An Improved Trust Evaluation Model Based on Bayesian for WSNs*

ZHOU Zhiping, SHAO Nannan*

(*Engineering Research Center of Internet of Things Technology Applications Ministry of Education, Wuxi Jiangsu* 214122, *China*)

Abstract: Based on Bayesian and entropy, an improved trust evaluation model for wireless sensor networks (WSNs) is proposed. Considering the abnormal behavior caused by non-invasive factors, the abnormal discount factor is introduced to modify the Bayesian equation which is used to estimate the direct trust. The sliding window and adaptive forgetting factor is used for the update of the direct trust. Then, according to the confidence level, whether the direct trust is credible enough to be a comprehensive trust can be determined, which effectively reduces energy consumption and the impact of malicious feedback. Finally, if the direct trust is not reliable enough, the comprehensive trust should be calculated, which uses entropy to assign weights to different recommendation. Simulation results show that the proposed model can detect malicious nodes effectively and reduce energy consumption of the network to a great extent.

Key words: wireless sensor networks (WSNs); trust evaluation; Bayesian theory; entropy; confidence level

EEACC: 6150P **doi:** 10.3969/j.issn.1004-1699.2016.06.023

基于贝叶斯的改进WSNs信任评估模型*

周治平*, 邵楠楠

(江苏物联网技术应用教育部工程研究中心, 江苏 无锡 214122)

摘 要: 基于贝叶斯和熵, 提出一种改进的 WSNs 信任评估模型。考虑到非入侵因素带来的网络异常行为, 引入异常衰减因子, 利用修正后的贝叶斯方程估算直接信任, 并利用滑窗和自适应遗忘因子进行更新。根据直接信任的置信水平确定其是否足够可信来作为综合信任, 减少网络能耗, 并降低恶意反馈的影响。如果直接信任不足够可信, 计算间接信任来获得综合信任, 利用熵来对不同的推荐赋予权重, 克服主观分配权重带来的局限性, 加强模型的适应性。仿真实验表明, 该模型能够有效检测恶意节点, 具有较高的检测率和较低的误检率, 同时在很大程度上降低了网络的能量消耗。

关键词: 无线传感器网络; 信任评估; 贝叶斯理论; 熵; 置信度

中图分类号: TP393 **文献标识码:** A **文章编号:** 1004-1699(2016)06-0927-07

近年来, 传感器网络已经成为最有用的技术之一并得到研究者越来越广泛的关注。由于具有数据采集、处理和传输能力, 无线传感器网络被部署于许多应用场景, 如环境监测、战场探测、工业安全监督及医疗保健等[1]。然而, 由于无人值守的恶劣的部署环境及无线传感器网络自身的特点, 传感器节点容易受到攻击, 其面临的安全威胁日益复杂[2]。在许多应用中, 传感器节点总是存在被敌方捕获节点加密密钥的危险, 其结果是敌方节点可能会被误认为网络中的正常节点, 使得敌方拦截、删除及插入信息成为可能。一旦节点妥协, 整个网络的可用性和完整性就会遭到破坏, 因此, 网络安全是一个需要加以解决的至关重要的问题。

在网络安全领域, 非对称密码机制被广泛用来处理 Internet、Peer-to-Peer 以及 Ad Hoc 网络中的外部攻击。然而, 由于复杂性及巨大的计算内存, 加密算法并不适用于处理能力有限、资源受限[3]的传感器节点。此外, 基于加密的安全机制只能解决外部安全问题, 不能有效处理内部攻击。节点的特殊性使得无线传感器网络不同于其他网络, 节点可以

项目来源: 国家自然科学基金项目(61373126); 江苏省自然科学基金项目(BK20131107); 中央高校基本科研业务费专项资金项目(JUSRP51510)

收稿日期: 2015-11-22 **修改日期:** 2016-01-29

为了节约资源而拒绝与服务请求者进行合作，这类节点被称为自私节点，虽然他们不主动攻击网络，但是大量自私节点可能会在网络中造成严重后果，而现有的加密机制是无法识别出通过认证的自私节点所造成的风险。因此，需要建立一种有效的安全机制来解决这些问题。

1 相关工作

近年来，信任管理被认为是保证传感器网络安全的有效补充机制[4]。基于历史行为，评估一个节点的信任值，可以估计该节点执行一项特定任务的可信度。目前，针对无线传感器网络研究者已经提出许多典型的信任模型[5]，包括贝叶斯信任模型、熵信任模型、模糊逻辑信任模型、D-S证据信任模型及博弈论信任模型等[6]。

