# 工业无线安全

## 安全需求和问题

工业无线网络是基于事件驱动，需要及时对传感器节点采集的数据进行分析和评估，以便于实时（接近于实时）、高效、准确的进行环境感知与决策。在无线传感器网络中，敌对方或攻击者往往通过发起各种网络攻击行为，达到其破坏网络通信、窃取敏感信息的目的。根据网络攻击的来源不同，针对无线传感器网络的攻击行为主要分为两类：外部攻击和内部攻击。外部攻击是指来源于无线传感器网络外部的攻击，发起攻击行为的外部节点是未经授权的，是非法节点。与之相对，内部攻击是指攻击者利用某种手段获取网络的认证授权信息后，将攻击节点伪装成为合法节点，或者直接利用已经通过认证的具有合法身份的网络内部节点攻击网络。相较于外部攻击，网络内部攻击隐蔽性更高，难以被察觉，所以更加难以抵御，相应的，对网络造成的破坏性就会更明显。

无线传感器网络的安全主要是指保障网络中的数据和资源安全，以降低恶意攻击的概率，提高网络抵抗性为目标。一般可以从两个方面考虑无线传感器网络的安全性。

1. 消息安全

消息安全也就是信息安全，指网络中通信传输的数据包要满足数据机密性、完整性、可认证性和新鲜度。

1）机密性：无线传感器网络中传输的所有敏感数据都需要保持机密性，以防止恶意攻击者入侵网络直接获取消息内容。

2）真实性：在无线传感器网络中，数据的真实性要求节点在接收来自其他节点的数据信息时，能够准确判断其接收的数据消息是从正确的网络节点传输过来的，这一安全隐患通常是由攻击者向网络注入虚假信息造成的。

3）完整性：在数据传输过程中，要求保证节点收到其他节点发来的数据包在传输过程中未被恶意篡改，即保证数据的完整性。

4）新鲜性：在无线传感器网络中，攻击者可能会重复发送相同的或者过时的消息给接收者，从而耗费其有限的资源，干扰其进行正常的网络服务。

消息安全是确保无线传感器网络安全的基本要求，也是首要任务，一般采用加解密和认证机制来保证消息安全。

1. 节点安全

节点安全意味着即使正常节点被控制为恶意节点，系统能快速找出问题节点，防止更大的损失。与传统的网络相比，无线传感器网络中的节点更容易受到损害，因此只依靠加密算法确保信息安全是不够的。在节点妥协或被捕获的情况下，其加载的秘密信息可能会泄露并被敌方不合理的利用，因此，及时识别出网络中妥协节点并将其剔除网络至关重要。

## 国内外研究进展

### 消息安全防护技术

#### （1）加密算法

目前国内外对于消息数据的保护和对恶意攻击的防御，则主要依靠用于数据加密和身份认证的加密算法的能力。

由于无线传感器网络的能量有限性，大量论文集中于改进现有对称加密算法在无线传感器网络的应用。比如文献[22，31]，他们分别针对AES加密，DES加密提出了自己的改进思路。文献[22]比较侧重于从算法上减少复杂度，以求得功耗和安全性的平衡。而文献[31]则是从加密体制上提出了分簇加密的思路。几种方法都有缺陷，不能完全符合无线传感器网络实际应用的需要。

由于无线传感器网络是一个易受攻击的网络，因此网络的运行需要大量的认证运算。文献[21]从此需求出发，针对ECC算法在认证上的优势，将ECC算法与MD5算法结合使用，降低ECC算法运算复杂度，以使其真正可以应用在无线传感器网络上，但实验结果表明，此方法仍存在密钥管理困难等问题。

另外，对称-非对称的混合加密体制也受到了关注。比如文献[28，29]均提出了AES-ECC混合加密体制。混合体制一个显而易见的好处是综合了对称加密的加密强度高、计算复杂度小的优点，同时又有非对称加密体制易于认证、易于进行密钥更新的优点。但目前现有的方案大多数仍是几种加密算法的简单混合，在无线传感器网络应用时仍有缺陷。比如，文献[28]提出的AES-ECC加密方法，虽然可方便地进行认证，但是实际网络往往是协调器-路由器-终端节点的拓扑结构，普通非对称加密算法在认证时，发起认证方仍需要首先从服务器获得待认证节点的公钥，来发起对其他节点的认证。也就是说每次认证都需要首先与服务器通信。而这在拓扑复杂，通信采用多跳的无线传感器网络中是不合适的，这也决定了直接使用非对称加密算法仍具有局限性。文献[30]提出了IBE的改进算法以解决普通非对称加密算法认证困难的问题。但是由于作者没有考虑到无线传感器网络密钥更新的问题，而是采用了私钥预置于WSNs点的方法，这也导致了此方法存在密钥更新困难的问题。

