软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(Suppl.(1)):122−130

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于云信任模型和蚁群算法的 WSN 簇可信路由算法*

蔡绍滨[1], 潘虹杞[1], 姚念民[2], 方 伟[1]

[1](哈尔滨工程大学 计算机科学与技术学院,黑龙江 哈尔滨 150001)

[2](大连理工大学 计算机科学与技术学院,辽宁 大连 116024)

通讯作者: 蔡绍滨, E-mail: caishaobin@hrbeu.edu.cn, http://www.hrbeu.edu.cn

摘 要: 在无线传感器网络中,信息的传输需要安全的保护.在分簇管理的基础上,GTMS(group-based trust management scheme)算法利用节点的可信度来实现路由的安全.但是,它的可信度表示方法过于简单,无法反映信誉复杂性.因此,在基于区间的云相似度比较算法的基础上,以云理论为基础构建节点可信度,提出了基于云信任模型和蚁群算法的无线传感器网络簇可信路由算法.研究结果表明,在准确判定簇内节点可信度的基础上,CRPCTMAS (cluster reliability protocol based on cloud trust model and the ant scheme)算法建立了安全、有效的路由,保证了路由的高有效发包率,延长了网络的生命周期.

关键词: 无线传感器网络;安全路由;信任;蚁群算法;簇

中文引用格式: 蔡绍滨,潘虹杞,姚念民,方伟.基于云信任模型和蚁群算法的 WSN 簇可信路由算法.软件学报,2014,25(Suppl.(1)):122−130. http://www.jos.org.cn/1000-9825/14014.htm

英文引用格式: Cai SB, Pan HQ, Yao NM, Fang W. Cluster reliability routing algorithm based on cloud trust model and ant colony algorithm for WSN. Ruan Jian Xue Bao/Journal of Software, 2014,25(Suppl.(1)):122−130 (in Chinese). http://www.jos.org.cn/1000-9825/14014.htm

Cluster Reliability Routing Algorithm Based on Cloud Trust Model and Ant Colony Algorithm for WSN

CAI Shao-Bin[1], PAN Hong-Qi[1], YAO Nian-Min[2], FANG Wei[1]

[1](School of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

[2](School of Computer Science and Technology, Dalian University of Technology, Dalian 116024, China)

Corresponding author: CAI Shao-Bin, E-mail: caishaobin@hrbeu.edu.cn, http://www.hrbeu.edu.cn

Abstract: In WSN (wireless sensor network), the security of message transmission is needed. GTMS (group-based trust management scheme) guarantees the security of routing by node trust. However, its description of trust is too simple to represent the complexity of the entity. Hence, based on the comparison method of cloud similarity, this paper establishes a node trust, and proposes a new routing protocol CRPCTMAS (cluster reliability protocol based on cloud trust model and the ant scheme). The performance analysis show that, based the correct judgment of node trust, CRPCTMAS can find a security route not only to guarantee the high ratio of data packet emission but also to prolong the lifetime of the network.

Key words: wireless sensor network; security route; trust; ant colony optimization; cluster

无线传感器网络(wireless sensor network,简称 WSN)是一种没有基础设施的无线自组织网络,具有快速展开、高健壮性和抗毁性等特点.因此,它在军事,环境检测和预报,智能家居等诸多领域具有广泛的应用,已经引起了世界许多国家军界、学术界和工业界的高度重视[1].目前,传感器网络的路由算法大多采用链路层加密和认

* 基金项目: 国家自然科学基金(41176082); 教育部新世纪优秀人才支持计划(NCET-13-0753); 教育部博士点基金(20132304110031); 黑龙江省自然科学基金(42400621-1-14076); 哈尔滨市自然科学基金(2014RFQXJ012)

收稿时间: 2014-05-10; 定稿时间: 2014-08-26

证、多路径路由、身份认证、双向连接认证和认证广播等安全机制.文献[2]概述了目前无线传感器网络安全路由协议的研究状态.

