一种基于 Bayes 估计的 WSN 节点信任度计算模型

刘 涛[1,2] 熊 焰[2] 黄文超[2] 陆琦玮[2] 关亚文[1]
(安徽工程大学计算机与信息学院 芜湖 241000)[1]
(中国科学技术大学计算机科学与技术学院 合肥 230027)[2]

摘 要 鉴于传统网络安全策略无法阻止或识别传感器网络内部节点的攻击或异常行为,结合节点资源受限的特点,提出了一种无线传感器网络节点信任度计算模型。该模型采用 Bayes 估计方法,通过求解基于 Beta 分布的节点行为信誉函数的期望值得到直接信任并将其作为 Bayes 估计的先验信息,将来自邻居节点的推荐信息作为其样本信息。仿真实验表明,本方案有较好的稳定性,能够有效识别异常节点,从而阻止内部节点对网络的攻击,与 RFSN 相比,不仅节约了存储空间、运算时间与通信量,而且能够避免恶评现象对节点信任度计算的影响。

关键词 无线传感器网络,信任度计算模型,Bayes 估计,先验信息,信誉,Beta 分布
中图法分类号 TP393 **文献标识码** A

Trust Computation Model of Nodes Based on Bayes Estimation in Wireless Sensor Networks

LIU Tao[1,2] XIONG Yan[2] HUANG Wen-chao[2] LU Qi-wei[2] GUAN Ya-wen[1]
(School of Computer and Information, Anhui Polytechic University, Wuhu 241000, China)[1]
(College of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China)[2]

Abstract Traditional network security policy can not prevent attack or identify abnormal behavior of the internal nodes in the sensor network. This paper presented a trust computation model of nodes based on Bayes estimation in wireless sensor networks (Abbreviates as TCM-BE) according to the node resource-constrained characteristics. The direct trust which calculates the expectations of the reputation function on nodes behavior based on beta distribution is priori information and the recommendation information from neighbor nodes as sample information in Bayes estimation method. The simulation shows that the scheme has good stability, can effectively identify abnormal node, thereby can prevent attack from the internal nodes of the network. The analysis shows that compared with RFSN scheme it not only can save storage space and computing time with traffic, but also can avoid the phenomenon of malicious evaluation on the node trust.

Keywords Wireless sensor networks, Trust computation model, Bayes estimation, Priori information, Reputation, Beta distribution

1 概述

无线传感器网络(Wireless Sensor Networks, WSN)由大量能独立进行信息采集、无线通信、数据存储和处理的节点以自组织的方式组成,其节点和物理世界紧密相连,由于无需预先部署基础设施,在车辆流量控制、目标跟踪、战场环境、抢险救灾、环境威胁探索等领域具有广泛的应用前景[1]。但是用于通信的无线通道可以被任何人访问,同时节点在计算能力、存储、通讯带宽和电池能量等方面严重受限,使得任何恶意的攻击者都可以发动一组特定的攻击导致网络部分或全部不可用。因此,WSN 突显的重要性由于安全问题而受阻[2]。为了解决 WSN 的安全问题,必须采取一套安全策略,如加密、认证等安全机制。但大多数机制都假定网络中所有的节点本身是可信的,然而网络中节点有可能因被捕获或者自私行为而提供错误的服务或不提供服务,从而变得不可信,采用完全信任的方式将导致泛洪攻击和拒绝服务等攻击,从而引发大量安全问题,因此需要对节点的可信性进行评估。目前关于 WSN 可信研究最多的是基于节点行为的信任管理,文献[3]利用通信实体的信誉计算其信任度,并指出信誉分布服从 Beta 分布的特点;文献[4]将文献[3]的思想应用于 WSN,提出了一种经典计算信任模型 RFSN;文献[5]也采用同样的方法计算节点的信任度;文献[6]采用主观逻辑改进 RFSN 的信誉更新方法,这类模型可较好地识别低信誉度节点,但无法消除高信誉节点的恶意推荐对网络造成的影响;文献[7]针对