一些学者根据某些无线传感器网络的使用特点提出了改进思路，如文献[23]从某些网络对数据的不敏感性出发，提出了数据预存储的概念。但此种方案其实用到了大量的服务器，具有很高的局限性。此方案假设的数据不敏感和大量服务器分布式存储的方法只能应用于特定的网络。因此不适合普通的无线传感器网络。某些学者则另辟蹊径，采用从无线传感器网络物理传输上进行改进的方式。比如文献[24]提出信道加密的方法，但作者没有说明频繁变换信道是否会造成WSNs节点通信负担的增加（因为往往对于WSNs节点来说，通信能耗是很严重的，往往某些时候甚至大于数据采集和计算的能耗）。

#### （2）密钥管理

安全的密钥管理机制，是传感器网络中数据加密和安全通信的前提。受限于传感器节点存储空间与性能，传统网络中应用的安全密钥机制，并不能通用于无线传感器网络中，这也对无线传感器网络节点安全带来很大的挑战。许多学者针对传感器节点的特性，提出许多密钥管理机制，以提高无线传感网的抗风险性能。

依据数据加密算法不同，可分为基于对称密码机制的密钥管理协议和基于非对称密码机制的密钥管理协议。

1. 基于对称密码机制的密钥管理协议

对称密码机制是指通信双方使用相同的密钥和加解密算法对数据进行加密和解密，其优点是密钥长度相对较短，占用的存储、计算及通信资源比较少，适用于传感网，一直是传感网密钥管理协议的主流研究方向。传感网对称密钥管理协议研究的核心问题是采用什么样的数学模型，将各种先验知识和异构因素结合，设计出具有较高密钥连通率、较低物理耗费和更好网络抗毁性等较好性能的密钥管理协议。其中，先验知识是指网络部署模型、节点地理位置、周围环境、路由知识等外部知识，一旦传感网部署完毕，先验知识不再受人为控制；异构因素包括节点异构性（高性能节点、低性能节点）、链路异构性（通信链路的不对称性）、网络异构性（基于成簇的层次型传感网）、通信协议异构性（低速通信协议、高速通信协议）等，在不做跨层设计的情况下对称密钥管理协议设计中所考虑的异构性主要是节点异构和网络异构。

对称密钥管理协议的研究成果众多，从密钥分配方式的角度，可以将其划分成密钥集中分配协议和密钥预分配协议两大类。密钥集中分配协议是指节点间的通信密钥直接由某一可信实体进行分配，如基站作为可信实体负责给节点间分配密钥或者建立密钥，这种由密钥分配中心（Key Distribution Center，KDC）集中地为节点分配密钥的密钥管理协议，占用存储空间少，抗毁性高，但灵活性差，协议的安全性依赖于基站，一旦基站被攻击，整个网络被破坏。密钥预分配协议的研究在密钥管理协议中最为广泛，研究方法层出不穷。密钥预分配协议的基本思想是，传感网部署之前，在传感器节点里预置了一个或多个密钥或者密钥材料，一旦传感网组成，节点间通信时会根据某种关系或者原则确立或者生成共享密钥。密钥预分配协议分为三个阶段：密钥预分配阶段，共享密钥发现阶段和路径密钥建立阶段。这三个阶段中，密钥预分配阶段是初始化过程，也是预分配协议的核心部分，是指从密钥池中选取若干密钥组成密钥环，然后将密钥环预分配传感器节点，密钥环的构成决定了密钥预分配协议的性能。密钥池中的每个密钥都有一个独一无二的ID，用作网络中的身份标识。如果密钥环中的密钥是以随机的方式从密钥池中选出，则该协议属于随机性密钥管理协议，如果以某种确定的方式选出，则属于确定性密钥管理协议。

1. 基于非对称密码机制的密钥管理协议

非对称密码体制的安全强度要远高于对称密码体制，但由于受传感器节点物理性能的限制，传感网发展初期，研究者们普遍认为计算复杂性高的非对称密码运算并不适应于无线传感网。随后研究人员发现，将少量高性能节点加入到传感网中形成层簇式异构传感网，复杂的公钥操作计算可以在高性能节点中完成，基于公钥机制的非对称密钥管理协议在异构传感网中得以实现。随着椭圆曲线密码算法（Elliptic Curve Cryptography, ECC）、身份基、属性基等公钥密码技术研究的深入，公钥密码机制在传感网密钥管理中的研究逐渐体现了优势。基于非对称密码机制的密钥管理协议的思想是在每个节点中预装载公私钥对，采用公钥机制在两个节点间协商生成会话密钥，节点的增删不影响其他节点的安全。

