高技术通讯 2010 年 第 20 卷 第 12 期:1253 ~ 1259

doi:10.3772/j.issn.1002-0470.2010.12.008

基于 Mamdani 模糊推理的无线传感器网络可信簇头选举算法①

冯仁剑②* 成 竖** 许小丰* 万江文③*

(*北京航空航天大学仪器科学与光电工程学院 北京 100191)

(**武汉军械士官学校无人机系 武汉 430075)

摘 要 为了解决无线传感器网络中恶意节点成为簇头而引起的层次路由安全问题,提出了一种基于 Mamdani 模糊推理的可信簇头选举算法(TCEM)。TCEM 算法根据节点的行为表现,采用贝叶斯原理评估节点信任值,在此基础上,结合密集度及向心度,使用 Mamdani 模糊推理方法计算节点优越度,选择最优者作为簇头,从而实现簇头的可信选举。仿真实验结果表明,该算法能有效阻止恶意节点成为簇头,且在簇头合理分布、网络整体能效等方面均有良好表现。

关键词 无线传感器网络,簇头选举,路由安全,Mamdani 模糊推理

0 引 言

无线传感器网络的层次路由协议具有网络能耗小、通信效率高、管理方便、可扩展性强的优势[1,2],有广阔的应用前景。现实中复杂的应用背景对层次路由提出了严格的安全要求,基于密钥体系的安全机制只能抵抗外部攻击,设计思路与实现机制都无法解决网络内部节点被俘导致的路由安全问题[3,4]。网内的被俘节点会被改造成恶意节点,使网络受到路由丢弃、贪婪破坏和方向误导等攻击。当一定比例的簇头成为恶意节点时,整个网络就陷入瘫痪[5]。如何选择安全可信的簇头是层次路由必须解决的问题。因此,作为密钥安全体制的有效补充,信任管理的概念被引用到簇头选举过程中。

Crosby 等人[5]提出由成员节点对邻居节点进行信任的投票,原簇头统计得票并选取得票最多者作为新的簇头,以确保新簇头的可信。但该算法未考虑节点的剩余能量问题,且在共谋攻击下,容易错误地选择恶意节点作为簇头。Krasniewski 等人[6]利用基站对簇头选举进行集中式信任管理,若发现新簇头不可信,则重新选举簇头,有效避免了恶意节点充当簇头,但这种管理增大了网络通信负荷,被动的信任决策降低了簇头选举的收敛速度。Song 等人[7]在低能耗自适应分簇分层(LEACH)算法中加入信任成分,使节点选择信任值最高的邻居节点作为簇头。其分布式的算法收敛速度快,但基于信誉推荐的信任管理容易受到共谋攻击,对节点基于二元逻辑的信任分类限制了节点的使用效率。Hsieh 等人[8]利用基站对 LEACH 算法所得簇头进行筛选,剔除信任值较低的簇头,有效提高了簇头选举的安全性,但该算法要求簇头与基站直接通信,加快了节点的能量耗尽,缩短了网络生命周期。以上算法均偏重于簇头的可信,对簇头的合理分布考虑不够充分,不能均衡信任管理带来的额外能耗,导致了网络整体能效的降低。为了进一步提高无线传感器网络层次路由的安全,本文提出了一种基于 Mamdani 模糊推理的可信簇头选举算法(trusted cluster-head election algorithm based on Mamdani fuzzy inference, TCEM)。该算法能够选择最优节点为簇头,从而确保所选簇头的可信和合理分布,提高网络的安全性和整体能效。

1 网络初始化

包含若干节点的无线传感器网络,被随机布撒在某检测区域,分布足够密集。节点能量初始同构,且消耗后无法补充。网络布置完成后,节点完成以下初始化任务:

(1)通过 GPS 等手段获取自身位置信息;

(2)广播查询邻居节点的 ID 和坐标值;

(3)建立邻居节点信任表 $< i, S_i, F_i, T_i >$。其中:i 为邻居节点的 ID;S_i 和 F_i 分别是对邻居节

① 863 计划(2009AA01Z201),国家自然科学基金(60873240,60974121)和北京市教育委员会共建项目专项资助。

② 男,1976 年生,博士,副教授,硕士生导师;研究方向:传感网络与信息融合,传感系统与仪器等。

③ 通讯作者,E-mail: sensory@buaa.edu.cn

(收稿日期:2009-08-08)

