稀疏无线传感器网络中基于 beta 分布的信任模型 *

徐小龙[a]，林亚平[a,b]，周四望[b]，朱铁军[a]
（湖南大学 a. 计算机与通信学院；b. 软件学院，长沙 410082）

摘　要：针对无线传感器网络节点随机部署的不均匀性、节点能量消耗的非均衡性以及节点容易被俘获窜改的妥协性等，提出一个基于 beta 分布的稀疏网络信任模型。该模型充分考虑了稀疏网络的自身特点，利用 beta 密度函数构建节点的信任值并进行实时更新。模拟实验与分析表明：该模型能有效剔除节点发送的虚假数据和准确识别出失效节点，优化网络性能，为拓扑控制算法、数据收集压缩算法等提供一个可信的支撑环境。

关键词：无线传感器网络；信任模型；稀疏网络；beta 分布；妥协性
中图分类号：TP393　　**文献标志码**：A　　**文章编号**：1001-3695(2009)06-2232-03
doi:10.3969/j.issn.1001-3695.2009.06.070

Trust model based on beta distribution for sparse wireless sensor networks

XU Xiao-long[a], LIN Ya-ping[a,b], ZHOU Si-wang[b], ZHU Tie-jun[a]
(*a. School of Computer & Communication, b. School of Software, Hunan University, Changsha* 410082, *China*)

Abstract: Considering the wireless sensor network isn't uniformly distributed, and energy consumption for each node can't be balanced, even some nodes are captured or compromise to send forged data and so on, this paper proposed a trust model for sparse network based on beta distribution. After the characteristic of the sparse network had been fully taken into account, then each node's trust value could be easily computed and updated in cycle by the beta density function. Simulation results and analysis show that this trust model can eliminate the false data which is sent by malicious nodes effectively and identify failure nodes accurately, thereby optimizes the performance, provides a credible supporting environment for topology algorithm, data compression algorithm etc.

Key words: wireless sensor networks; trust model; sparse networks; beta distribution; compromise

无线传感器网络是由大量传感器节点通过无线自组方式构成的非传统网络，已经广泛应用于军事、环境检测和预报、智能家居、城市交通控制、空间探索、复杂机械监控等领域[1,2]。因为部署传感器网络的区域通常是难以接近的区域（如敌方军事区域）或不能接近的区域（如自然保护区）等，非和平的人文环境或恶劣的自然环境使得这些随机部署在野外的节点容易受到各种各样的损害。比方说敌方捕获到网络中某个节点对其结构进行窜改，恶意向邻居节点或簇头发送虚假数据，甚至干扰正常的路由；部署在热带雨林自然保护区里的传感器节点则可能受高温多雨的影响导致内部的传感器模块、通信模块发生故障，从而引发较高的误警率。因此，传感数据是否可信已逐渐成为衡量无线网络性能的一个重要指标。

为保证无线传感器网络数据可信度，一些学者将传统网络中的数据认证机制和数字水印技术分别引进无线网络来剔除或过滤虚假数据，取得了一定的研究成果[3,4]。但是数据认证机制需要在数据包后附加 t 个 MAC 信息，从而额外消耗了网络能量，这对能量受限的传感器网络来说不是很理想。数字水印技术并不需要这种额外的认证信息，而是将水印离散分布到数据的各个部分，同样可以达到防窜改目的。然而对数字水印技术来说，一旦某个节点被捕获和控制就极容易泄露用于认证的密钥，从而可以伪造虚假数据和用于认证的秘密信息，因此数字水印技术也不适合传感器网络。

另有一些学者借鉴传统网络电子商务中的信任体系[5]构建适合无线传感器网络特点的信任模型，也取得了一定的研究成果[6~9]。他们的工作都是基于密集无线网络考虑的，存在各自的缺点。如文献[6]假设簇内节点监测数据服从正态分布 $N(\mu,\sigma)$ 来构筑信任体系过于牵强；文献[7]提出的信任模型要求每个节点维持一个参数数据库较为苛刻；文献[8]假设存在第三方信任节点过于理想化等；文献[9]则仅仅将文献[5]中的基于 beta 密度函数的信任模型直接引入了传感器网络，并未对参数的取值进行优化。