基于公钥机制的密钥管理协议克服了对称密钥管理协议中的一些缺点，具有密钥连通性强、网络扩展性好且网络抗毁性强等优点，但其计算代价相对较高，能量消耗大。因此，设计出高有效性、低能量耗费的公钥机制的密钥管理协议，一直是学者们的研究目标。

#### （3）物理层认证

物理层认证技术原理是利用传输媒介天然的物理特性来实现通信的机密性和安全认证。与传统的基于秘钥计算的安全加密算法相比，物理层认证技术在某些方面具有更高的安全性能。

首先，物理层介质具有优良的机密性，无线信道的物理特性可用来提升传输信息的机密性。其次，利用通信介质唯一性、时变性和复杂性的特点，能很好实现身份加密和认证，并且其特征很难被模仿。而在基于密钥计算的传统加密方式中由于计算机性能的不断提升窃听者可以获得无限的计算能力来发动暴力窃取或干扰攻击。另外，物理层认证技术不需要考虑物理层之上的安全机制的执行方式，有很好的兼容性。同时也不会增加额外开销消耗大量的通信资源或基础设施。最后，物理层认证技术可以在对信号进行解调和解码之前快速地对通信节点进行身份认证，从而避免对信号处理资源的浪费。

在不同的检验指标和通信方式下物理层认证技术具有不同的特点。一般更关注物理层认证技术的检测指标按不同的认证指标可分为嵌入标签的水印认证技术、基于射频指纹的认证技术、基于信道特征的认证技术。其中，射频指纹用于对硬件设备进行识别，另外两类技术是对用户身份进行认证。基于信道特征的认证技术是目前物理层认证领域中的研究热点。

1. 嵌入水印的认证机制

这种机制的原理是发送端把认证标签与主信号消息混合生成带有水印的信息再一起传输，在接收端通过认证标签检测进行身份认证。其通常采用叠加，乘积以及频率调制等形式与信号进行混合。在现有技术方案中，密钥信息，身份证书，随机序列，信道状态信息以及信号的频率相位等信息都可以作为认证标签。此外还能引入可控的码间干扰产生认证标签，通过对认证标签和数据信息分别调制的方式完成水印加密和认证。

Paul L和John S等人提出一种广义的水印认证方法，在传输的数据信息中加入认证信息标签，接收端通过信号标签检测获得密钥进行验证实现身份认证。其基本思想是，先通过秘钥信息产生认证标签与数据信息进行波形叠加，再通过能量控制使含有认证标签的信号与原始的数据信号具有近似强度从而隐藏认证信息。文献[23]将有限长信道脉冲响应作为认证标签，再与传输信号进行乘积得到水印信号。再将水印信号通过信道估计得到抽头系数权值，通过检测抽头系数与代表信道脉冲响应的认证标签进行对比实现身份认证。文献[24]通过加入人工噪声的方式对信息进行处理提出一种主动认证的方法。通过将双方已知的加密信息加入到随机序列中作为询问信号，当对方收到后即可根据已有的密钥进行解密和认证。以上方式都是通过将认证标签作为噪声的方式混合加入到数据信息中。这种认证机制实现复杂需单独的设计认证标签同时还需要权衡消息信号与标签信号的能量比。

1. 基于射频指纹的认证机制

基于射频的认证机制其原理是利用物理设备的机械性能做为身份检测的指标。具体表现为各种硬件设备具有不同的天然瑕疵也就是射频指纹，其具有唯一性能很好的表征身份信息。目前该技术主要是基于瞬态信号或调制域信号来实现射频指纹的获取[25]。这种认证技术对检测器件的性能要求非常高，要求其能对射频指纹进行精密提取和分析，技术成本非常高昂。

文献[26]将边信道信息作为设备指纹。其特点是能够基于密钥产生相同的副信道信息，被认证用户的设备不需要任何改变。但该方案限制了认证双方之间的通信距离，强烈依赖于侧通道探测器的性能质量同时对环境噪声等因素敏感，会随之强烈地变化而影响认证效果。文献[27]利用微型延迟电路中序列响应作为不可复制的密码，对无线网络中认证协议的问题提供了有效的解决方法。文献[28]基于硬件的安全原语特征挖掘多媒体设备的认证潜力。该技术方案能够完成对硬件设备和多媒体信息的认证，同时将硬件资源和功率开销降到最小，对硬件本身的性能影响较小。