贝叶斯理论是一种广泛使用的信任评估工具，基于贝叶斯理论，Ganeriwal等人[7]提出一个典型的信任框架RFSN，在此框架下，利用传感器网络贝塔信誉系统BRSN来评估节点的可信度。此外，Ganeriwal等人得出一个结论，即信誉分布与β函数能够很好地拟合，并将其数学期望作为节点的信任值。然而，只有良好的节点信誉允许传播，会导致网络中恶意节点的信誉信息不能及时传递。基于非合作博弈论，Mejia等人[8]提出一个完全分布式的信任模型，然而，博弈论并不是一种预测工具，只能建议博弈参与者应该如何决策，因此，并不适用于解决无线传感器网络中的信任问题。Tian和Yang提出一种基于风险评估的信任管理模型R2 Trust[9]，该模型根据信誉和风险来估算信任值，但是没有研究动态行为如何影响信任值。在文献[10]中，针对分簇无线传感器网络，Bao等人提出一种分层动态信任管理协议，该协议充分考虑社会信任和QoS信任，将亲密度和诚实度作为社会信任的度量，并选择网络能量和节点非自私性来衡量QoS信任。Anita等人[11]基于模糊理论提出一种路由信任预测模型，根据历史行为、一定时间段内信任的波动及推荐的非一致性，该模型能预测邻居节点未来的行为，但模糊理论的应用可能会导致信息的丢失。Aivaloglou等人[12]结合基于证书的方法和基于行为的方法，提出一种混合信任和信誉管理模型，该模型利用部署前的网络拓扑及信息流的相关知识来支持网络角色高度多样化的节点需求，但是该模型难以获取部署前的信息，因而难以实现。结合模糊结合和灰色理论，Wu等人[13]提出一种具有激励机制的信任模型来评估节点的可靠性，然而，由于模型计算复杂并不适用于节点处理能力有限的传感器网络。Zhang等人[14]提出一种多层次信任管理框架MLTRUST，在此框架下，三个层次的信任，即主观信任、客观信誉及推荐信任被用来建立节点之间的信任关系，但是该模型缺少信任共享及更新机制。

上述模型都在一定程度通过信任评价来识别恶意节点，并提供了进一步研究的理论基础，但是仍然没有解决以下一个或多个问题。第一，忽略网络中非入侵因素导致的节点异常行为，即环境干扰、网络异常等因素导致的节点不合作行为，如数据包丢失、数据包转发延时等，容易造成较大的误检率；第二，如何根据当前信任信息和历史信息分配遗忘因子，给历史信息赋予更大的权重能阻止恶意节点短期内通过某些行为来补偿其较低的信任值，而给当前信息赋予更大的权重则能迫使恶意节点正常执行网络任务，因为，一旦恶意节点发起攻击，就会受到严厉的惩罚；第三，考虑间接信任能够获得准确的信任值，但会导致更多的网络能耗。因此，需要建立一个良好的信任-能量平衡方案；第四，为了降低虚假推荐的影响，需要某种加权方案对节点推荐信任赋予不同的权值，保证信任的客观性及准确性。

针对上述问题，本文提出一种基于贝叶斯的WSN信任评估改进方案，利用直接信任和间接信任来获得节点的综合信任，并改进算法使其更具有适应性和可靠性。首先，根据历史交互记录，基于贝叶斯理论计算直接信任值，考虑到非入侵因素带来的网络异常行为，引入异常衰减因子对贝叶斯方程进行修正；然后来计算直接信任的置信度来确定是否需要计算间接信任，并根据熵对高度可信的节点赋予较大的权重，客服了主观赋予权重的弊端；最后，利用一个自适应权重因子来计算综合信任。

2 模型描述

传感器网络中信任一般有如下定义，即[5]评价节点对被评价节点未来行为的一种主观期望。完整的信任包括主观实体的观察及第三方的推荐，为了减少能量消耗并降低算法复杂度，本文仅在直接信任可信度不足情况下采用推荐信息。假设节点i需要计算节点j的信任值，首先根据历史交互信息更新计算直接信任所需的相关参数，然后根据置信