在 DSR 算法的基础上,INSENS(intrusion-toleration routing in wireless sensor networks)[3]算法建立了冗余多径路由来保证路由安全,防止入侵者阻塞节点采集数据的发送.SPIN(security protocols for sensor networks)算法[4]利用轻量级的对称密钥以及简单的加/解密,实现了数据的加/解密和广播认证.SPKI(simple public key infrastructure)/SDSI(simple distributed systems infrastructure)算法[5]采用应用层安全措施来保证节点间的安全通信.

在 TRANS(trust routing for location-aware sensor networks)安全算法[6]中,节点预置其邻居节点的信任值,并在利用地理位置信息的基础上,通过将信息发给可信邻居来保证信息包沿着信任节点到达目的地.在 TRPBCH (trusted routing protocol based cluster head)算法[7]中,簇内节点计算邻居节点的可信度,并通知簇首,簇首计算每个节点可信度的均值.当可信度均值低于阈值时,节点为恶意节点.在 GTMS(group-based trust management scheme)算法[8]中,节点计算其邻居节点的可信度,并向簇首报告邻居节点可信状态为可信、不可信或不确定.根据收到的节点可信状态,簇首按照中心极限定理构造标准正态随机变量,并将其期望作为一个节点最终的可信状态.文献[9]提出了一个基于灰色马尔可夫模型的信誉评测模型的安全路由协议.文献[10]提出了一个基于分簇的无线传感器网络安全路由协议.

以上的研究表明,由于没有考虑网络节点行为的可信度,基于密钥管理的安全路由算法不能很好地抵制网络内部恶意节点的破坏行为,信誉评测的方式能够较好地识别和防范恶意节点.在信誉评测的基础上,GTMS 算法利用节点的可信度来实现路由的安全.但是,其可信度表示方法太简单,无法反映信誉复杂性.因此,本文在基于区间的云相似度比较算法的基础上,以云理论为基础构建节点可信度,提出了基于云信任模型和蚁群算法的无线传感器网络簇可信路由算法(cluster reliability algorithm based on cloud trust model and the ant colony algorithm).

1 基于云信任模型的簇可信度管理机制

1.1 云信任模型

隶属云模型把定性概念的模糊性、随机性和不确定性有机综合在一起,实现了概念的定性定量之间的转换.因此,在基于区间的云相似度比较算法[11]的基础上,我们将云理论引入到无线传感器网络安全领域中,提出了基于云理论的信任模型(cloud-based trust model,简称 CTM).

节点在时间段 Δt 内监听邻居节点的行为,并将监听到的信息保存在一个矩阵中.n 个时间段后,节点 i 对节点 j 的行为属性的监听矩阵为

$$X_{ij}=\begin{vmatrix} x_{11} & x_{12} & L & x_{1n} \\ x_{21} & x_{22} & L & x_{2n} \\ M & M & O & M \\ x_{m1} & x_{m2} & L & x_{mn} \end{vmatrix},$$

其中,行数 m 为属性的个数,列数 n 为时间段个数.

对于某个属性上的信息集合,可以根据逆向云生成器算法[12]计算出云的 3 个数字特征,构造这个属性的信任云 $C(Ex,En,He)$:

(1) 求出样本均值 $\bar{X}=\frac{1}{n}\sum_{i=1}^{n}x_i$, 一阶样本中心矩 $d=\frac{1}{n}\sum_{i=1}^{n}|x_i-\bar{X}|$, 样本方差 $s^2=\frac{1}{n}\sum_{i=1}^{n}(x-\bar{X})^2$;

(2) $Ex=\bar{X}$;

(3) $E_n=\sqrt{\frac{\pi}{2}}\times d$;

(4) $He=\sqrt{s^2-En^2}$.