射频指纹认证通常来说具有不可移植性，每个设备的性能特征具有唯一固定性。其认证的性能与器件的属性紧密相关，且在受到外界干扰和噪声的影响下性认证能效果波动巨大。在复杂多变的衰落信道更加难以进行准确的认证检测往往需要高端昂贵的仪器才能保证认证效率，具有硬件局限性。

1. 基于信道特征的认证机制

物理信道有着丰富的资源为身份认证提供了多种特征检测指标。该认证机制的特点在于挖掘物理信道特征来实现身份认证。现有认证技术方案中常用的信道特征有信道脉冲响应、接收信号的强度、时域及频域等特征。这些特征随着用户位置空间的变动而改变能够作为不同用户在不同场景下的身份检测指标。其次在自由空间中这些特征呈现出随时间无规律变化的特性，一般很难被模仿并能够有效抵御模拟攻击等普通攻击。

信道脉冲响应（Channel Impulse Response，CIR）是物理层认证中常用到的信道特征。不同位置的用户具有不同的CIR，其包含了用户的位置信息，可根据脉冲响应的历史记录查找身份特征[34]。文献[35]提取CIR中的变化分量作为身份特征，利用二元假设方法来确定相邻时刻的通信信息是否来自同一终端。在低信噪比（Signal Noise Ratio，SNR）情况下基于CIR特征的认证准确度会显著降低。针对对该问题Fiona J和Xianbin Wang等人设计了一种二维量化方案[29]来容忍CIR的这些随机误差，以降低误检概率（False Acception Rate，FAR和漏检概率（False Reject Rate，FRR）率。目前，基于CIR的认证技术在快速时变的移动环境下存在认证准确率较低[36-37]的问题。

对于信号的频域特征可对载波频率偏移（Carrier Frequency Offset，CFO）进行估计[38]，在正交频分复用（Orthogonal Frequency Division Multiplexing，OFDM）系统中估计CFO与历史数据对比进行认证。对于信道状态特征文献[31]对接收信号强度（Received Signal Strength，RSS）、到达时间（Time of Arrival，TOR）及信道循环向量三个特征进行认证检测，具有较好的认证效果，但需要同时考虑三个特征计算复杂度高。文献[40]采用接收信号强度特征使用贝叶斯技术来进行认证。通过实时检测和更新每个用户位置的RSS估计从而能够根据物理位置进行认证。

### 节点安全防护技术

#### （1）异常检测

异常检测的主要原理是通过定义在一定时间区间[*T1,Tn*]内的数据相关性*R*，若某一传感器节点的数据变化造成与其他相关传感器节点的数据关系不再持续，则可认定该传感器节点采样值为异常采样值。

在工业无线网络中，异常检测具备多种类型，根据异常检测方法的不同，相应的异常检测算法可以分为4类，分别是：基于统计的异常检测算法，基于邻近过滤的异常检测算法，基于聚类的异常检测算法和基于分类的异常检测算法。其中前三类算法计算资源消耗较低，且不需要前期的训练过程，能够应用于工业无线网络中资源受限的传感器节点上。

1. 基于统计的异常检测算法

基于统计的方法是最早的异常检测方法，主要通过建立概率分布模型检测异常数据。在文献[20]中，Wu等人提出了一种本地化（传感器节点可对异常数据进行检测而不需要将数据上传至服务器再进行检测）的异常检测算法，通过传感器节点采样值的空间相关性，界定事件边界，从而实现网络中传感器节点的异常检测。在方案中，每个节点会计算自身读数与相邻节点读数的中值读数之间的差，并对该差值进行标准化，作为相应读数的偏移度。如果其读数偏移度的绝对值大于预先选择的阈值，则节点被认为是外围节点。通过上述算法，当一个地理区域中的节点偏移度远超过另一区域节点偏移度，则认为该区域有异常事件发生。然而，该方案忽略了传感器节点读数的时间相关性，漏检率较高。