度水平判断直接信任是否足够可信，如果直接信任的置信度高于阈值，直接将其作为节点的综合信任值，否则，计算全局间接信任，并根据熵的理论定义自适应权重，将直接信任和间接信任进行融合，从而得到节点 j 的综合信任。具体算法流程如图 1 所示，其中 ω_D 和 ω_R 分别为直接信任和间接信任在综合信任中所占比重，即自适应权重。

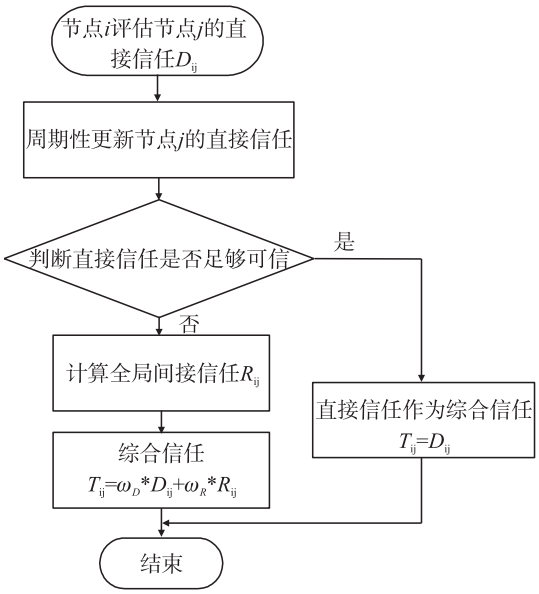

图1　算法流程图

2.1　直接信任评估方法

2.1.1　基于beta分布的信任值计算

贝叶斯理论是一种广泛使用的信任评估工具，Ganeriwal 等人提出的 RFSN[7]是无线传感器网络中最具有代表性的贝叶斯信任管理框架。该模型利用贝叶斯公式对信誉分布与 beta 分布进行拟合，得到节点的信誉服从 beta 分布的结论，即 $\text{reputation}_{ij} \sim \text{Beta}\left(\alpha_{ij}+1,\beta_{ij}+1\right)$，其中 reputation_{ij} 表示节点 i 关于节点 j 的信誉分布，α_{ij} 和 β_{ij} 分别表示节点 i 与节点 j 过去成功交互的数目及失败交互的数目。节点 i 的直接信任 D_{ij} 可以用信誉分布的统计期望表示，即

$$D_{ij}=E\left(\text{Beta}\left(\alpha,\beta\right)\right)=E\left(f\left(p|\alpha,\beta\right)\right)=\frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \quad (1)$$

其中

$$f\left(p|\alpha,\beta\right)=\frac{p^{\alpha-1}(1-p)^{\beta-1}}{\int_0^1 u^{\alpha-1}(1-u)^{\beta-1}\mathrm{d}u}=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{\alpha-1}(1-p)^{\beta-1} \quad (2)$$

2.1.2　信任计算方案的改进

节点信任评估的最终目标是检测出网络中的恶意节点并将其隔离出网络，因而检测率、误检率及漏检率是衡量一个信任评估模型的重要指标。一般来说，检测率越高，误检率越低，信任评估模型就越可靠。然而，原有的基于 Beta 分布的信任评估方案忽略了非入侵因素带来的不合作影响，即由于网络自身故障所带来的节点异常行为，因而，可能会造成较大的误检率。为解决这一问题，本文引入异常衰减因子的概念，对原有方案进行改进。异常衰减因子记为 q，表示网络中节点行为异常时，该异常是由攻击造成的概率，其表达式如下：

$$q=\frac{N_{\text{intrusion}}}{N_{\text{detection}}} \quad (3)$$

其中，$N_{\text{intrusion}}$ 表示由于入侵因素即网络攻击行为导致的节点不合作次数，$N_{\text{detection}}$ 表示网络中检测出的节点不合作总数。通常，在实际应用中，异常衰减因子的取值不是固定的，需要根据具体的网络环境进行调整。因此，将评价节点 i 判断出的节点 j 的失败交互次数进行衰减，削弱非入侵因素带来的不合作行为的影响，才是比较接近实际的节点 j 的失败交互次数，即由网络中入侵因素所导致的节点不合作行为。因此，式(1)可以修正为：

$$D_{ij}=\frac{\alpha_{ij}+1}{\alpha_{ij}+q\beta_{ij}+2} \quad (4)$$

2.1.3　直接信任值的更新

信任值基于历史交互计算并随时间动态变化，一般来说，新的历史交互比旧的历史交互对信任决策的影响更大。考虑到传感器节点资源有限的特点，本文采用滑动窗口 W 来进行信任的计算与更新，只有滑动窗口内的交互记录是有效的，即有效交互记录的最大值为 W。