稀疏无线传感器网络主要是指节点稀疏分布，允许存在黑洞或盲点现象，而现有的信任模型都在回避这种情形。因此，本文在充分考虑稀疏无线传感器网络特点的基础上，构建一个基于 beta 密度函数的信任模型，同时对参数的取值进行优化。

1　相关研究

Beta 分布的密度函数如下：

$$f(x|\alpha,\beta)=\Gamma(\alpha+\beta)/[\Gamma(\alpha)\Gamma(\beta)]x^{\alpha-1}(1-x)^{\beta-1} \quad (1)$$

其中：$0<x<1$；$\alpha>0$；$\beta>0$。

在文献[5]中，Josang 指出：之所以可以用 beta 密度函数来构建信任体系，是因为它的简单性和灵活性同时具有很强的统计理论基础。例如对流行的 C2C 电子商务来说，参数 α 和 β 可以分别代表交易双方的成功次数和失败次数，甚至可以根据

收稿日期：2008-10-09；**修回日期**：2008-12-06　　**基金项目**：国家“863”计划资助项目(2006AA01Z227)

作者简介：徐小龙(1983-)，男，湖北孝感人，硕士研究生，主要研究方向为无线传感器网络拓扑控制、可信计算(longrenren@126.com)；林亚平(1955-)，男，湖南邵阳人，教授，博导，主要研究方向为计算机网络、机器学习；周四望(1971-)，男，湖南岳阳人，副教授，博士，主要研究方向为无线传感器网络小波分析；朱铁军(1981-)，男，湖南娄底人，硕士研究生，主要研究方向为无线传感器网络数据压缩算法分析与设计.

交易时间早晚、交易金额大小等因素对 α、β 进行加权等优化计算,从而得到较为稳定可靠的电子商务信任体系。文献[9]接受了这种先进的思想和经验,将 beta 密度函数引进无线传感器网络来构建信任模型。但其对 beta 密度函数参数的选取非常简单直观,α 就是任意两个节点发送数据成功的次数(successful interactions),β 就是任意两个节点发送数据失败的次数(unsuccessful interactions),从而得到节点 s_i 和 s_j 在任意时刻 t 的信任值:

$$R^t_{s_{ij}} = \Gamma(\alpha+\beta+2)/[\Gamma(\alpha+1)\Gamma(\beta+1)]x^{\alpha}(1-x)^{\beta} \quad (2)$$

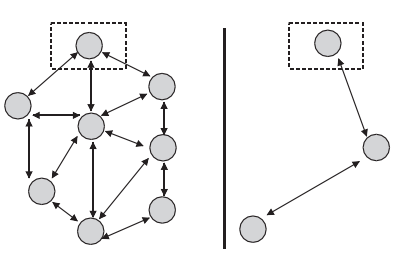
从参数的选取上看模型[2]太过粗糙,因为传感器网络毕竟不同于传统电子商务网络,数据发送成功或失败次数的多寡并不能主导信任值的度量,同时传感器网络是以数据为中心的网络。因此,主导信任值度量的应该是数据的质量。那么在无线传感器网络中构建基于 beta 密度函数的信任函数时应该以发送数据的质量为主要出发点,在对信任值进行更新时才考虑节点间的合作次数(cooperations)。对于以事件为驱动的特殊应用型传感器网络,这种考虑是尤为必要的。

还有一点也很重要,那就是传感器网络节点稀疏与否。通常情况下认为节点应该是大规模高密度随机分布,应该以节点数量的巨大来保证数据的可信。但事实并非如此,有些区域是不可能密集分布的(如地方军事区域或自然保护区等),即便密集分布也不代表是均匀分布,总有很多地方出现盲点或黑洞现象。当然节点能量非均衡消耗导致网络变得稀疏同样值得去考虑。在密集网络下,信任模型比较容易构建,如 2.1 节提出的信任邻居节点可以构建一个较好的信任模型。但是,在稀疏网络中这样的信任邻居节点是不存在的,因此相对而言稀疏网络中的信任模型构建要困难得多。显然,文献[9]没有意识到这种问题的存在而缺少必要的细节处理,模型性能的稳定性就得不到保证。