在文献[21]中，Palpanas等人提出了一种分布式的基于核的、在线数据流离群值检测算法，该算法不需要相应的先验知识，而是通过核密度估计获取传感器分布情况。方案中，每一个传感器节点可以在本地，通过计算传感器采样值与近似数据分布模型的偏移程度识别异常节点。当某一个传感器采样值在其邻域中的数量小于用户指定的阈值，则该传感器采样值将被认为是异常值。因为该算法基于分布式网络，所以可以应用于高层节点，并可通过全网角度实施更大范围的异常检测。然而该算法对阈值具备高依赖性，且阈值的选择相当困难，单一阈值无法适用于多维数据，同时该方案忽略了传感器采样值频繁更新带来的近似数据分布模型更新问题。针对文献[21]中因为数据频繁更新造成的近似数据分布模型更新困难的问题，Papadimitriou等人在文献[22]中设计并提出了一更具鲁棒性的算法：LOCI。在该方案中，每一个传感器节点会从簇首节点上获得近似数据分布模型备份，并通过该模型在本地实施异常检测。针对文献[21]的单一阈值无法适用于多维传感器采样值的问题，Subramaniam等人在文献[23]设计并提出了一种非参数化在线异常检测模型，该模型允许网络中每一个节点都能够使用与Palpanas等人相同的方法检测相邻节点，之后将异常传感器采样值发送至簇首节点进行检测，从而实现全局的异常检测。实验结果表明，这些技术提高了数据分布估计的精确度并保障了高检测率，在一定程度上减少了通信开销与存储开销，但因为没有考虑相邻传感器采样值之间的空间相关性而不能检测空间离群值。

1. 基于邻近过滤的异常检测算法

基于邻近过滤的异常检测算法主要通过定义两个相邻数据之间的距离概念（相似性度量），对异常传感器采样值进行检测。在文献[24]中，Branch等人定义了一种全局异常检测算法，在网络中每个节点会计算与相邻节点的传感器采样值距离相似性，当发现异常采样值之后，该节点会将其广播至相邻节点进行验证，相邻节点会重复该过程，直至全网所有节点对该异常传感器采样值的观点达成一致。然而该方案主要通过广播进行通信，导致过多的通信开销。且随着网络规模的增大，会增加不必要的广播次数，导致通信开销进一步增长，不适于大规模应用。

在文献[25]中，Zhang等人提出了一种基于树形分簇网络拓扑的异常检测方案，在该方案中，簇内节点会将传感器采样值发送至簇首节点，簇首节点汇总簇内节点发送数据，并计算不同数据之间的距离相似度。当检测出异常传感器采样值之后，簇首节点会将其发送给簇内节点进行验证。如果簇内节点不认同该异常值，将会发送额外的数据给簇首节点用于再一次异常检测。该过程会不断重复，直至簇内所有节点对簇首节点计算结果认同为止。该方案只考虑了一维数据，且没有考虑网络中关键节点（簇首节点）被捕获后的问题，且具备较高的计算开销。

1. 基于聚类的异常检测算法

基于聚类的异常检测算法主要是通过对传感器采样值进行分类（具备类似行为的数据会被归于一个群集），来进行异常检测。在文献[26]中，Rajasegarar等人提出一种基于聚类的异常检测方案，在该方案中簇首节点会首先对簇内节点的传感器采样值进行异常检测，之后数据会汇总与服务器进行再一次异常检测，从而减少通信开销。在该方案中簇内节点会对每次测量的数据进行聚合，并发送相应的聚合数据至簇首节点，簇首节点通过归纳合并簇内所有节点的聚合数据，计算相应的数据距离，当该距离超过阈值该聚合数据将被定义为异常数据。该方案主要基于KNN算法（一种邻近过滤算法），算法中k值的定义并不容易，同时每个传感器节点所发送的数据为聚合数据，对事件发生时的响应较慢，实时性较低。

在文献[27]中，潘渊洋等人通过数据距离（本文数据距离通过欧式距离进行定义）定义数据相似度，并通过数据相似度对数据点进行分类，在该方案中，基站通过DBSCAN距离算法训练并提取环境特征集，并将该特征集发送至各节点，其中，环境数据特征值会随着环境变化进行动态更新。同时，相应的训练特征集需要配置两个全局密度参数，参数设置较为困难，当参数选择不正确时会导致检测率的不稳定问题。针对上述问题，在文献[28]中，费欢等人提出一种基于K-means算法的异常检测算法。在该方案中，异常检测的实施不需要事先配置参数，在数据量较大的时候能够保障较高的检测率。该算法主要通过汇总一定时间段采集的数据并生成相应的检测数据集，通过欧式距离算法计算数据集中的数据相似度，将数据点进行分类，生成不同的群集，当一个传感器采样值距离群集距离较远或一个群集具备数据点数远小于其他群集的时候则认为这些传感器采样值为异常数据。但是因为方案主要通过