点 i 网络行为正确和错误次数的统计值，初始值均为0；T_i 为邻居节点 i 的信任值，初始值为0.5。

2 TCEM算法

TCEM算法的实现过程如下：网络采用簇头轮选机制。每次簇头选举开始时，节点采用LEACH算法所得簇头作为候选簇头，普通节点根据信任表评估邻居候选簇头的信任值，同时，候选簇头计算自身密集度和向心度，并向邻居普通节点广播，最后，普通节点利用邻居候选簇头的信任值、密集度和向心度，采用Mamdani模糊推理方法计算其优越度，选择优越度最大者为簇头，并加入该簇。

2.1 信任值

评估一个节点的可信程度是对该节点未来行为好坏的预测。因此，节点的信任值就是其行为随机分布的数学期望值。在网络初始化阶段，由于缺乏先验信息，无法预先确定节点的行为分布。因此，如何确定节点行为分布情况是评估节点信任值的关键和难点。

2.1.1 节点信任评估模型

设本地节点对邻居节点 i 进行信任值评估，节点 i 的网络行为正确率为 γ，服从行为分布 $p(\gamma)$。在网络初始化阶段，由于缺乏先验信息，可以认为 γ 平均分布于[0,1]，即 $p(\gamma)=Uni(0,1)=Beta(1,1)$，故信任初始值 $T_i=\mathrm{E}[Beta(1,1)]=0.5$，并假设在这一段时间内本地节点观察得到节点 i 的网络行为正确和错误的次数分别为 S_i 和 F_i。已知 $Beta(1,1)$ 为 γ 的先验分布，而网络行为样本服从于参数为 γ 的二项分布，根据贝叶斯原理，γ 的后验分布为[9]

$$p(\gamma)=\frac{Bin(S_i+F_i,S_i)\cdot Beta(1,1)}{Normalization}=Beta(S_i+1,F_i+1) \tag{1}$$

由式1可知，节点 i 的网络行为正确率 γ 服从于参数为 S_i+1 和 F_i+1 的 $Beta$ 分布。因此，节点 i 的信任值计算公式如下式所示：

$$T_i=E[Beta(S_i+1,F_i+1)]=\frac{S_i+1}{S_i+F_i+2} \tag{2}$$

2.1.2 候选簇头的信任值评估

候选簇头的信任值评估过程设置如下：(1)网络行为的记录：本地节点对所有邻居节点近期网络行为进行统计，为簇头选举中候选簇头信任值的计算提供依据；(2)信任值的计算：簇头选举开始时，本地节点更新邻居节点信任表中的网络行为记录，计算邻居候选簇头的信任值。为了提高算法的收敛速度，并抵制恶意节点的共谋攻击，信任评估过程中不采用节点间的推荐。

(1) 网络行为的记录

在簇头轮选的间隙，本地节点对邻居节点 i 监听，统计节点 i 网络行为正确、错误次数的变化 ΔS_i 和 ΔF_i。为保证信任的新鲜性，每次信任值的计算完成后，本地节点将 ΔS_i 和 ΔF_i 置零，并重新计数。

(2) 信任值的计算

簇头选举开始时，本地节点利用 ΔS_i 和 ΔF_i 更新信任表中节点 i 的网络行为表现 S_i 和 F_i，如式

$$\begin{cases}S_i=(1-\omega)\cdot S_i+\omega\cdot\Delta S_i\\F_i=(1-\omega)\cdot F_i+\omega\cdot\Delta F_i\end{cases} \tag{3}$$

所示，其中

$$\omega=\begin{cases}\omega_h, \text{ if } \Delta S_i<\Delta F_i\\\omega_l, \text{ if } \Delta S_i\geqslant\Delta F_i\end{cases} \tag{4}$$

是更新权重。如式(4)所示，在更新过程中，根据节点行为的变化趋势动态选取 ω，这样既可以体现对节点恶意行为的严厉惩罚，又能够防止恶意节点的信任补偿，提高信任评估算法对恶意节点策略性攻击的鲁棒性。其中 $0<\omega_h,\omega_l<1$，且 $\omega_h>>\omega_l$。

若节点 i 被选为候选簇头，则将更新后的 S_i 和 F_i 值代入式(2)，即可计算得到该候选簇头的信任值。

综上所述，根据网络行为表现，采用贝叶斯原理实时计算候选簇头的信任值，可为综合评估候选簇头优越度提供安全依据。

2.2 密集度和向心度

候选簇头通过广播查询得知邻居节点的个数和坐标值，即可计算获得自身的密集度和向心度。

节点的密集度是指节点的邻居节点密集程度，即邻居节点的个数，用 N 表示。簇头的密集度越高，簇内通信能效相对越高[4]。由于无线传感器网络节点分布不均匀，因此考虑候选簇头的密集度有助于提高网络能效。