到稿日期:2012-12-25 返修日期:2013-04-07 本文受国家自然科学基金青年科学基金(61300170,61202404),国家自然科学基金(61170233,61232018),安徽省教育厅自然科学基金(KJ2013A040,KJ2012B012),安徽省自然科学基金(1308085MF88)资助。
刘 涛(1973—),女,硕士,副教授,CCF 会员,主要研究方向为计算机网络与信息安全;熊 焰(1960—),男,教授,博士生导师,主要研究方向为计算机网络与信息安全、移动计算与移动网络等,E-mail:dqcltdz@126.com;黄文超(1982—),男,博士后,主要研究方向为信息安全与移动计算;陆琦玮(1988—),男,博士生,主要研究方向为信息安全与移动社交网络;关亚文(1990—),男,硕士生,主要研究方向为网络安全。

Ad-hoc网络提出了基于半环代数理论的信任模型，该模型有较好的恶意行为检测能力，但是采用信任链的方法聚合推荐信任，因其收敛速度慢而降低了可扩展性。文献[8]对文献[7]思想进行改进并将其应用在WSN中，设计出针对路由和数据分组丢弃攻击的模糊信任模型。文献[9]同样指出为了评测节点的不良行为，需要引入信誉系统。文献[10]以TCG规范[11]为目标，在节点认证前提供硬件级别的强安全机制来保证节点的可信性，但TCG规范所规定的基于装载前度量的可信传递方式并不能保证系统运行时处于可信状态[12]，另外其复杂运算及硬件成本也使得该方法难以推广。在WSN中，要求信任模型的计算只能具有轻量级的时空复杂度，并具有很强的可扩展性[8]。本文针对大规模无人值守WSN设计一种轻量级的节点信任度计算模型，该模型根据信任度可以判断节点是否可信，保证节点只与可信节点进行通信，从而提高网络服务的安全性。

2 基于Bayes估计的信任度计算(TCM-BE)

WSN经常部署在无人值守的环境，易遭敌手攻击或因自身能量消耗等原因而变得不可靠，因此需引入可信评估机制来确保通信对象是可信的。在分布式WSN中，节点以自组织方式实现一个节点对另一个节点的信任度计算，计算的依据主要是两个节点直接交互行为结果形成的直接评价即直接信任，以及来自两节点共同邻居的推荐信息即间接信任。

2.1 Bayes估计方法

Bayes估计是将决策方法应用于研究统计的一种方法，贝叶斯推论视为科学方法的一种应用，因为通过贝叶斯推论来更新概率要求从对于不同假设的初始信任度出发，采集新的信息，然后根据新的信息调整原有的信念。

设给定样本：$X=(X_1,X_2,\cdots,X_n)=(x_1,x_2,\cdots,x_n)$，如果总体$X\sim N(\mu,\sigma^2)$，$\mu$未知$\sigma$已知，$\mu$的先验分布为$\mu\sim N(\mu_1,\sigma_1^2)$，则可求出$\mu$的Bayes估计为[13,14]：

$$\bar{\mu}=\left(\frac{n\bar{x}}{\sigma^2}+\frac{\mu_1}{\sigma_1^2}\right)/\left(\frac{n}{\sigma^2}+\frac{1}{\sigma_1^2}\right) \tag{1}$$

且$\bar{x}=\frac{1}{n}\sum_{i=1}^{n}x_i$。

式中，μ是待估计的参数，μ_1是μ的先验信息，先验信息不会是一个确定的值，而是一个分布。此时，$L(\mu,d)=(\mu-d)^2$即损失函数为二次损失函数，是参数点估计中常用的一种损失函数。Bayes估计是将μ的先验信息和样本信息在Bayes公式作用下，推导出μ的后验信息，即μ的估计值。