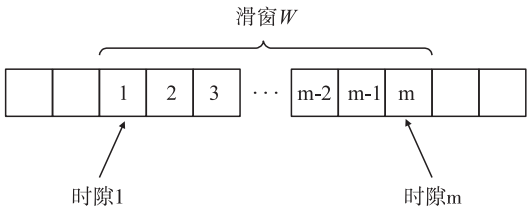

图2　滑动窗口

如图 2 所示，每一滑窗记录最近 W 次交互，并被划分为 m 个时隙，从左到右依次为 $1,2,\cdots,m-1,m$。尽管获得好的信誉需要长期的一致的合作行为，然而几个恶意行为就会破坏它，这就意味着信誉容易丢失，难以获得。基于此，本文引入自适应遗忘因子 θ_l 给不同的时隙设置权重：

$$\theta_l=1-D_{ij}^l, l=1,2,\cdots,m \quad (5)$$

在(5)中，D_{ij}^l 是第 l 个时隙末的节点直接信任，式(5)说明恶意行为会被记住较长时间。对于时隙

l 来说，节点 i 监测节点 j 的行为并在时隙末记录成功交互数目 α_{ij}^{l} 及失败交互数目 β_{ij}^{l}，因此，信任的更新等同于参数 α_{ij}^{l} 和 β_{ij}^{l} 的更新：

$$\alpha_{ij}^{\text{new}}=\sum_{l=1}^{m}\alpha_{ij}^{l}\theta_{l}^{m-l},\quad l=1,2,\cdots,m$$
$$\beta_{ij}^{\text{new}}=\sum_{l=1}^{m}\beta_{ij}^{l}\theta_{l}^{m-l},\quad l=1,2,\cdots,m \tag{6}$$

因此，直接信任可以按下式进行更新：

$$D_{ij}=\frac{\alpha_{ij}^{\text{new}}+1}{\alpha_{ij}^{\text{new}}+q\beta_{ij}^{\text{new}}+2} \tag{7}$$

2.1.4 直接信任置信度判断

现有大部分信任评估模型在计算节点综合信任值时会同时考虑直接信任和间接信任，虽然可以获得一个更加准确的结果，但是却以更多的能量消耗为代价。为解决准确性与能耗之间的矛盾，对直接信任的置信度进行判断，即如果直接信任的置信度高于阈值，直接将其作为节点的综合信任值，否则，综合信任值需要根据节点直接信任和间接信任进行计算。

直接信任的置信度可以通过区间估计进行评价，设置 $(D_{ij}-\varepsilon,D_{ij}+\varepsilon)$ 为 D_{ij} 在置信度 γ 下置信区间，那么置信度 γ 可以由式(8)获得：

$$\gamma=\frac{\int_{D_{ij}-\varepsilon}^{D_{ij}+\varepsilon}P^{\alpha_{ij}-1}(1-p)^{\beta_{ij}-1}dp}{\int_{0}^{1}P^{\alpha_{ij}-1}(1-p)^{\beta_{ij}-1}\mathrm{d}p} \tag{8}$$

式中，ε 表示误差水平，$0<\varepsilon<\min(1-T_{ij},T_{ij})$，其具体值依赖具体的应用环境。以 γ_0 表示阈值，通常 $0.8\leqslant\gamma_0\leqslant1$。如果 $\gamma\geqslant\gamma_0$，则 $T_{ij}=D_{ij}$，否则，则需要计算节点的间接信任。

2.2 间接信任评估方法

2.2.1 熵的相关概念

熵是热力学、统计力学及信息论中的概念，主要用来衡量一个信号或随机事件中的随机性，也可以用来评价一个信号中所携带的信息量。在信息论中，信息熵反映了多个评价指标对于待评价事物的影响程度，即各指标在评价过程中提供有效信息的多寡程度。因此，可以利用信息熵来度量各指标信息的有效程度并据此分别确定其相应的权重。

