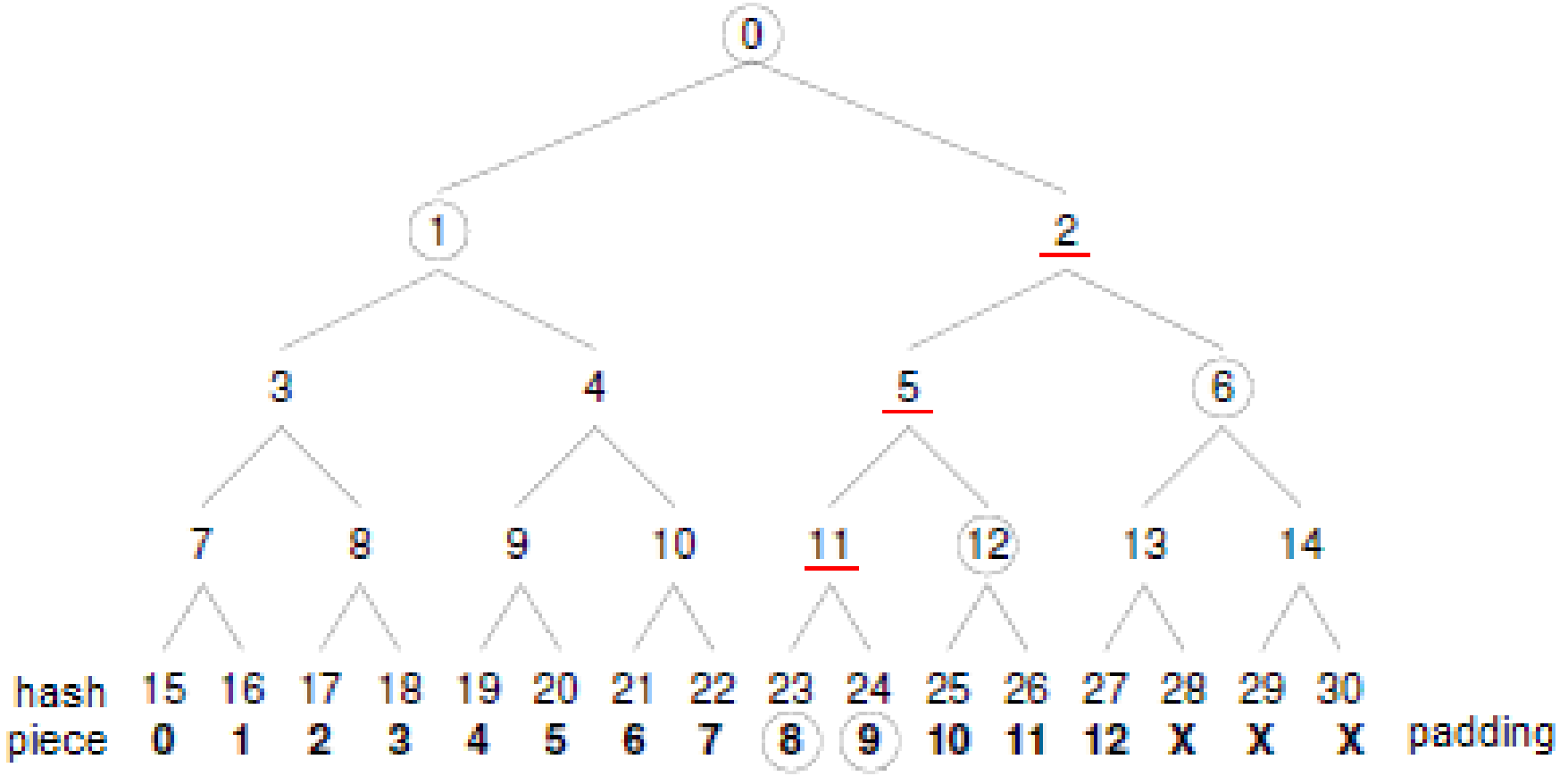
每个传感器节点需要保存所有密钥链的链头密钥。当使用的密钥链较多时，传感器节点存储开销较大，为了减少存储开销，引入Merkle哈希树，以所有密钥链的的链头密钥的Hash值作为叶子节点构造Merkle树。这样每个传感器节点仅需要存储Merkle树的根信息，就能够分配密钥链的链头密钥和认证用户的请求信息。

Merkle哈希树

右图给出了一个二进制的哈希树(二叉哈希树).哈希树的特点很鲜明: 叶子节点存储的是数据文件，而非叶子节点存储的是其子节点的哈希值(称为MessageDigest) 这些非叶子节点的Hash被称作路径哈希值, 叶子节点的Hash值是真实数据的Hash值。



Merkle哈希树



我们如果使用SHA1算法来做校验值, 比如数据块8对应的哈希值是*H*23, 则按照这个路径来看 应该有

*H*11 = *SHA*1(*H*23 // *H*24)　　*H*5 = *SHA*1(*H*11 // *H*12)　　*H*2 = *SHA*1(*H*5 // *H*6)

*H*0 = *SHA*1(*H*1 // *H*2)　　其中 // 是表联接的意思.