2　基于 beta 密度函数的信任模型

2.1　稀疏网络分析

图 1(a)是传感器网络节点密集分布示意图,从图中可以很清楚地知道每个节点至少有两个邻居节点或者更多。这种图连通性强,当虚线矩形对应的节点监测到异常数据时,它周围邻居节点的监测数据也会有相应的波动。图 1(b)是传感器节点稀疏分布示意图,处在网络边缘的节点仅有一个邻居节点(图论中称为悬点)。这种网络图的连通性极差,当虚线矩形对应的节点检测到异常数据时,它惟一的邻居节点可能并未检测到。



(a) 密集图示意　　(b) 稀疏图示意

图 1　网络节点分布示意图

本文就是研究图 1(b)这样的稀疏网络。为了研究的方便,首先给出信任邻居节点的形式化定义:称节点 j 是节点 i 的信任邻居节点,当节点 j 满足下面的条件:

$$\text{trust\_value}(j,t) - \text{trust\_thresholdValue}(t) \geqslant 0 \quad (3)$$

$$\sqrt{(x_i-x_j)^2+(y_i-y_j)^2} \leqslant \text{distance\_thresholdValue}(t) \quad (4)$$

$$|\text{node\_data}(j,t) - \text{node\_data}(i,t)| \leqslant \text{data\_thresholdValue}(t) \quad (5)$$

其中:trust_value(j,t)表示节点 j 在 t 时刻的信任值;(x_j,y_j)是节点 j 的地理位置坐标;节点 j 在 t 时刻的检测数据为 node_data(j,t)。在稀疏网络中这样的信任邻居节点是不存在的。

2.2　可移动节点引入

对于稀疏传感器网络,某节点发送异常数据时当前簇头并不能判断出它是否正确,因为此节点的周围并不存在信任邻居节点。直观上可以让整个网络试运行一段时间以积累信任值,那么当节点的信任值稳定以后簇头再根据各节点的信任值就很容易判断。问题在于,传感器网络是资源受限的特殊网络,节点电源不可更换;同时,节点在网络后期发生故障或者遭遇攻击的可能性更大。因此,数据发送成功或失败的次数的多寡并不能主导信任值的度量。图 2 是节点潜伏攻击的实例。敌方首先实施技术攻击捕获和窜改正常节点,然后让其正常工作一段时间以积累较高的信任值,最后在关键时刻让节点发送虚假数据来实施攻击;此外,节点发送错误数据还具有很大的随机性。那么在稀疏网络中单纯依赖节点的历史行为来构建信任模型的性能并不是很稳定。因此,本文假设每个节点所在的簇均存在一个可移动节点。这点事实上是可以保证的,一方面节点可移动不存在任何技术难题,没有大规模部署是因为成本太大;另一方面可移动节点的投放可在普通节点之后进行,因为数量不是很多,所以均匀投放很简单。引入可移动节点是本文基于 beta 分布信任模型的基础。这些节点并不进行正常的数据监测任务,绝大部分时间处于空闲状态以节省能量。当簇内出现异常数据时,由簇头广播数据需要核实消息,簇内普通节点不予回应,簇内可移动节点则执行相应的数据核实任务,示意图如图 3 所示。

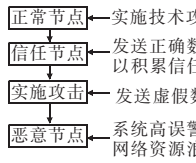


图 2　恶意节点潜伏攻击实例图

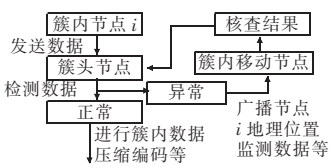


图 3　簇内可移动节点工作示意图

簇内移动节点在接收到簇头广播的数据核查消息后,根据消息中包含的发送异常数据节点的地理位置信息移动到该节点的检测区域内进行数据检测,然后将检测到的结果和簇头广播的数据核查消息中的数据利用式(5)进行比较。如果满足式(5),则认为核查结果为真向簇头发送 OK 消息确认;否则发送 error 消息否定。

2.3　Beta 密度函数参数选取

在稀疏网络中引入可移动节点之后,就可以对节点发送的异常数据进行真假核实。前面已经指出 beta 密度函数很适合构建信任体系;同时,beta 密度函数的两个参数 α 和 β 对模型的性能影响很大。为了保证信任模型性能的稳定性,两个参数的选取仍要依赖上节引入的可移动节点。