节点的向心度是指节点与邻居节点重心之间的接近程度，用 D 表示。设节点 i 为簇头，其坐标为 $(x_i,\ y_i)$，簇内成员节点是簇头 i 的邻居节点，坐标分别为 $(x_1,\ y_1),(x_2,\ y_2),\cdots,(x_n,\ y_n)$，则理想通信环境下，依据参考文献[10]，可以给出簇头 i 的簇内广播通信能耗 E_{total} 关于其坐标 $(x_i,\ y_i)$ 的函数：

$$E_{\text{total}}=\sum_{j=1}^{n}k[(x_i-x_j)^2+(y_i-y_j)^2] \tag{5}$$

其中 k 为常量系数。可以证明,当簇头 i 位于成员节点重心 $(\frac{1}{n}\sum_{j=1}^{n}x_j, \frac{1}{n}\sum_{j=1}^{n}y_j)$ 时,E_{total}最小,且簇头 i 越接近成员节点重心,E_{total}越小。证明过程如下。

根据二元函数极值定理可知,E_{total}在 $(\frac{1}{n}\sum_{j=1}^{n}x_j, \frac{1}{n}\sum_{j=1}^{n}y_j)$ 处取得最小值的充要条件是:①式(5)在 $(\frac{1}{n}\sum_{j=1}^{n}x_j, \frac{1}{n}\sum_{j=1}^{n}y_j)$ 处的一阶偏导数 $\frac{\partial E_{total}}{\partial x_i}$ 和 $\frac{\partial E_{total}}{\partial y_i}$ 均为零;②式(5)在 $(\frac{1}{n}\sum_{j=1}^{n}x_j, \frac{1}{n}\sum_{j=1}^{n}y_j)$ 处的二阶偏导数 $\frac{\partial^2 E_{total}}{\partial x_i^2}$ 大于零,且 $(\frac{\partial^2 E_{total}}{\partial x_i \partial y_i})^2$ 与 $\frac{\partial^2 E_{total}}{\partial x_i^2}\cdot\frac{\partial^2 E_{total}}{\partial y_i^2}$ 的差小于零。

首先,对式(5)求一阶偏导,得到式

$$\frac{\partial E_{total}}{\partial x_i} = 2kn(x_i - \frac{1}{n}\sum_{j=1}^{n}x_j) \tag{6}$$

$$\frac{\partial E_{total}}{\partial y_i} = 2kn(y_i - \frac{1}{n}\sum_{j=1}^{n}y_j) \tag{7}$$

由式(6)和式(7)可知,当 $x_i = \frac{1}{n}\sum_{j=1}^{n}x_j$, $y_i = \frac{1}{n}\sum_{j=1}^{n}y_j$ 时,$\frac{\partial E_{total}}{\partial x_i}$ 和 $\frac{\partial E_{total}}{\partial y_i}$ 都等于零,满足条件①。

其次,对式(5)求二阶偏导数 $\frac{\partial^2 E_{total}}{\partial x_i^2}$,并计算 $(\frac{\partial^2 E_{total}}{\partial x_i \partial y_i})^2$ 与 $\frac{\partial^2 E_{total}}{\partial x_i^2}\cdot\frac{\partial^2 E_{total}}{\partial y_i^2}$ 的差:

$$\begin{cases} \dfrac{\partial^2 E_{total}}{\partial x_i^2} = 2kn \\ (\dfrac{\partial^2 E_{total}}{\partial x_i \partial y_i})^2 - \dfrac{\partial^2 E_{total}}{\partial x_i^2}\cdot\dfrac{\partial^2 E_{total}}{\partial y_i^2} = -4k^2n^2 \end{cases} \tag{8}$$

由式(8)可知,当 $x_i = \frac{1}{n}\sum_{j=1}^{n}x_j$, $y_i = \frac{1}{n}\sum_{j=1}^{n}y_j$ 时,条件②也能满足。因此,当簇头 i 位于成员节点重心时,E_{total}最小。

由式(6)和式(7)可知,当 $x_i < \frac{1}{n}\sum_{j=1}^{n}x_j$, $y_i < \frac{1}{n}\sum_{j=1}^{n}y_j$ 时,E_{total}单调递减,当 $x_i > \frac{1}{n}\sum_{j=1}^{n}x_j$, $y_i > \frac{1}{n}\sum_{j=1}^{n}y_j$ 时,E_{total}单调递增。因此,簇头 i 越接近成员节点重心,E_{total}越小。

簇头 i 的向心度 D_i 如式

$$D_i = 1 - \frac{\sqrt{(x_i - \frac{1}{n}\sum_{j=1}^{n}x_j)^2 + (y_i - \frac{1}{n}\sum_{j=1}^{n}y_j)^2}}{r} \tag{9}$$