2.2 Bayes估计方法与节点信任度计算拟合

节点信任度的估算依据直接评价和来自邻居节点的推荐评价，记节点i收集到来自n个有效节点对j的评价值为$(x_1,x_2,\cdots,x_n)$。文献[15]指出邻域内不同节点对同一节点通信行为的信任总体分布X近似服从正态分布$N(\mu,\sigma^2)$，因为一个节点的信任取值范围为[0,1]，所以可取总体方差σ为1。文献[13]指出先验信息μ_1具有"矫正"样本带来的错误信息的作用，为了避免RFSN模型中高信誉节点恶意推荐的影响，并考虑网络拓扑的动态性，本文采用以直接信任为先验信息，即以节点的主观信任为主、以其他节点的推荐信任为辅的思想，这符合WNS复杂的动态拓扑和无线信道不稳定带来的不确定性特征，也适应传感器网络安全自治的需求。文献[3,4]指出节点的直接信任来自对节点信誉的评价，而节点的信誉服从Beta分布，因此直接信任不是固定值，是一个分布，这从理论上也证明可用直接信任代替先验信息，用$\mu\sim N(\mu_1,\sigma_1)$表示。这里先验方差$\sigma_1$的选择将决定对推荐信任的采纳程度，若先验方差足够小，则估计值大大向直接信任靠拢，从而缓解恶评数据对估计的影响，当方差较大时则更多考虑其他节点的推荐意见，具体方差的值可以依据应用环境来确定。另外，因为信任总体分布X服从正态分布，所以对信任估计的损失函数可以选取为二次损失函数，即$L(\mu,d)=(\mu-d)^2$。

因此，对于信任的估计，式(1)的前提条件都满足，故可利用Bayes估计方法求节点的信任度。

2.3 先验信息μ_1的计算

由上述知，本案的先验信息为一个节点对另一节点的直接信任。文献[3]指出用户信誉分布服从Beta分布，本文和RFSN模型[4]一样采用Beta分布来表示传感器节点行为的信誉，并对文献[3]中信誉更新进行改进，求得节点i对j的直接信任度。

Beta分布有两个参数(α,β)，利用伽玛函数Γ表示Beta分布$f(p|\alpha,\beta)$如下[3]：

$$p\in[0,1],\alpha>0,\beta>0 \tag{2}$$

Beta分布的概率期望值为：

$$E(p)=\alpha/(\alpha+\beta)$$

$$f(p|\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{\alpha-1}(1-p)^{\beta-1} \tag{3}$$

事件发生后有两种结果：成功或失败。用s表示某时段成功通信事件发生的总次数，f表示某时段失败通信事件发生的总次数。那么经过$s+f$次事件后，后验分布仍然服从Beta分布，函数中参数(α,β)满足：

$$\alpha=s+1,\beta=f+1 \tag{4}$$

其中$s,f\geqslant 0$。

则直接信任值T_{ij}计算如下：

$$T_{ij}=E(Beta(s+1,f+1))=\frac{r+1}{r+s+2} \tag{5}$$

根据文献[3]思想，假设在t_1时刻节点i关于节点j的信誉分布的先验概率为X，服从Beta分布，记为$X\sim Beta(\alpha_j+1,\beta_j+1)$，$t_2$时刻节点$i$和节点$j$又执行了$s+f$次事件之后，信誉的分布仍然服从Beta分布且新的分布X'满足：

$$X'\sim Beta(\alpha_j+s+1,\beta_j+f+1) \tag{6}$$

式(4)中没有考虑节点信誉动态性问题，这里引入时间遗忘因子$\theta(\theta\in[0,1])$来调整阶段历史信誉对最近信誉的影响，则直接信誉更新计算公式表达为[5]：

$$X'\sim Beta(\alpha_j\theta+s+1,\beta_j\theta+f+1) \tag{7}$$

为了便于计算，采用递归的方式求Beta分布的参数，因此执行了$s+f$次事件之后Beta分布参数变化为[4]：

$$\alpha_j=\alpha_j\theta+s,\beta_j=\beta_j\theta+f \tag{8}$$

直接信任计算公式更新为：

$$T_{ij}=E(Beta(\alpha_j+1,\beta_j+1))=\frac{\alpha_j+1}{\alpha_j+\beta_j+2} \tag{9}$$

因此，根据节点存储的(α_j,β_j)值，可以求出对节点评价的先验信息μ_1即T_{ij}。

2.4 推荐信息的获取

网络预部署时为每个节点分配一个标识ID并设定系统参数(σ,σ_1,T_r)，T_r为信任阈值。为了节省能量，每个节点只与相邻节点发生直接交互。网络部署后每个节点广播自己的

ID，相应节点记下自己邻居的 ID，并设置 α_j，β_j，r，f 初值。每隔一个周期，节点 i 向邻居节点发送包含目标 j 标识的信任请求包，邻居节点 k 在收到发起节点 i 的请求包后，查询节点 j 是否在自己的邻居列表中，根据查询结果，产生一个应答包，将自己对被评估节点 j 的信任度 T_{kj}^k 送给节点 i。为了防止低信誉度节点攻击，主节点将所有收集到的邻居节点对目标节点的推荐信任值进行预处理，若 i 对 k 的信任 $T_{ik}<T_r$，则舍弃该节点 k 发送的推荐评价。