K-means算法对数据群集进行分类，当数据数量较少时，所计算出的均值误差较大会造成检测率较低，同时方案对事件发生时辨别和区分效率较低。

综上所述，大多数异常检测方案主要通过计算数据距离定义相似数据，只单一考虑了数据的空间相关性或时间相关性，缺少集数据空间相关性与时间相关性为一体的异常检测算法。即便通过数据的空间与时间相关性提高了异常数据的检测率，也无法保障相应的通信开销与对事件的响应效率。同时一些方案忽略了网络的信息安全问题。在关键节点（如簇首节点）被捕获后异常检测方案可能无法继续实施，甚至网络瘫痪。所以，异常检测方案的研究应从多方面进行考虑，不仅要考虑检测率的问题，还需要考虑通信开销等问题，针对工业的苛刻环境，还需要保障网络的可靠性，在关键节点失效的情况下能够保证网络以及异常检测方案的正常运行。

#### （2）信任管理

传统基于认证和加密机制的安全技术只能抵御来自网络外部的攻击，而不能有效识别通过认证的节点发起的网络内部攻击。作为一种有效的补充机制，信任管理系统能根据节点行为特征对节点的信任度进行评估、分析，并据此判断节点是否可信，保证节点之间通信的安全性，从而进一步灵活调整网络安全措施，保证网络的安全性与可靠运行。

无线传感器网络资源受限，因此，将节点“信任”进行量化评估是目前很多无线传感器网络环境中信任管理机制广泛采用的基本思想，具体来说，量化评估过程包括与被评估节点交互行为的观察、记录及其他推荐节点推荐意见的收集、处理等操作，其重点聚焦于如何设计适当的信任评估模型，在保证信任评估结果准确、客观，即保证网络安全性的前提下满足资源利用轻量级的要求。设计适当的信任管理机制能够实现对网络节点准确、高效的安全度量，并根据被评估节点的信任值灵活调整网络的具体安全措施，如将信任值用于安全路由协议、簇头选举、数据融合等机制。

目前，无线传感器网络信任研究可以划分为三类：信任模型、信任管理机制及协议优化。

在信任模型研究方面，2004年，Ganeriwal和Srivastava提出一种基于信誉的分布式无线传感器网络信誉管理框架BRSN(Beta Reputation-system for Sensor Networks)[45]，利用贝叶斯公式将信誉分布和Beta分布进行拟合，从而得出信誉值服从Beta分布的结论，节点的信誉可以通过计算Beta分布的期望得到。2007年，肖德琴等人对BRSN进行改进，能够在一定程度上消除来自低信誉节点的虚假推荐影响[46]。由于现有的大部分信任计算模型对异常行为的检测都比较单一，仅检测和评判节点某种特定类型的攻击行为，忽略了真实网络情况下节点恶意行为具有复杂性和多样性。此外，大部分现有的信任评价模型，在评估节点信任值时，很少考虑到第三方节点恶意评价带来的风险。对此，杨光等人基于BRSN模型提出MA&TP-BRSN(multiple attacks&third party-BRSN)[47]模型，通过定义节点通信行为和节点评价行为来评判提供建议的第三方是否可信，有效消除了第三方的恶意评价，并综合考虑多种攻击行为，克服了以往信誉系统评价单一的问题，仿真结果表明该模型能更快更准确地识别出恶意节点，在一定程度上消除了高信誉节点的恶意诽谤行为。2010年，Zhang等人提出一种无线传感器网络动态信任建立与管理框架[48]，在以往信任管理系统的基础上，采用一些新措施来改进信任管理系统。2014年，Sinha和Jagannatham提出一种基于高斯分布的MIMO衰减信道无线传感器网络信誉模型[49]，基于多元高斯分布和贝叶斯定理，考虑MIMO无线衰减信道的影响，作者将直接信誉和间接信誉进行融合，并计算信誉值和信任值，该模型能有效隔离恶意节点，但是计算过程复杂并不适用于能量有限的无线传感器网络。2015年，Jiang等人提出一种有效的分布式无线传感器网络信任模型[50]。该模型根据传感器节点接受数据包的数目选择性计算直接信任和推荐信任，在直接信任的计算过程中，考虑通信信任、能量信任及数据信任等因素，并定义了信任可靠性和熟悉度来提高推荐信任的准确性。