设簇内有 n 个工作节点,在第 k 轮簇的数据通信阶段,节点 i 发送异常数据经簇内移动节点确认是正确和错误数据的次数为 o_i^k 和 p_i^k,t_i^k 和 m_i^k 为其正常发送和没有发送数据的次数。那么对任意 $i \in \{1,2,\cdots,n\}$,对应节点的信任值系数为

$$\alpha_i^k = w_1 o_i^k + w_2 t_i^k + 1 \quad (6)$$

$$\beta_i^k = w_1 p_i^k + w_2 m_i^k + 1 \quad (7)$$

其中：w_1 和 w_2 是信任值惩罚因子，且 $w_1 + w_2 = 1$。

2.4 信任值计算与更新

本节根据在上节确定的 beta 密度函数的两个参数式(6)和(7)来计算簇内任意节点在第 k 轮的信任值，用 temp_value(i,k)来表示，有

$$\text{temp\_value}(i,k) = \Gamma(\alpha_i^k + \beta_i^k)/[\Gamma(\alpha_i^k)\Gamma(\beta_i^k)]x^{a_i^k}(1-x)^{\beta_i^k} \quad (8)$$

其中：x 是一个概率变量满足 $E(x) = a_i^k/(\alpha_i^k + \beta_i^k)$。

又假设 trust_value$(i,k-1)$为节点 i 在 k 轮的信任值，那么 k 轮过后，节点的信任值按式(9)更新：

$$\text{trust\_value}(i,k) = w_1^* \times \text{trust\_value}(i,k-1) + w_2^* \times \text{temp\_value}(i,k) \quad (9)$$

其中：w_1^* 和 w_2^* 为信任值均衡因子，且 $w_1^* + w_2^* = 1$。初始条件：$\forall i \in \{1,2,\cdots,n\}$，trust_value$(i,0) = 0.5$。

需要说明的是，利用 beta 密度函数计算节点在每一轮的信任值并没有一味地依赖节点的历史发送数据，而是对发送数据，进行了两次加权使得潜伏节点并不能获得较高的信任值。例如第一次加权式(6)(7)可令 $w_1 = 0.9$，$w_2 = 0.1$；第二次加权式(9)可令 $w_1^* = 0.4$，$w_2^* = 0.6$。

3 模拟实验与分析

在模拟实验中有两个概念：a)节点失效等级(node fai-lure level)，用符号 FL 表示，定义为失效节点数目占所有工作节点数目之比；b)节点失效模式(node failure pattern)，用符号 FP 表示，为研究方便只考虑节点持续发送异常数据(记 FP = 0)、间断发送异常数据(记 FP = 1)、偶尔发送异常数据(记 FP = 2)三种情形。此外，记簇内可移动节点能有效达到目标区域的概率为 r。此时引入参数 r 是必要的，一方面可移动节点并不总能有效到达指定监测区域；另一方面考虑到随着技术的进步，r 必将增大趋于 1，因此没有在模型的构建中提出而仅仅将其作为模拟实验的一个参数。

利用仿真软件 OMNeT ++ 3.3 Win32(exe)建立一个稀疏仿真网络。网络监测区域为 300 × 300，节点数目 100 个，按虚拟网格 100 × 100 将其分为 9 个簇。节点每隔 10 s 向簇头发送一次数据，簇的理论维持时间为 1 000 s，之后重新进行簇头选举。为简单起见，簇头选举算法仅仅比较各竞选簇头节点的信任值，信任值第一的可成功竞选。

图 4 给出了当 $r = 30\%$ 和 50% 时模型过滤虚假数据的结果，一共进行了 10 次实验。当 $r = 30\%$ 时虚假数据过滤率维持在 66% 左右，当 $r = 50\%$ 时则其达到了 85% 左右。这表明在稀疏网络中引入可移动节点是合理且有效的，而且随着 r 的增大，模型性能将会有显著提升。

最后对比了模型(式(2))(记为 original method)和本文模型(式(9))(记为 our method)在不同 FP 下的节点失效诊断率。为使本文的模型更具说服力，在对比实验中 r 取值仅为 30%。如果 r 的取值较大，虽然实验结果更显著但与实际不相吻合。