在构造信任基准云的基础上,可以利用云相似度比较算法来计算信任云与基准云的相似度[11],并定义为该信任云的可信度,则节点 i 对节点 j 的直接可信度为

$$t_{i,j}^{direct}=similar_{ij} \tag{1}$$

如果节点 k 和 m 和节点 i 有直接交互行为,k 与 j 有直接交互行为,而 m 与 j 无交互历史,m 的邻居节点 n 和 j 有交互历史,因此,m 先从 n 处获得 j 的可信度,然后再将这一可信度传递给节点 i.这样,节点 i 获得的节点 j 的间接可信度为

$$t_{i,j}^{indirect}=t_{i,k}^{direct}\times t_{k,j}^{direct}+t_{i,m}^{direct}\times(t_{m,n}^{direct}\times t_{n,j}^{direct}) \tag{2}$$

将直接信任与间接信任加权相加即可得到总体可信度:

$$t_{i,j}=\omega_1\times t_{i,j}^{direct}+\omega_2\times t_{i,j}^{indirect} \tag{3}$$

其中, $0<\omega_1,\omega_2<1,\omega_1+\omega_2=1$.

为了体现信任的具有慢升快降的特点,在更新函数 $t_{new}=\omega t_1+(1-\omega)t_2, 0<\omega<1$ [13]的基础上,我们将上升幅度变成原来的 $\frac{1}{n}$, 将下降幅度变成原来的 m 倍,得到:

$$t_{new}=\begin{cases}[(n+\omega-1)t_1+(1-\omega)t_2]/n, & t_1\geqslant t_2\\ (1-m+m\omega)t_1+m(1-\omega)t_2, & t_1<t_2\end{cases} \tag{4}$$

其中,t_1 为之前的可信度,t_2 为新计算得到可信度,ω 为时间衰减因子.

2 基于云信任模型和蚁群算法的簇可信路由算法

2.1 基于云信任模型的簇可信算法

在基于云信任模型的簇可信算法中,首先,要定义簇首节点,簇首节点不但负责簇内节点的可信度的综合评判,而且负责计算其他簇的可信度;其次,定义一个候选簇首节点,候选簇首节点负责计算簇首节点的可信度,当簇首节点失效或被判为恶意节点后,取代原簇首;再次,定义属于两个或两个以上簇的公共节点为网关节点;最后,定义簇内其他节点均为普通节点.

由于信任具有主观性,因此不同节点对同一个节点的信任状态判定可能不同,有时甚至完全相反.因此,本文利用簇来管理可信度.也就是说,一个节点是否被隔离出网络不是由某个节点决定的,而是簇首利用簇内所有节点对其可信的判断来决定该节点的可信状态.

利用基于云理论的信任模型,所有节点计算其邻居节点的可信度.簇首节点 O 获得簇内所有节点的可信度.这样,对于簇内的节点 A,其簇首 O 对 A 有一个可信度向量,该向量内的元素为 A 的邻居节点计算所得的 A 的可信度, $X_{OA}=\{T_{BA},T_{CA},...,T_{NA}\}$.

簇首节点 O 在获得 A 的可信向量后构造信任云,并计算与信任基云的相似度,该相似度即为节点 A 的全局可信度,决定其在簇内的可信状态.簇首节点的全局可信度由其邻居节点计算,并将其报告候选簇首,由候选簇首判断簇首的可信状态.当簇内节点出现全局可信度低于阈值时按以下方式处理:

(1) 普通节点:簇首通知簇内节点,将其隔离出网络.

(2) 网关节点:簇首通知簇内节点,隔离出本簇,但不影响其在其他簇中的可信度.

(3) 候选簇首节点:簇首通知簇内节点,隔离出本簇,选出新的候选簇首.

(4) 簇首节点:候选簇首通知簇内节点簇首失效,并取代原簇首.

(5) 若候选簇首和簇首互相信任,则采取投票机制,由二者共同的邻居节点投票决定.

当一个簇 m 要获取簇 n 的可信度时,簇 m 从网关节点的所有邻居节点处获取其所在簇 n 的可信度值,然后如前文所述过程一样构造信任云,计算所得可信度值.若簇 n 的可信度低于阈值,则簇首 m 告知其网关节点,令其不再与簇 n 中的节点进行通信.