概率质量函数为 $\Phi(\mu)$ 的随机变量 μ 的熵如下式定义：

$$H(\mu)=-\sum\Phi(\mu)\log_2\Phi(\mu) \tag{9}$$

根据信息熵的概念，全局间接信任的计算过程就相当于根据多个评价指标对待评价事物的影响对其进行综合评价的过程[15]，这里的评价指标即为第三方节点对评价节点的间接信任值（推荐信息）。因此，推荐信息 R 的熵可以用两个参数进行衡量，即 R 和 $1-R$，R 为第三方节点对待评价节点的信任程度，相应地，$1-R$ 为第三方节点对其怀疑程度，从而可以得到推荐信息的信息熵为：

$$H(R)=-R\log_2R-(1-R)\log_2(1-R) \tag{10}$$

2.2.2 间接信任的计算

当需要间接信任来计算综合信任时，节点 i 向其邻居节点广播一个查询信息获取节点 j 的推荐信任，一旦收到该查询信息，推荐节点 k（节点 i 和节点 j 的共享节点）以其对节点 j 的直接信任作为推荐信息返回给节点 i。

假设有 n 个推荐节点，相应的有 n 个间接信任 $R_{ij}^{1},R_{ij}^{2},\cdots,R_{ij}^{n}$。由于并非推荐节点都是可信的，因此，需要考虑不同推荐的权重，本文引入信息熵的概念来给不同的间接信任值分配权重，能有效改善主观分配权重带来的问题，也能增强模型的适应性。根据式(10)，首先计算 R_{ij}^{k} 的熵，如

$$H(R_{ij}^{k})=-R_{ij}^{k}\log_2R_{ij}^{k}-(1-R_{ij}^{k})\log_2(1-R_{ij}^{k}) \tag{11}$$

信息熵反映信息的无序化程度，而各推荐信任的熵则反映了它们之间的差异程度，也即各推荐信任偏离推荐信任集合这一整体的程度。恶意节点出于诽谤正常节点或哄抬恶意节点的目的，其对评价节点的推荐信任必然偏离节点的实际信任值，可以利用信息熵将其识别出来，从而降低其对节点信任值客观性和准确性的影响。一般来说，推荐信任值之间的差异程度越小，其对节点的评价就相对越客观，因而，可以利用熵根据式(12)计算推荐信任的权重如下：

$$\omega_k=\frac{1-\dfrac{H(R_{ij}^{k})}{\log_2R_{ij}^{k}}}{\displaystyle\sum_{k=1}^{n}\left[1-\frac{H(R_{ij}^{k})}{\log_2R_{ij}^{k}}\right]} \tag{12}$$

最后，全局间接信任可以由式(13)计算得到：

$$R_{ij}=\sum_{k=1}^{n}\left(\omega_kR_{ij}^{k}\right) \tag{13}$$

2.3 综合信任

全局间接信任计算完成后，评价节点 i 利用熵权法将直接信任和间接信任进行合成，从而得到被评价节点 j 的综合信任值，提高信任评估的准确性，并避免了主观分配权重的局限性。根据信息熵来确定权重，其实质就是利用评价指标所提供信息的效用值，也就是根据评价指标值之间的差异程度对

指标的权重进行修正，因此，综合信任可以由式(14)计算：

$$\begin{cases} T_{ij} = D_{ij} & \gamma \geqslant \gamma_0 \\ T_{ij} = \omega_D D_{ij} + \omega_R R_{ij} & \text{else} \end{cases} \tag{14}$$

其中，ω_D 和 ω_R 分别为直接信任和间接信任的自适应权重，$H(D_{ij})$ 和 $H(R_{ij})$ 分别为直接信任和间接信任的信息熵，分别计算如下：

$$H(D_{ij}) = -D_{ij}\log_2 D_{ij} - (1-D_{ij})\log_2(1-D_{ij}) \tag{15}$$

$$H(R_{ij}) = -R_{ij}\log_2 R_{ij} - (1-R_{ij})\log_2(1-R_{ij}) \tag{16}$$

$$\omega_D = \frac{1-\dfrac{H(D_{ij})}{\log_2 D_{ij}}}{\left[1-\dfrac{H(D_{ij})}{\log_2 D_{ij}}\right]+\left[1-\dfrac{H(R_{ij})}{\log_2 R_{ij}}\right]} \tag{17}$$

$$\omega_R = \frac{1-\dfrac{H(R_{ij})}{\log_2 R_{ij}}}{\left[1-\dfrac{H(D_{ij})}{\log_2 D_{ij}}\right]+\left[1-\dfrac{H(R_{ij})}{\log_2 R_{ij}}\right]} \tag{18}$$