所示,其中 r 为节点通信半径。

由式(9)可知,簇头向心度越高,说明簇头与成员节点重心越接近,E_{total}也就越小。选择向心度高的簇头,有利于降低簇内通信能耗。此外,LEACH 算法所得的候选簇头分布不均匀,将导致网络通信能耗的增大,通过对候选簇头向心度的分析可以改善上述情况。因此,考虑候选簇头的向心度有助于簇头的合理分布,提高网络通信能效。

综上所述,通过对候选簇头密集度和向心度的分析,有利于簇头的合理分布,减少网络通信能耗,可为综合评估候选簇头优越度提供能效依据。

2.3 优越度的 Mamdani 模糊推理

候选簇头的优越度是根据其信任值、密集度和向心度计算得出的。由于信任的主观性、向心度的低准确性和优越度因子的不完备性会导致常规算法的不确定性,而模糊逻辑符合主观思维,模糊推理能在输入准确性较低、因子不完备的情况下得到实时的、确定的输出,且其模糊分类方式有利于提高节点的使用效率,因此节点优越度采用 Mamdani 模糊推理方法[11]来计算。

Mamdani 模糊推理过程如图 1 所示。输入模糊化接口将信任值、密集度和向心度的输入确定值转化为模糊集形式。模糊推理机根据输入模糊集,结合模糊规则库计算优越度的输出模糊集。最后,输

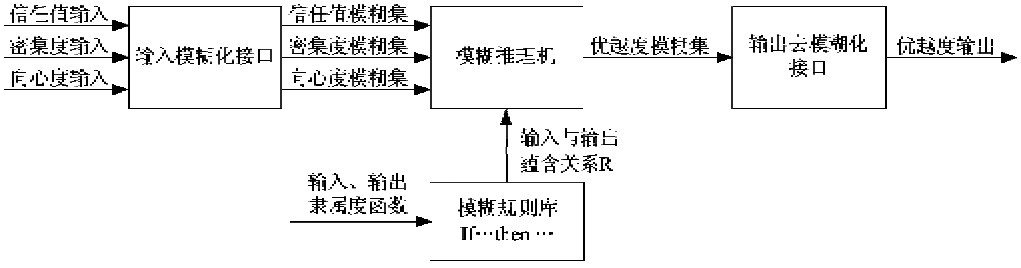


图 1 优越度的 Mamdani 模糊推理

出去模糊化接口将优越度模糊输出转化为确定值形式。

2.3.1 信任值、密集度及向心度的输入模糊化

候选簇头的信任值、密集度及向心度均为确定值形式，而模糊推理的输入必须是信任值、密集度、向心度的模糊集，因此必须对输入变量进行模糊化。设候选簇头 i 的信任值 $T_i = t^*$，密集度 $N_i = n^*$，向心度 $D_i = d^*$，对其进行单点模糊化，得到相应的模糊输入 $T^*(t)$、$N^*(n)$和 $D^*(d)$，如下式所示：

$$T^*(t) = \begin{cases} 1, \text{如果 } t = t^* \\ 0, \text{其他} \end{cases}$$
$$N^*(n) = \begin{cases} 1, \text{如果 } n = n^* \\ 0, \text{其他} \end{cases} \quad (10)$$
$$D^*(d) = \begin{cases} 1, \text{如果 } d = d^* \\ 0, \text{其他} \end{cases}$$

2.3.2 优越度的模糊推理

a.模糊规则库的建立

首先，建立输入、输出的语言变量集，即划分候选簇头信任值、密集度、向心度及优越度的模糊子集，并建立相应的隶属度函数。为了降低计算复杂度和减轻节点负荷，选择线性划分法并采用三角函数和梯形函数建立模糊子集的隶属度函数。

信任值、密集度和向心度的论域分别为：$T = \{t \mid t \in [0,1]\}$，$N = \{n \mid n \in [n_{\min}, n_{\max}]\}$，其中 $n_{\max}$ 和 $n_{\min}$ 分别为邻居节点个数的上限和下限，$D = \{d \mid d \in [0,1]\}$。使用线性划分法将信任值分为 $\{low, medium, high\}$，密集度分为 $\{few, adequate, rich\}$，向心度分为 $\{far, medium, close\}$，优越度分为 $\{very\ low, low, medium, high, very\ high\}$，如图 2 所示。

其次，依据推理经验，建立模糊推理规则，并表示为“*if*…*then*…”的形式。这里优越度用 *ad* 表示，其模糊集表示为 $AD(y)$。共建立 27 条规则：