2.5 节点信任度的计算

设 i 收集到的关于 j 的 n 个有效推荐评价即样本信息为 $(x_1,x_2,\cdots,x_n)$，i 保存 j 的历史信誉分布参数 (α_j,β_j) 以及最近交互的结果 (s,f)，σ 和 σ_1 已给定。计算过程如下：

S1：将历史信誉分布参数和最近交互的结果代入式(8)计算新的信誉分布参数 (α_j,β_j)；

S2：将新的信誉分布参数代入式(9)计算 μ_1；

S3：求出 $\bar{x}$，利用式(1)求 $\bar{\mu}$。

$\bar{\mu}$ 即为 i 对 j 的总体信任评价即信任度，i 根据 $\bar{\mu}$ 的值对 j 作出决策。

3 方案分析

在设计方案时，既要保证方案的安全性，又要考虑运行的效率，特别是对于资源受限的 WSN 更要考虑运行的效率。

3.1 理论分析

(1)安全性分析

节点定期计算邻居节点的信任度，避免了与具有 Sinkhole 攻击、Wormhole 攻击、选择性转发攻击、能量不足或自私节点的交互，提高了网络安全性和服务效率。但是信任系统本身也是攻击者攻击的对象，本文在构建信任模型时采用一定的策略来保证节点的安全性。如引入节点的身份标识，以保证身份与实体唯一对应关系，避免节点通过非法宣称多个身份而实现 Sybil 攻击，同时预防节点通过有意的离开再加入系统来消除以前身份的低信任度的 Newcomer 攻击；引入时间遗忘因子预防叛国者攻击；对推荐信息进行预处理，遏制低信誉度节点的错误推荐攻击。

(2)效率分析

本案与 RFSN 的直接信任计算方法一致，因此两者在计算直接信任时的资源消耗一样。下面比较两者对信任的合成。

将本模型中式(1)化解为：

$$\bar{\mu}=(AS+B\mu_1)/(An+B) \tag{1'}$$

式中，$A=\sigma^{-2}$，$B=\sigma_1^{-2}$，为了减少传感器节点计算的次数，在网络部署前进行节点预处理时直接加载 A、B；$S=x_1+x_2+\cdots+x_n$。因此本案中在直接信任已知的前提下，需要做约 $n+5$ 的数学运算即可求得最终信任值。在存储空间上 n 个 x_k 累加求和只需要两个变量，即每收到一个有效评价就直接加入总和 S 中，因此共需要 7 个变量或常量参与运算。通讯上，每个节点只发送一个数据 x_k 作为推荐信息。

在 RFSN 中，最终信任值 T 的计算如下[4]：

$$T=E(beta(\alpha_j^{new},\beta_j^{new}))$$

其中，

$$\alpha_j^{new}=\alpha_j+\sum_{i=1}^{n}\frac{2\alpha_{k_i}\alpha_j^{k_i}}{(\beta_{k_i}+2)(\alpha_j^{k_i}+\beta_j^{k_i}+2)+2\alpha_{k_i}}$$

$$\beta_j^{new}=\beta_j+\sum_{i=1}^{n}\frac{2\alpha_{k_i}\beta_j^{k_i}}{(\beta_{k_i}+2)(\alpha_j^{k_i}+\beta_j^{k_i}+2)+2\alpha_{k_i}}$$

计算 α_j^{new} 和 β_j^{new} 需要 $20n$ 次数学运算。计算 T 需要 n 对 (α_k,β_k) 和 n 对 (α_j^k,β_j^k)，因此共需变量为 $4n+5$ 个。通讯上，每个节点发送两个数据 (α_j^k,β_j^k) 作为推荐信息。

由上可知，与 RFSN 相比，本案运算次数、通信量都减少了，存储空间大幅下降，更适合资源有限的 WSN。

3.2 仿真分析

通过在 Matlab7.0 环境下仿真，考察本模型对环境和节点“状态”变化的适应能力，以及与 RFSN 的比较。实验参数设置：α_j，β_j，r，f 初值均为 0，$\sigma=1$，$\sigma_1=0.1$，$T_r=0.5$，网络节点数为 $N=200$，两个节点的共同邻居 $n=10$。