在信任管理机制研究方面，2009年，Hui-hui等人将无线传感器网络信任评估归纳为三个方面：通信信任、数据信任和能量信任[51]。所谓通信信任，是指传感器网络中能相互发送、接受数据的两个合作节点之间计算的一种信任关系值，数据信任是指对数据容错性和一致性的信任评估，能量信任则是指节点剩余能量与完成一项新的通信和数据处理任务所需能量阈值之间的关系。针对分簇拓扑结构，Shaikh等人提出一种基于群组的信任管理方案[52]，该方案设计时首先考虑能耗问题，降低了信任评估成本。2010年，Yu等人对无线通信系统中的信任和信誉管理（Trust and Reputation Management，TRM）系统进行归纳[53]，将现有TRM分为两类：个体水平的信任模型和系统水平的信任模型。个体水平的信任模型主要关注一个节点对其他节点的信任评估，而系统水平的信任模型则包括信任和信誉评价模型以及协议，并根据节点信誉进行奖惩。Li等人提出一种以数据为中心的无线传感器网络信任评估机制DTSN[54]，有效解决了基于实体的传统信任评估方法难以应用到无线传感器网络的问题。Zia和Islam提出一种基于公共声誉和个体信任的解决方案CRIT(Communal Reputation and Individual Trust)[55]，节点行为由看门狗进行监测，每一节点保存其相邻节点的信任表和声誉表。Ukil提出一种基于协同计算的信任和信誉方案，利用该方案可以选择最优路径[56]。2012年，Bao等人提出一种分层信任管理方案[57]，并将其应用到基于信任的路由及入侵检测中。2013年，Li等人提出一种轻量级高可靠性的信任系统LDTS(Lightweight and Dependable Trust System)[58]，根据网络中节点角色选择信任决策方案有效降低了网络能耗。2014年，Duan等人提出一种基于博弈论的信任推导方法[23]，作者首先分析了网络安全需求，然后在保证网络安全的前提下，利用风险模型来激励节点合作并得到一个最优的合作节点数目。最后，利用博弈论的方法来进行信任推导从而减少这一过程中的开销。

协议优化方面，2012年，Tajeddine等人提出一种基于信任的集中式高效路由协议[59]，该协议中，基站通过计算恶意性、合作性、兼容性等不同的节点质量度量来估计节点数据信任及转发信任，然后基于节点历史信息利用有效的技术手段将恶意节点隔离，并广播更新后的路由信息。Gerrigagoitia等人提出一种新颖的入侵检测系统设计方案[60]，该方案基于节点的信誉和信任来进行决策及恶意攻击来源的分析。根据节点在事件感知、数据转发和数据融合方面的行为表现，2013年，Fang等人提出一种信誉管理方案[61]，该方案描述了信誉的初始化、更新、存储及恶意节点的惩罚和恢复等问题，并将其应用到SPIN(Security Privacy In Sensor Network)协议中，提出一种新的信任增强的路由协议，仿真结果表明，该协议提高了分布式环境下无线传感器网络的数据转发率。基于信任和中心度，Duan等人提出一种分布式细粒度的访问控制模型TC-BAC(Trust and Centrality Degree based Access Control)[62]，考虑信任和风险两方面因素对节点授予访问权限。2015年，Li等人提出一种应用于无线医疗传感器网络的新的认证协议[63]。基于ACO(Ant Colony Optimization)算法，Zhang提出一种新的生物启发的可信路由方案[64]，通过实时监测节点行为以及接受基站反馈来进行信任评估，并根据ACO算法来进行可靠的路由选择，该方案在一定程度上解决了移动节点的信任评估问题。

目前，信任管理机制在开放网络以及其他分布式网络中得到了广泛的应用，但在无线传感器网络环境下的研究相对较少，也不是很成熟，虽然无线传感器网络信任管理机制的研究已经取得了一定的进展，但其仍然处于一个起始阶段，面临很多挑战，且大部分信任评估模型停留在理论研究阶段，还未在实际应用中得到检验。这主要是因为无线传感器网络存在诸多限制，如何在网络安全和资源消耗等方面寻求一个平衡，还没有一个综合的信任评估机制可以有效解决这些问题。