If Trust is low, Concentration is few and Centrality is far, then ad is very low;

……

If Trust is medium, Concentration is adequate and Centrality is medium, then ad is medium;

……

If Trust is high, Concentration is rich and Centrality is close, then ad is very high;

最后，求取输入与输出的模糊蕴含关系。先求取单条模糊规则下的蕴含关系，如式

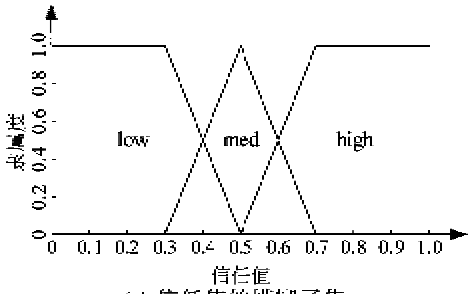
$$R_l = \text{“}T_h^l \text{ and } N_i^l \text{ and } D_j^l\text{”} \rightarrow AD_k^l = T_h^l(t) \wedge N_i^l(n) \wedge D_j^l(d) \wedge AD_k^l(y) \quad (11)$$

所示。其中 $T_h^l(t)$、$N_i^l(n)$ 和 $D_j^l(d)$ 为第 l 条模糊规则下的输入模糊子集，$AD_k^l(y)$ 为第 l 条模糊规则下的输出模糊子集。$\wedge$ 为 Zadeh 算子，表示 min 运算。输入模糊子集又可表示为

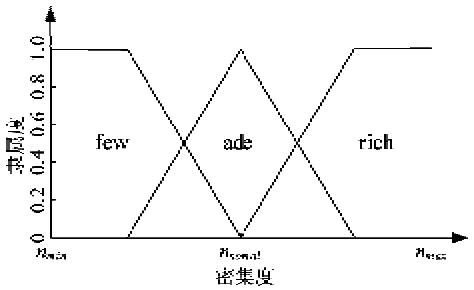
$$T_h^l(t) \wedge N_i^l(n) \wedge D_j^l(d) = A^l(t,n,d) \quad (12)$$

将式(12)代入式(11)，将式(11)转化为式(13)所示的简化形式：

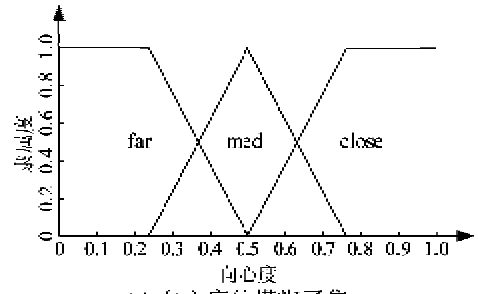
$$R_l = A^l(t,n,d) \wedge AD_k^l(y) \quad (13)$$



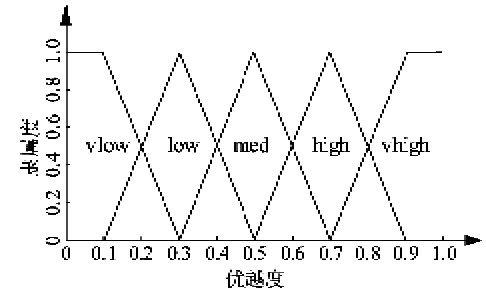
(a) 信任值的模糊子集



(b) 密集度的模糊子集



(c) 向心度的模糊子集



(d) 优越度的模糊子集

图 2 信任值、密集度、向心度及优越度的模糊分类

再将所有规则下的蕴含关系进行综合,即可得到多重规则下的蕴含关系式

$$R = \bigvee_{l=1}^{m} R_l = \bigvee_{l=1}^{m} (A^l(t,n,d) \wedge AD_k^l(y)) \quad (14)$$

其中,$\vee$ 为 Zadeh 算子,表示 max 运算,$m = 27$。

b.优越度的计算

式(10)中的模糊输入又可表示为

$$A^*(t,n,d) = T^*(t) \wedge N^*(n) \wedge D^*(d) \quad (15)$$

如式(16)所示,将模糊输入与模糊蕴含关系进行推理合成,即可求得候选簇头 i 的优越度模糊输出 $AD^*(y)$:

$$AD^*(y) = A^*(t,n,d) \circ R = \bigvee_{l=1}^{m} (q(A^l, A^*) \wedge AD_k^l(y)) \quad (16)$$