3　仿真实验与分析

本文利用 NS2 作为仿真工具来分析所提信任模型的性能，假设网络中所有节点都处于静止状态，仿真环境设置如下：100 个节点随机分布在 100 m×100 m 的正方形检测区域内，所有节点的数据转发率均设置为区间[0.9，1.0]内的随机数，从而模拟网络中非入侵因素导致的节点数据异常。随机选择 0~20%的节点为恶意节点，恶意节点发起选择性转发攻击、欺骗篡改攻击，并向其他节点提供虚假推荐信任。具体仿真参数如表 1。

表1　仿真参数

参数	值
仿真区域	100 m×100 m
节点数	100
节点半径	20 m
节点初始能量 E_{init}	0.5 J
传输和接收能耗 E_{elec}	50 nJ/bit
放大器功耗 ε_{amp}	10 pJ/(bit/m^2)
每个节点每轮传递数据包大小	80 bit

3.1　节点信任的变化

图 3 给出了正常节点和恶意节点的信任变化趋势图。由图 3 可以看出，正常节点的信任值随采样周期逐渐上升并趋近于 1，恶意节点的信任则随采样周期递减而最终趋近于 0，表明本文所提方案能够有效区别正常节点和恶意节点，从而检测出网络中的恶意节点并将其隔离出网络。

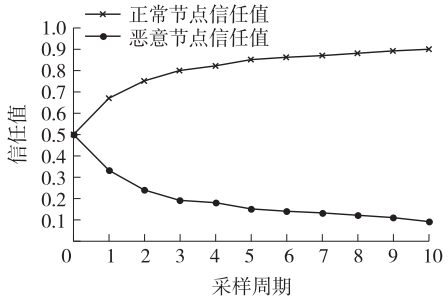

图3　节点信任变化趋势

3.2　引入置信度的合理性

直接信任的置信度水平用来确定直接信任是否足够可信能够作为综合信任。为分析引入置信度的合理性，将本方案与文献[16]中的方法进行比较，如图 4 所示。从图 4 中可以看出，尽管直接信任值保持基本不变，但是本文中直接信任的置信度随着交互数据的增加而增大，而文献[16]中直接信任的置信度基本保持不变，显然，本文方案能有效区分具有相同直接信任值的不同节点的置信度，而文献[16]中的方法则不能。

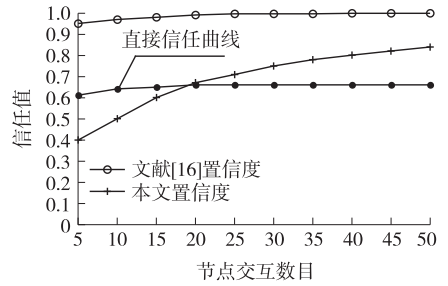

图4　置信度在不同交互数目下的变化趋势

3.3　网络安全性分析

信任模型根据网络中节点的行为特征对节点进行量化信任评估，其最终的目标是识别出网络中恶意节点，因此，检测率和误检率是分析信任模型性能的两个重要指标。这里的检测率是指利用信任评估方案检测出的恶意节点与网络中所有恶意节点之比，而误检率是指利用信任评估方案被误检的节点占网络中所有被检测节点总数的比例，其中误检包括正常节点被检测成恶意节点及恶意节点被检测为正常节点。为分析本文所提方案的优劣，将本文方案与不带异常衰减因子 q 的方案及文献[7]中的方案进行比较，不同恶意节点比例下的检测率和误检率如图 5 和图 6 所示。

从图 5 可以看出，随着恶意节点比例的增加，三种方案的节点检测率都逐渐下降，其中文献[7]方案下降趋势最快，这是因为文献[7]在进行信任融合时，仅传播好的声誉，由此得到的节点信任并

不准确，有些恶意节点可能会因其冲突行为特征导致信任值较高，从而无法被检测到。本文方案相较于无 q 时的方案，其检测率略低，这是因为 q 的存在，削弱了恶意节点的某些异常行为，因而可能导致部分恶意节点漏检，但是，在仿真实验中，通过调整 q 值可以获得较大的检测率和较小的误检率。