## 待解决的问题和后续研究

在工业无线网络中，大量廉价的工业传感器节点部署在工厂车间，用于监测生产环境，这些传感器节点将会产生海量的数据，由于节点通信能力和能量的限制，如何对这些数据进行统计分析是一项挑战。数据融合就是解决资源受限的工业无线网络的一种重要手段。主要方法是对数据进行汇聚并通过融合算法（例如：求和、求最值、平均数等）减少网络内传输的数据量，以减少网络通信开销，降低系统时延，延长生命周期。在资源受限的工业无线网络中，数据融合面临如下的安全问题：

1. 消息篡改

攻击者可以截获网络内传输的数据包，并故意插入或删除部分数据从而导致融合结果的错误。

2. 窃听攻击

由于无线信道的开放性，攻击者可以使用无线嗅探工具任意抓取无线数据包，如果数据未进行加密处理的话，节点传输的数据将会泄露。

3. 拒绝服务攻击

攻击者声称自己是合法节点，向网络中某个节点发送大量无意义的数据，消耗节点能量，造成网络瘫痪从而使合法节点无法正常获取服务。

4. 重放攻击

攻击者获取某个节点的历史数据后，向融合节点发送旧的数据包，由于该数据包已经失去时效性，历史数据的融合将无法反映实时的统计情况，造成决策者的错误判断。

5. 女巫攻击

攻击者利用单个节点来伪造多个身份存在于网络中，女巫节点会广播自己的ID，使其出现在其它节点的路由表中，当有数据要经过女巫节点转发时，它可能会转发给其它女巫节点或者直接不转发，从而降低了网络的冗余性和健壮性，干扰数据融合的正常操作。

针对工业无线网络中数据融合的安全性，后续拟开展“工业无线网数据安全融合技术”的研究，包括数据融合隐私保护技术和数据融合节点检测技术。

1）数据融合隐私保护技术在保证数据融合结果正确的前提下，即使是采集到的数据在传输、融合处理过程中被外部捕获、解密或是内部其它可信节点被捕获，也能够阻止隐私数据被获取；

2）数据融合节点检测技术的目标是有效识别通过认证的节点发起的网络内部攻击，阻止恶意节点的进一步破坏，保障网络的通信安全，提高系统的转发率。

## 研究内容和技术路径

1. 数据融合隐私保护技术

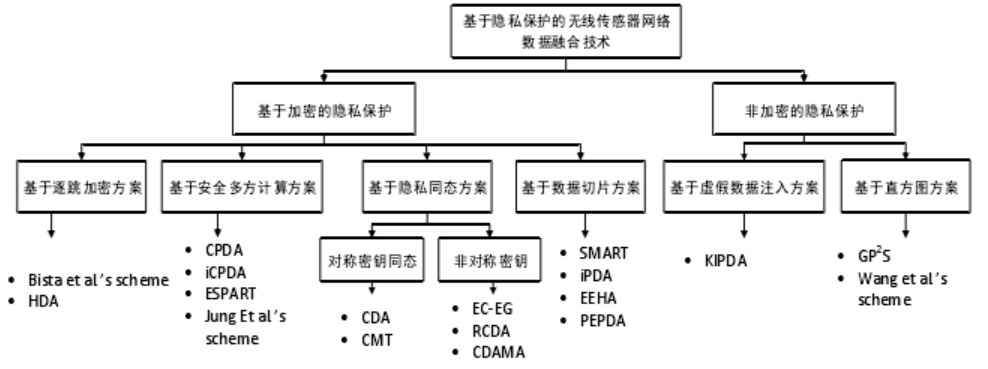


图 1 现有数据融合隐私保护方案分类

技术路径：将不同场景下的工业无线传感器网络数据融合隐私威胁、分级、保护和评估机制合理的整合在一起，形成统一的工业无线传感器网络融合隐私保护架构和模型；比较目前主要的数据融合隐私保护算法，从隐私保护能力、融合时延、通信开销等方面分析各类算法在工业无线网络场景下的适用性。如图1所示，可能具有基于加密和基于非加密两个隐私保护研究路径：对于加密技术的隐私保护方案，研究面向工业无线传感网数据融合安全和隐私保护的密钥管理和加密策略；对于非加密技术的隐私保护方案，研究适用于工业无线传感器网络数据融合过程的差分隐私数据发布技术。

1. 数据融合节点检测技术

技术路径：研究工业无线传感网的网络拓扑结构和入侵攻击方式，建立不同工业场景下的传感器节点异常模型；考虑节点被捕获的情况，引入信任的概念，研究相应的信任模型和信任管理机制；依据工业无线网的节点类型，研究信任机制下的异常节点检测算法；研究工业无线网异常节点检测机制的衡量指标（检测率、误检率、ROC曲线等）。