其中,$q(A^l, A^*)$为 $A^l(t, n, d)$与 $A^*(t, n, d)$的贴近度,反映了实际输入与模糊规则中的假设输入间的接近程度。$\circ$为 Zadeh 算子,表示合成运算。$q(A^l, A^*)$又可表示为

$$q(A^l, A^*) = \bigvee_{t,n,d \in T \times N \times D} (A^l(t,n,d) \wedge A^*(t,n,d)) = q(T_h^l, T^*) \wedge q(N_i^l, N^*) \wedge q(D_j^l, D^*) \quad (17)$$

将式(10)代入式(17),得

$$q(A^l, A^*) = T_h^l(t^*) \wedge N_i^l(n^*) \wedge D_j^l(d^*) \quad (18)$$

将式(18)代入式(16),即可得到优越度的模糊推理输出 $AD^*(y)$:

$$AD^*(y) = \bigvee_{l=1}^{m} (T_h^l(t^*) \wedge N_i^l(n^*) \wedge D_j^l(d^*) \wedge AD_k^l(y)) \quad (19)$$

2.3.3 优越度的去模糊化

将候选簇头 i 优越度的模糊输出 $AD^*(y)$去模糊化,即可得到其确定值 ad。这里采用式

$$ad = COG = \int_{AD^*} [AD^*(y) \cdot y]\, dy \Big/ \int_{AD^*} AD^*(y)\, dy \quad (20)$$

所示的重心法计算 $AD^*(y)$隶属度函数曲线包围区域的重心 COG。

综上所述,根据信任值、密集度和向心度,利用模糊分类,结合模糊蕴含关系,采用模糊合成算法,普通节点能够实时地、准确地计算得出各个邻居候选簇头的优越度,将优越度最高者选为簇头,从而完成簇头的可信选取过程,提高层次型网络的安全性。

2.4 算法复杂度分析

设网络节点总数为 N,分布区域面积为 S,节点的平均邻居个数为 n_{ave}。已知节点通信半径为 r,则 n_{ave}可表示为

$$n_{ave} = \frac{N\pi r^2}{S} \quad (21)$$

单节点运行 TCEM 算法选举可信簇头,最多需要计算 n_{ave}个候选簇头的优越度,而 $n_{ave} = N\pi r^2/S$,故计算复杂度为 $O(N)$。计算中,须存储相应的信任表、密集度、向心度以及优越度数据,存储量为 $4N\pi r^2/S$,故存储复杂度为 $O(N)$。

对于整个网络来说,实现 TCEM 算法最多需要计算 $N \times n_{ave}$个候选簇头的优越度,因此,计算复杂度为 $O(N^2)$。同理,存储复杂度也为 $O(N^2)$。

3 仿真实验与结果分析

实验基于 Matlab 平台,分别对 LEACH 算法、可信 LEACH(TLEACH)算法及 TCEM 算法进行了仿真。场景设置如下:200 个节点随机布撒在 100m × 100m 的检测区域;节点通信半径为 20m;设置 10%的节点为恶意节点,恶意节点有 80% ~ 100%的丢包率和 80% ~ 100%的错误转发率;节点采用文献[10]中的通信能耗模型。

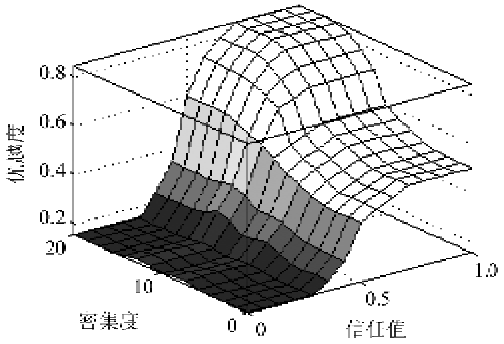
3.1 模糊推理模型分析

图 3 为 Mamdani 模糊推理模型中信任值、密集度和向心度输入与优越度输出之间的模糊蕴含关系。可以看出:当信任值较低时,不管密集度、向心度输入如何变化,优越度均偏低。当信任值逐渐增大时,优越度才随着密集度和向心度的增大而逐渐增大。这是由于在模糊规则的建立过程中,信任值被要求作为优越度的决定性前提。实际情况中,恶意节点为了提高自身优越度,会提供虚假的密集度、向心度信息。采用了这种模糊蕴含关系,算法就能有效地屏蔽恶意节点的欺骗行为。