2.2 基于云理论和蚁群算法的簇可信路由算法

在基于云理论的簇可信度管理机制的基础上,我们提出基于云信任模型和蚁群算法的簇可信路由算法.

在蚁群算法中,假设蚂蚁移动过一步需要一个单位时间,那么如果从时刻 t 开始移动,在 $t+p$ 时刻所有的蚂蚁都结束移动,完成一个循环.路径(i,j)在 $t+p$ 时刻的信息素的浓度按式(5)更新:

$$\tau_{i,j}(t+P)=(1-\rho)\tau_{i,j}(t)+\sum_{k=1}^{n}\Delta\tau_{i,j}^{k}(t,t+p) \tag{5}$$

在 CRPCTMAS 算法中,当向汇聚节点发送数据时,以簇为单位进行路由选择.如果蚂蚁 k 在簇首节点处,则按照式(5)计算转移概率:

$$P_{i,j}^{k}(t)=\begin{cases}\dfrac{[\tau_{i,j}(t)]^{\alpha}[T_{m,n}]^{\beta}}{\sum\limits_{s\in allowed_k}[\tau_{i,s}(t)]^{\alpha}\sum\limits_{l\in allowed\_gp_k}[T_{m,l}]^{\beta}}, & j\in allowed_k, n\in allowed\_gp_k\\ 0, & \text{otherwise}\end{cases} \tag{6}$$

其中,β 为簇可信度权重因子,$T_{m,n}$ 为簇 n 在簇 m 中的可信度(节点 i 在簇 m 中,节点 j 可以通往簇 n), $allowed\_gp_k$ 代表簇 m 可选的下一跳簇.

若蚂蚁 k 在簇内其他节点处,则按照式(6)计算转移概率:

$$P_{i,j}^{k}(t)=\begin{cases}\dfrac{[\tau_{i,j}(t)]^{\alpha}(\eta_j)^{\gamma}}{\sum\limits_{s\in allowed\_gp_k}[\tau_{i,s}(t)]^{\alpha}[\eta_s]^{\gamma}}, & j\in allowed\_gp_k\\ 0, & \text{otherwise}\end{cases} \tag{7}$$

其中,γ 为剩余能量权重因子,η_j 为节点 j 的剩余能量, $allowed\_gp_k$ 为簇首计算确定的下一跳簇.

CRPCTMAS 算法不但在簇级以簇可信度作为标准,而且在节点级以剩余能量作为标准.因此,CRPCTMAS 算法在提高路由安全性的同时平衡能量的消耗.

CRPCTMAS 算法伪代码如下:

```
Begin
(初始化,假定网络中有 m 只蚂蚁,n 个节点,给出算法中其他参数的值,NC=0,NC 是循环计数器)
While (NC<MAX) {
For (k=0, k<m, k++)
初始化蚂蚁 Ants[k]的起始位置
If (蚂蚁在簇首节点){
While (下一跳簇集合非空) {
依据式(5)和式(6)计算下一跳簇的转移概率,并将该簇从集合中除去,若下一跳簇集合为空,则蚂蚁跳出该循环.
}
选择转移概率最高的簇,并更新路径上的信息素.
End while
Else
初始化下一跳节点集合,保证下一跳节点可达下一跳簇
While (下一跳节点集合非空) {
依据公式(7)计算下一跳节点的转移概率,并将该节点从集合中除去,若下一跳节点集合为空,则蚂蚁跳出该循环.
}
选择转移概率最高的节点,并按照式(5)更新路径上的信息素.
End while
```

End if
End for
NC=*NC*+1;
}
End

3 性能分析

在无线传输能耗模型[14]的基础上,定义节点接收和传送能耗为 $E_{elec}=50$ nJ/bit, 传送放大器工作能耗为 $\varepsilon_{amp}=100$ pJ/bit/m^2. 即,数据大小和传输距离决定发送数据能耗,数据大小接收数据能耗.当节点之间距离为 d, 数据大小为 k bit 时,数据发送能耗为 $E_{elec}\times k+\varepsilon_{amp}\times k\times d^2$, 数据接受能耗为 $E_{elec}\times k$.