图 5 给出 FP = 0 时，两种模型的节点失效诊断率几乎都接近 1，这是因为失效节点持续发送虚假数据会导致自身的信任迅速下降。从图 6 可以看出，当 FP = 1 时，随 FL 的增大 our method 呈微弱的上升趋势，而 original method 则出现较小的波动。但在图 7 中，两种模型均有微弱的上升趋势，原因可能是 FP = 2 时失效节点发送虚假数据的随机值种子小所导致。通过对比图 5 ~ 7 不难发现，本文的信任模型较原始的信任模型在性能上有较大的改善而且比较稳定，特别在 FP = 1 和 2 时效果尤为显著。

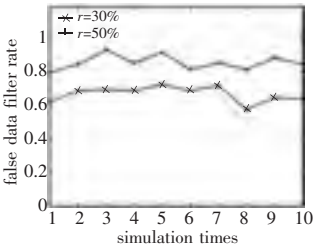


图 4 r=30%和 50%时虚假数据过滤

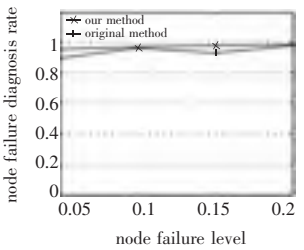


图 5 FP=0 时失效节点诊断率对比

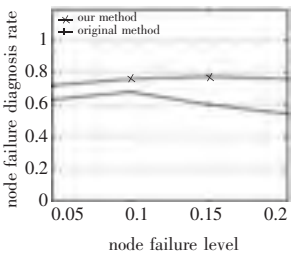


图 6 FP=1 时失效节点诊断率对比

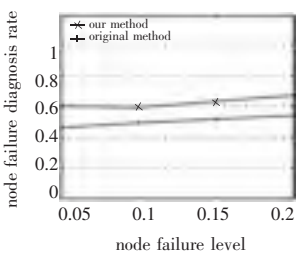


图 7 FP=2 时失效节点诊断率对比

4 结束语

本文通过分析传感器网络数据可信和稀疏网络的自身特点，在簇内引入可移动节点，提出一个基于 beta 分布的稀疏网络信任模型。该模型利用 beta 密度函数对节点的信任值进行构建和实时更新。模拟实验与分析表明：该模型能有效剔除节点发送的虚假数据和准确识别出失效节点，优化网络性能，为拓扑控制算法、数据收集压缩算法等提供一个可信的支撑环境。下阶段将重点考虑基于此信任模型构建无线传感器网络中的数据压缩算法和拓扑控制算法。

参考文献：

[1] ARAMPATZIS T H, LYGEROS J, MANESIS S. A survey of applications of wireless sensor networks[C]//Proc of the 13th Mediterranean Conference on Control and Automation. 2005: 27-29.

[2] 李建中，高宏. 无线传感器网络的研究进展[J]. 计算机研究与发展，2008，45(1)：1-15.

[3] YE Fan, LUO Hai-yun, LU Song-wu. Statistical en-route filtering of injected false data in sensor networks[J]. IEEE Journal on Selected Areas in Communication, 2005, 23(4): 732-744.

[4] 彭志娟，王汝传，王海艳. 基于数字水印技术的无线传感器网络安全机制研究[J]. 南京邮电大学学报：自然科学版，2006，26(4)：69-72.

[5] JOSANG A, ISMAIL R. The beta reputaion system[C]//Proc of the 15th Bled Electronic Commerce Conference. 2002: 1-14.

[6] ZHANG Wei, DAS S, LIU Yong-he. A trust based framework for secure data aggregation in wireless sensor networks[C]//Proc of the 3rd Annual IEEE Communications Society on Sensor and Ad hoc Communications and Networks. 2006: 60-69.

[7] YAO Zhi-ying, KIM D, DOH Y. PLUS: parameterized and localized trust management scheme for sensor networks security[C]//Proc of IEEE International Conference on Mobile Ad hoc and Sensor Systems. 2006: 437-446.

[8] HAN Guang-jie, CHOI D, LIM W. A novel sensor node selection method based on trust for wireless sensor networks[C]//Proc of International Conference on Wireless Communications, Networking and Mobile Computing. 2007: 2397-2400.

[9] CROSBY G V, PISSINOU N. Cluster-based reputation and trust for wireless sensor networks[C]//Proc of the 4th Consumer Communications and Networking Conference. 2007: 604-608.