(1)本模型信任收敛性

图 1 给出的是正常节点和异常节点随着网络运行其信任值的变化。由图 1 知，一个正常节点(或异常节点)经过多次通讯后，其信任值趋于稳定。某正常节点的信任值如果出现剧烈抖动，则可能遭到攻击或出现故障。

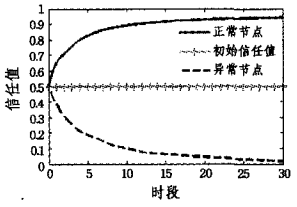

图 1 信任收敛趋势

(2)σ_1 对信任值的影响

图 2 给出在相同直接信任和推荐信息的前提下，先验方差取不同值时信任的变化。

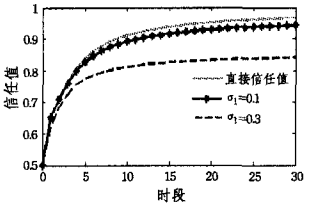

图 2 σ_1 对信任值的影响

由图 2 知，σ_1 取不同值时，节点信任值也在变化。σ_1 越小，信任值越接近直接信任。

(3)错误推荐攻击对信任的影响

图 3 给出了在网络中存在高信誉的第三方节点恶意推荐情况下两种模型计算信任值的变化。

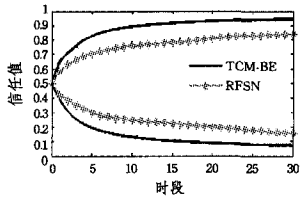

图 3 错误推荐攻击对信任影响的比较

由图 3 知，相对于 RFSN 方案，本案(TCM-BE)采用 Bayes 估计方法并以主节点对目标节点的直接信任作为先验信息，有效遏制高信誉节点的恶评现象，避免信任系统中有多个说谎者为系统提供错误推荐信息。

(4)耗能分析

文献[16]给出在 MICA2 传感器上，节点发送与接收一个字节的能耗分别为 59.2μJ 和 28.6μJ，设一个消息数据长度 $d=41$ 字节，节点做一次算术运算的功耗要远小于发送与接收的功耗，仿真时忽略不计。假设在一个计算信任周期内每个节点向邻居节点发送消息 c 次，同时对方接收消息 c 次，每个节点均要计算其邻居节点(网络节点为 N，邻居个数为 $n\approx\sqrt{N}$[17])的信任值。计算信任值的能耗 $E=E1+E2$，$E1$ 和 $E2$ 分别为计算直接信任与间接信任值时的能耗。两种方案的直接信任计算能耗一样，即 $E1\approx c*n(59.2+28.6)d)\mu J$，而本案中 $E2\approx(n*(59.2+28.6)d)\mu J$，RFSN 方案 $E2\approx(2*n*(59.2+28.6)d)\mu J$。仿真实验中假定 $c=10$，仿真结果如图 4 所示。

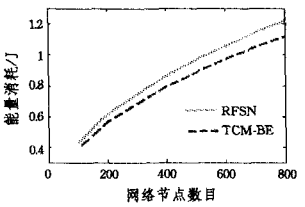

图 4　计算信任值时的能耗比较

图 4 表示的是两种方案在没有考虑算术运算时计算一次综合信任值所消耗能量的对比，而 RFSN 方案中涉及的算术运算次数远大于本案(TCM-BE)。因此，与 RFSN 相比，本案节约了能量，更适合能量有限的 WSN。

结束语　信任管理是安全机制的补充，本文提出了一种基于 Bayes 估计的节点信任度计算模型，该模型充分考虑 WSN 拓扑多变、高度自治、节点资源受限等特点，采用节点对其他节点信任度进行的评估以自身的经验为主，同时考虑邻居节点的推荐信息的轻量级计算方法，其可扩展性强，适合大规模无人值守网络。在不同的应用环境下可以通过改变先验方差 σ_1 的值来调节直接信任和推荐信息在信任值计算中的比重。实验结果表明，该计算模型能够以较小计算、存储与通信代价实现与 RFSN 同等程度的安全，将异常节点或恶意节点排除在网络之外，提高了网络的安全性。