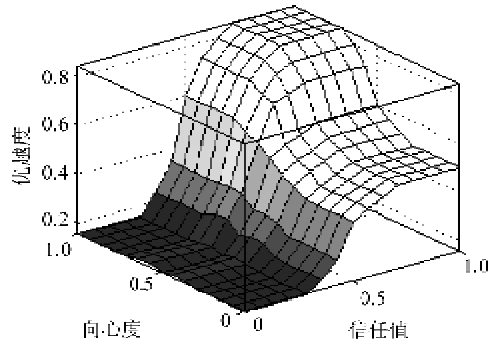
3.2 簇头信任分析

图 4 为 LEACH 算法、TLEACH 算法及 TCEM 算法下,网络前 100 轮簇头选举中恶意节点占簇头的比例。TCEM 算法下恶意节点占簇头的平均比例为 0.0045,明显低于 LEACH 算法下的 0.2705,并优于 TLEACH 算法下的 0.0130。这是因为 TCEM 算法重点考虑了候选簇头的信任值,并且由本地节点独立完成信任值评估,避免了共谋攻击,最大程度地确保了簇头的可信。由此可见,使用 TCEM 算法进行簇

头选举可以有效阻止恶意节点成为簇头。



(a) 信任值、密集度与优越度的蕴含关系



(b) 信任值、向心度与优越度的蕴含关系

图 3 TCEM 算法下的模糊蕴含关系

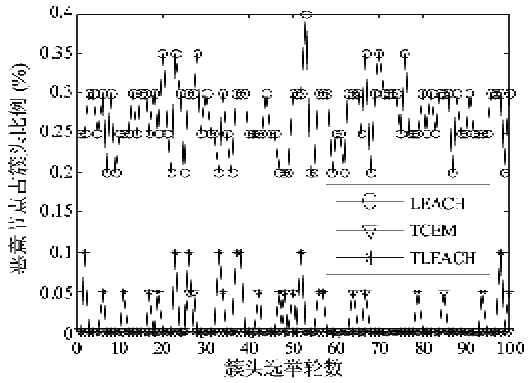


图 4 LEACH 算法、TCEM 算法和 TLEACH 算法下网络前 100 轮簇头选举中恶意节点占簇头比例

3.3 网络拓扑分析

图 5 和图 6 分别为使用 TCEM 算法和 LEACH 算法进行簇头选举后网络的拓扑结构。图中，TCEM 算法下簇头总数比 LEACH 算法有所减少，但整体分布比较均匀，且避免了 LEACH 中存在的簇头过于靠近和簇头边缘分布的现象，簇内的分布也比较合理，簇头靠近簇的重心。这是由于 TCEM 算法根据密集度和向心度对候选簇头进行筛选，避免了所选簇头的不合理分布，改善了网络拓扑结构，并提高了簇头的使用效率。由此可见 TCEM 算法对网络拓扑有较好的优化作用。

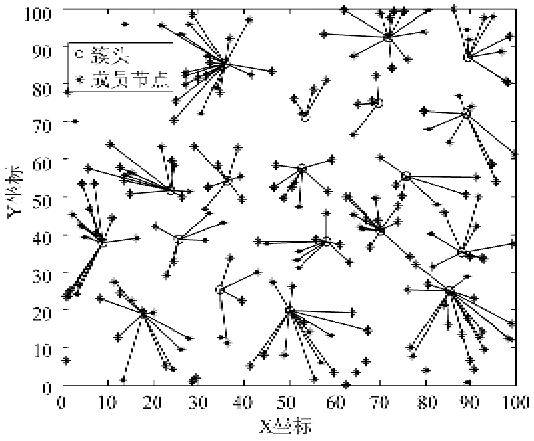


图 5 TCEM 算法下网络拓扑

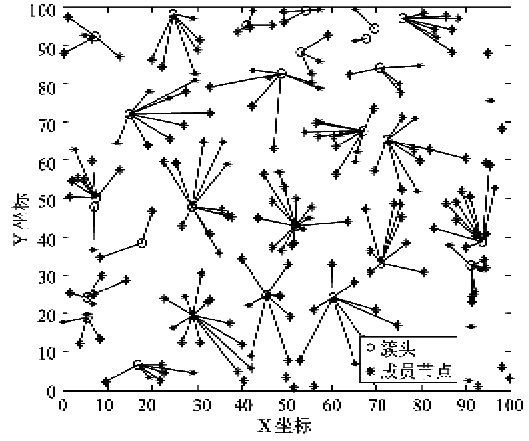


图 6 LEACH 算法下网络拓扑

3.4 网络能效分析

图 7 为 LEACH 算法、TLEACH 算法和 TCEM 算法下网络前 200 轮簇头选举中的节点有效率。这里以网络节点有效率大于 0.5 的簇头选举轮数作为网络生存时间。图中 TCEM 算法下网络的生存时间为