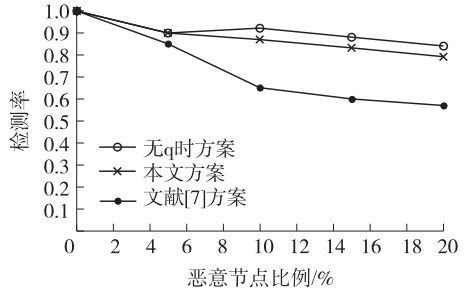

图5 检测率对比图

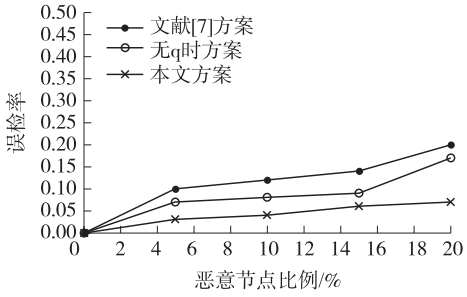

图6 误检率对比图

从图 6 可以看出，随着恶意节点比例的增加，三种方案中节点的误检率都逐渐升高，其中，本文方案的误检率最低，这是因为异常衰减因子的引入，排除了一部分非入侵因素导致的节点异常行为的影响，因此，降低了网络中节点的误检率，性能明显优于其他两种方案。

综上所述，本文方案可以实现较低的节点误检率，虽然异常衰减因子的引入会造成一定的恶意节点漏检率，但可以调整 q 值来实现较高的检测率和较低的漏检率。

3.4 q 对网络安全性的影响

为了分析异常衰减因子 q 对网络检测率及误检率的影响，即对网络安全性能的影响，在相同仿真环境下，分别设置 q 的取值为{0.2，0.4，0.6，0.8，1.0}，通过多次实验取平均值来比较其检测率和误检率，仿真结果如图 7 所示。

从图 7 可以看出，检测率随着 q 值的增大而增大，误检率则呈现先降低后增高的一个趋势，这是因为 q 值过低时，某些恶意节点的异常行为会被掩盖，造成其被误判为正常节点，而当 q 值过高时，可能会因为非入侵因素导致的节点异常行为的存在，而将正常节点误判为恶意节点。异常衰减因子的实质是由于入侵因素即网络攻击行为导致的节点不合作次数 $N_{\text{intrusion}}$ 与网络中实际检测出的节点不合作总数 $N_{\text{detection}}$ 之比，因而，在实际应用中，由于网络环境是动态变化的，异常衰减因子的取值并不是固定的，需要根据具体的网络环境进行自适应调整。从图中可以看出，在本文实验环境下，当 q 值为 0.8 时，网络的安全性能最高，即检测率和误检率的比值最小，也就是说网络获得了较高的恶意节点检测率及较低的正常节点误检率，因此，本文在仿真实现中设置异常衰减因子为固定值，即 q=0.8。

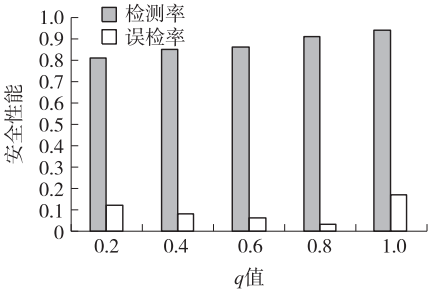

图7 q 值对检测率和误检率的影响

3.5 能耗分析

为分析本文模型的能耗，在不同网络情况下对能耗进行实验分析，利用文献[17]中的能量模型进行仿真实验，仿真结果如图 8 所示。图 8 给出了 1 000 轮仿真实验过程中，本文方案与 RFSN 方案的网络能量变化趋势，从图中可以看出，随着仿真实验的进行，网络能量均呈下降趋势，但本文方案在不同恶意节点比例下及不同实验阶段均高于 RFSN 方案。即无论在何种网络环境下，本文方案都比 RFSN 消耗更少的能量，这是因为本文方案仅在直接信任的置信度低于阈值的情况下，才需要计算间接信任，因此，有效节约了网络能量，提高了网络的生存周期。

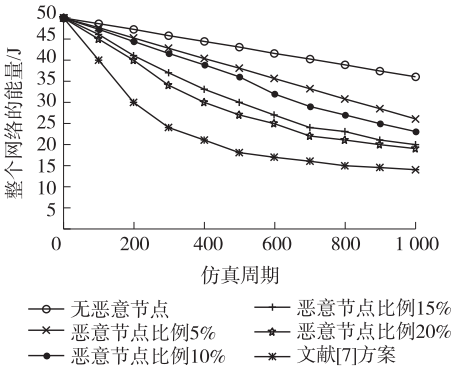

图8 网络能量变化趋势

4 结论

本文提出一种基于贝叶斯的改进 WSN 信任评估模型。考虑到非入侵因素带来的网络异常行为，

利用异常衰减因子来修正贝叶斯公式，在保证较高检测率的前提下，有效降低了网络的误检率；为了实现模型的轻量化，利用直接信任置信度的概念来判断是否需要计算间接信任。此外，自适应遗忘因子加强了模型的动态性和准确性，根据熵来分配权重克服了主观分配权重的局限性。仿真结果表明所提方案有较高的检测率和较低的误检率，同时有效节约了网络能量。