参 考 文 献

[1] 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

[2] Lopez J，Roman R，Agudo I，et al. Trust management systems for wireless sensor networks：Best practices[J]. Computer Communications，2010，33：1086-1093

[3] Jøsang A，Ismail R. The Beta Reputation System[C]// 15th Bled Electronic Commerce Conference. Bled，Slovenia，June 2002：41-55

[4] Ganeriwal S，Srivastava M B. Reputation-based framework for high integrity sensor networks[C] // Proceedings of the 2nd ACM Workshop on Se curity of Ad-hoc and Sensor Networks (SASN'04). Washington DC，USA，2004：66-77

[5] 肖德琴，冯健昭，杨波，等. 基于无线传感器网络的信誉形式化模型[J]. 计算机科学，2007，34(6)：84-87，100

[6] 谢福鼎，周晨光，张永，等. 应用主观逻辑的无线传感器网络信任更新算法[J]. 计算机科学，2011，38(9)：50-54

[7] Theodorakpoulos G，Baras J S. On Trust models and trust evaluation metrics for ad-hoc networks[J]. IEEE Journal on Selected Areas in Communications，2006，24(2)：318-328

[8] 王良民，郭渊博，詹永照. 容忍入侵的无线传感器网络模糊信任评估模型[J]. 通信学报，2010，32(12)：37-45

[9] Ahmed M R，Huang Xu，Sharma D. A Novel Misbehavior Evaluation with Dempster-Shafer Theory in Wireless Sensor Networks[C] // MobiHoc'12. Hilton Head，South Carolina，USA，June 2012：259-260

[10] Yussoff Y M，Hashim H，Baba M D. Identity-based Trusted Authentication in Wireless Sensor Network[J]. International Journal of Computer Science Issues，2012，9(3)：1694-0814

[11] Grawrock D. TCG specification architecture overview [EB/OL]. Technology Report. Trusted Computing Group Revision 1.4 (2007)，http：// www. trustedcomputinggroup. org/resources/tcg_architecture_overview_version_14，2012

[12] 张兴，黄强，沈昌祥. 一种基于无干扰模型的信任链传递分析方法[J]. 软件学报，2010，33(1)：74-81

[13] 数理统计编写组. 数理统计[M]. 西安：西北工业大学出版社，1997：42-49

[14] 陈希孺，倪国熙. 数理统计学教程[M]. 合肥：中国科学技术出版社，2009：189-211

[15] 杨光，印桂生，杨武，等. 无线传感器网络基于节点行为的信誉评测模型[J]. 通信学报，2009，30(12)：18-26

[16] 王卫生，张永. WSN 中一种高效鲁棒的对等认证方案[J]. 计算机工程与应用，2012，48(5)：65-70

[17] 蹇波，郭永辉，罗长远，等. 基于 ECC 的无线传感器网络密钥管理协议[J]. 计算机工程，2010，36(3)：142-144

(上接第 55 页)

[4] Yeh M-K，Jiang J-R，Huang S-T. Adaptive splitting and pre-signaling for RFID tag anti-collision[J]. Computer Comunications，2009(32)：1862-1870

[5] He Ming-xing，Horng S-J，et al. A Fast RFID Tag Identification Algorithm Based on Counter and Stack[J]. Expert Systems with Applications，2011(38)：6829-6838

[6] Lai Yuan-Cheng，Lin C-C. Two Couple-Resolution Blocking Protocols on Adaptive Query Splitting for RFID Tag Identification [J]. IEEE Transactions on Mobile Computing，2012(11)：1450-1463

[7] 丁治国，朱学永，等. 自适应多叉树防碰撞算法研究[J]. 自动化学报，2010，36(2)：237-241

[8] 张学军，蔡文琦，王锁萍. 改进型自适应多叉数防碰撞算法的研究[J]. 电子学报，2012，1：193-198

[9] 樊文静，张姗姗，田智慧. 基于后退式二进制搜索的 RFID 防碰撞算法的研究[J]. 计算机应用与软件，2012，29(5)：191-194

[10] 张航，唐明浩，程晖. 改进的返回式二进制防碰撞算法[J]. 计算机工程与应用，2011，47(25)：208-211

[11] 冯娜，潘伟杰，李少波，等. 基于新颖跳跃式动态搜索的 RFID 防碰撞算法[J]. 计算机应用，2012，32(1)：288-291