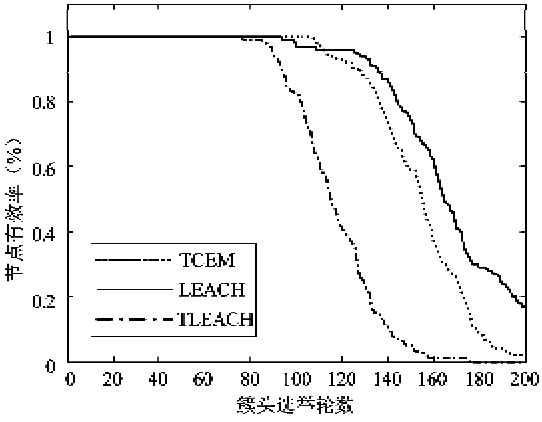


图 7 TCEM 算法、LEACH 算法和 TLEACH 算法下网络前 200 轮簇头选举内网络的节点有效率

157 轮,高于 TLEACH 算法下的 119 轮,比 LEACH 算法下的 169 轮略低。其原因是,采用的信任管理会不可避免地造成网络额外的通信能耗,导致网络寿命缩短,但 TCEM 算法采用了节点模糊分类、合理分布簇头等一系列能效改善措施,最大限度地均衡了能耗,相对于 TLEACH 算法延长了网络生存时间,并接近于 LEACH,从而提高了算法的实用性。由此可见 TCEM 算法对簇头分布问题的考虑是具有实际意义的。

4 结 论

针对密钥安全机制无法解决无线传感器网络中恶意节点成为簇头导致的层次路由安全问题,提出了一种基于 Mamdani 模糊推理的可信簇头选举算法 TCEM。该算法不仅能有效避免恶意节点成为簇头,实现可信簇头的选举,并能确保簇头的合理分布,从而均衡信任管理引起的额外能耗,提高网络的整体能效,延长网络生命周期。

参考文献

[1] Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks*, 2005, 3(3): 325-349

[2] Al-Karaki J N, Kamal A E. Routing techniques in wireless sensor networks: a survey. *IEEE Wireless Communications*, 2004, 11(6): 6-28

[3] 荆琦,唐礼勇,陈钟.无线传感器网络中的信任管理研究.软件学报,2008,19(7):1716-1730

[4] 孙利民,李建中,陈渝等.无线传感器网络.北京:清华大学出版社,2005.89-217

[5] Crosby GV, Pissinou N, Gadze J. A framework for trust-based cluster head election in wireless sensor networks. In: Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS 2006), Maryland, USA, 2006.10-22

[6] Krasniewski M, Varadharajan P, Rabeler B, et al. TIBFIT: trust index based fault tolerance for arbitrary data faults in sensor networks. In: Proceedings of the International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan, 2005. 672-681

[7] Song F, Zhao B H. Trust-based LEACH protocol for wireless sensor networks. In: Proceedings of the 2nd International Conference on Future Generation Communication and Networking, Sanya, China, 2008. 202-207

[8] Hsieh M Y, Huang Y M, Chao H C. Adaptive security design with malicious node detection in cluster-based sensor networks. *Computer Communications*, 2007, 30(11-12):2385-2400

[9] Ganeriwal S, Balzano L, Srivastava M. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks*, 2008,4(3):1-37

[10] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. In: Proceeding of the 33rd Annual Hawaii International Conference on System Sciences (HICSS), Maui, USA, 2000.3005-3014

[11] 章卫国,杨国忠.模糊控制理论与应用.第 1 版.西安:西北工业大学出版社,1999.71-87

A Mamdani fuzzy inference based trusted cluster-head election algorithm for wireless sensor networks

Feng Renjian*, Cheng Jian**, Xu Xiaofeng*, Wan Jiangwen*

(*School of Instrument Science and Optoelectronics Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100191)

(**Department of Unmanned Aerial Vehicle, Chinese People's Liberation Army Ordnance Institute of Technology, Wuhan 430075)

Abstract

A trusted cluster-head election algorithm based on Mamdani fuzzy inference (TCEM) is proposed to resolve the security issue of cluster-based routing in wireless sensor networks caused by malicious nodes selected as a cluster-head. According to nodes' behaviors, the TCEM applies the Bayes' theorem to evaluation of nodes' trust-value, and on the basis of this, performs the calculation of nodes' advantage using the Mamdani method with the combination of the concentration and the centrality so as to select the optimal nodes as trusted cluster-heads. The simulation results show that the TCEM can effectively prevent malicious nodes from being cluster-heads, and has the better performances both in proper distributing of cluster-heads and in improving the energy efficiency of the networks.

Key words: wireless sensor networks, cluster-head election, security of routing, Mamdani fuzzy inference