参考文献：

[1] 赵金辉，孙宇佳，硕良勋 . 基于集对分析的无线传感器网络风险信任模型[J]. 传感技术学报，2015，28(6)：927-932.

[2] Wahid A，Kumar P. A Survey on Attacks，Challenges and Security Mechanisms in Wireless Sensor Network[J]. International Journal for Innovative Research in Science and Technology，2015，1(8)：189-196.

[3] 房卫东，张小珑，石志东，等 . 基于二项分布的无线传感器网络信任管理系统[J]. 传感技术学报，2015，28(5)：703-708.

[4] Fang W，Zhang C，Shi Z，et al. BTRES：Beta-Based Trust and Reputation Evaluation System for Wireless Sensor Networks[J]. Journal of Network and Computer Applications，2016，59：88-94.

[5] Ishmanov F，Malik A S，Kim S W，et al. Trust Management System in Wireless Sensor Networks：Design Considerations and Research Challenges[J]. Transactions on Emerging Telecommunications Technologies，2015，26(2)：107-130.

[6] Kumar G E P，Titus I，Thekkekara S I. A Comprehensive Overview on Application of Trust and Reputation in Wireless Sensor Network[J]. Procedia Engineering，2012，38：2903-2912.

[7] Ganeriwal S，Balzano L K，Srivastava M B. Reputation-Based Framework for High Integrity Sensor Networks[J]. ACM Transactions on Sensor Networks(TOSN)，2008，4(3)：15.

[8] Mejia M，Peña N，Muñoz J L，et al. A Game Theoretic Trust Model for on-Line Distributed Evolution of Cooperation in MANETs[J]. Journal of Network and Computer Applications，2011，34(1)：39-51.

[9] Tian C，Yang B. Trust：A Reputation and Risk Based Trust Management Framework for Large-Scale，Fully Decentralized Overlay Networks[J]. Future Generation Computer Systems，2011，27(8)：1135-1141.

[10] Bao F，Chen I R，Chang M J，et al. Hierarchical Trust Management for Wireless Sensor Networks and Its Applications to Trust-Based Routing and Intrusion Detection[J]. IEEE Transactions on Network and Service Management，2012，9(2)：169-183.

[11] Anita X，Bhagyaveni M A，Manickam J. Fuzzy-Based Trust Prediction Model for Routing in WSNs[J]. The Scientific World Journal，2014.

[12] Aivaloglou E，Gritzalis S. Hybrid Trust and Reputation Management for Sensor Networks[J]. Wireless Networks，2010，16(5)：1493-1510.

[13] Wu G，Du Z，Hu Y，et al. A Dynamic Trust Model Exploiting the Time Slice in WSNs[J]. Soft Computing，2014，18(9)：1829-1840.

[14] Zhang B，Huang Z，Xiang Y. A Novel Multiple-Level Trust Management Framework for Wireless Sensor Networks[J]. Computer Networks，2014，72：45-61.

[15] 刘力，周建中，杨莉，等 . 基于熵权的灰色聚类在洪灾评估中的应用[J]. 自然灾害学报，2010，19(4)：213-218.

[16] Denko M K，Sun T，Woungang I. Trust Management in Ubiquitous Computing：A Bayesian Approach[J]. Computer Communications，2011，34(3)：398-406.

[17] Heinzelman W R，Chandrakasan A，Balakrishnan H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks[C]//Proceedings of the 33rd Annual Hawaii International Conference on System Sciences，2000，2：3005-3014.

周治平(1962-)，男，江苏无锡人，博士，江南大学教授，主要研究方向为检测技术与自动化装置、信息安全等，zzp@jiangnan.edu.cn；

邵楠楠(1990-)，女，山东烟台人，江南大学在读硕士研究生，研究方向为无线传感器网络安全，snnjiangnan@sina.com。