异常数据的检测

1. 贝叶斯算法实现异常数据的检测，贝叶斯算法是一个非常经典的分类算法，在定义好异常数据以及异常数据模型之后，通过一定的训练集，使得贝叶斯分类器能够有效的去检测异常数据。(Ni and Pottie 2012)。人工智能算法中的神经网络算法，在获得足够多的信任训练集下也可以实现异常数据的检测。已有的检测算法还包括了基于马尔科夫链的预测，线性自回归模型等。（贝叶斯分类法，通过训练集得到一个贝叶斯分类器，当节点传来数据时，可以识别该数据是否是正确的，如果不是的话，该节点的错误数据类型是哪种，都可以根据贝叶斯分类法得到。）
2. 传统的一些错误数据类型，以及前人做的一些检测错误数据的方法和第一篇综述类似。其中定义错误数据和错误数据模型的关键一点就是通过无线传感器网络的一系列网络特征，包括环境特征，系统特征，数据特征。文献给出了常见的错误类型数据，比如毛刺(数据在某一个点的变化特变大)，数据在一段时间内毫无波动(方差趋近于0)，高噪声高方差，数据校准错误，连接和硬件错误，数据丢失，电池能量低引起的错误等。在识别出一系列错误数据类型之后，通过训练集的方式，采用贝叶斯分类法去识别异常数据，并指出错误的原因。（或者利用模式匹配的方法，去找出异常数据）。(Ni, Ramanathan et al. 2009)
3. 提出将数据融合和错误数据检测结合在一起的系统（DAA，data aggregation and authentication protocol）。(Ozdemir and Cam 2010)
4. 相比较传统的传感器网络错误数据检测方案（在自己的本地网络中，不联网），本文提出的基于云计算的错误检测方案能够保证检测错误数据的前提下大大提高检测的速度(应用云计算平台的大数据计算能力和存储能力)。文章首先定义了9种数据异常类型，定义其异常数据模型，然后根据9种异常数据类型，来识别采集的数据集中是否存在异常数据。本文针对的是scale-free网络，这种网络的特点是，分成有限个簇管理传感器节点，当某个节点被检测出有异常数据时（通过异常数据检测算法检测），异常数据会在这个簇（该节点存在的簇）里面触发两个函数，首先检测数据是否是真的异常数据（因为存在将正确数据错误辨别为异常数据的概率），接着在该簇头中寻找错误的源节点位置。这样通过分簇的形式，能够大量节约检测的时间，提高异常数据的检测效率。这边文章重点看了（包括下载的资料，参考其中的算法，错误检测和错误定位）。(Yang, Liu et al. 2015)

（ 想到的一些东西，从仿真的结果看错误检测方案的优劣性。是否可以找到更加有效的错误数据检测方案使得比如说，错检检测消耗的时间更短，传感器节点的能量和资源消耗少，错误检测的准确性更高，误报率（正确数据检测为异常数据概率）尽可能小。

异常行为检测

1. 基于假设检验方案快速检测无线传感器网络中的移动副本节点攻击。文章的核心内容是：定义了一个异常行为模型：认为正常无线传感网中的正常节点移动的速度应该不超过系统规定的最大速度，但是一旦有节点被复制它的移动速度要超过系统规定的最大速度，这可以在一定程度上检测到恶意行为。但是由于存在阳性误差，当测量速度的系统有较大偏差时会带来很大的误报率。因此进一步提出了基于假设检验(SPRT)的方案，通过较多的样本来决策一个异常行为是否发生。(Jun-Won, Wright et al. 2011)
2. 使用序列分析快速检测无线传感器网络中的移动副本攻击。与第一篇论文类似(Jun-Won, Wright et al. 2009)
3. 使用序列假设检验方案快速检测和删除无线传感器网络中基于区域（基于区域的方案有利于加快检测的速度，提高效率）的恶意节点。文章的核心是通过序列假设检验方案识别可能发生恶意行为的区域(通过SPRT方案，使用信任管理机制计算出信任值，来判断某一个区域是不是可信任的，恶意节点是否存在在该区域)，紧接着对该被怀疑区域实行软件认证，可以顺利找到恶意节点并将恶意节点删除。这其中涉及到信任值的计算等等，把整个流程都看过了。基站最终获得各个区域的信任计算值，通过阈值去验证某个区域是否值得该信任（单一样本），最后利用SPRT方案利用多个样本做出决策。(Jun-Won, Wright et al. 2012)

（思考：信任值的计算方案是否可以影响对某个区域的判断是否可以减小误判率？这是可以思考的一个方向，同理是否可以找到更有效率的方法，能快速检测到恶意节点行为，而且能够保证资源开销不大）。

4、不确定性诊断：发现传感器网络中的无声故障。该文章创造性提出了，相关矩阵的概念。通过把衡量标准相关化，考虑衡量标准之间的相关性是否发生变化，进一步判断恶意节点，恶意行为是否存在，该方案可以不用有先验知识，即不必预先定义恶意行为的模式集，而是通过相关性矩阵的实时变化来进行判断！很新颖的一种办法

[1] Jun-Won, H., et al. (2009). Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis. 28th Annual IEEE International Conference on Computer Communcations (INFOCOM).

Jun-Won, H., et al. (2011). "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing." IEEE Transactions on Mobile Computing (TMC) **10**(6): 767-782.

Jun-Won, H., et al. (2012). "ZoneTrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing." IEEE Transactions on Dependable and Secure Computing **9**(4): 494-511.

Ni, K. and G. Pottie (2012). "Sensor network data fault detection with maximum a posteriori selection and bayesian modeling." ACM Transaction on Sensor Networks (TOSN) **8**(3): 1-21.

Ni, K., et al. (2009). "Sensor network data fault types." ACM Transaction on Sensor Networks (TOSN) **5**(3): 1-29.

Ozdemir, S. and H. Cam (2010). "Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks." IEEE/ACM Transactions on Networking **18**(3): 736-749.

Yang, C., et al. (2015). "A Time Efficient Approach for Detecting Errors in Big Sensor Data on Cloud." IEEE Transactions on Parallel and Distributed Systems **26**(2): 329-339.