假设所有的传感器节点具有相同的能量和通信半径,并且每次广播时都已经实现了数据融合,即不考虑数据融合所消耗的时间和能量,且节点接收和发送的数据大小固定为 2 000 bit.此外,实验中其他参数的设置见表 1.

在仿真分析 CRPCTMAS 算法之前,本文首先信息素浓度α,簇可信度 β 和节点剩余能量 γ 在转移概率中对最佳路径长度和收敛速度有重要影响.为了使路由安全性更高,能量消耗更均衡,本文令簇可信度和节点剩余能量同等重要,且都高于信息素浓度要,即α=1,β=γ,且都大于 1.

图 1 描述了 β 和 γ 在取值不同值时算法的收敛速度与最佳路径长度之间的关系.当$1\leqslant\beta,\gamma\leqslant3$时,随着 β 和 γ 的增大,簇可信度与节点剩余能量的重要性增强,随着循环次数的增加逐渐发挥作用,最佳路径长度近似且收敛速度逐渐变快.当$4\leqslant\beta,\gamma\leqslant5$时,由于其与$\alpha$的差值较大,使得信息素浓度比重较小,路由建立更侧重于簇可信度,最佳路径较长,增加网络总体能耗.因此,本文在实验中将 β 和 γ 设置为 3,在保证较快的收敛速度的同时还保证路径长度较短,以节约能量.

Table 1 Simulation parameters

表 1 仿真实验参量

参数名称	取值
监测区域范围	(0,0)~(100,100)
汇聚节点位置	(0,100)
节点总数 N	200 个
初始化能量 E	2.0J
通信半径 r	10 m
初始信息素	10
挥发率	0.75
Q	100
迭代次数 m	200 次

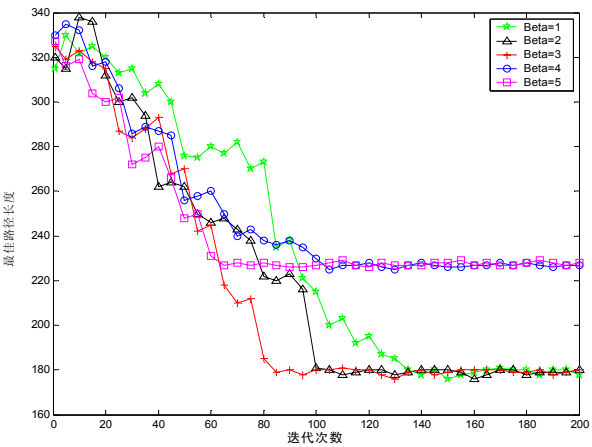


Fig.1 Influence of weighted factor

图 1 权重因子的影响

4 CRPCTMAS 算法仿真

仿真实验采用 Berkeley 实验室采集的数据.即,在一个簇内,对其中一个普通节点加入噪声模拟为恶意节点,通过 100 轮的实验来比较 CRPCTMAS 算法、TRPBCH 算法和 GTMS 算法的性能.在 GTMS 算法中,由于簇内节点交付于簇首的是由 0,1 和 2 表示的信任状态而非准确的数值,使得簇首对数据的处理失真较大,判断精度不高,仅约为 62%.由于只是对可信度求均值,忽略了可信度的跳跃性和不均匀性,在一个恶意节点可信值波动很大,但均值维持较高的情况下,该机制无法准确判断.与 GTMS 算法相比,TRPBCH 算法判断精度有所提高,约为

83%.CRPCTMAS 算法既考虑到了可信度的平均水平又兼顾了波动情况,使得该算法具有极高的检测精确度.其精度接近 100%.

图 2 描述了 CRPCTMAS 算法与 BLEACHAR(based on leach and ant routing)[15]的最佳路径查找的收敛速度.两者都是利用蚁群算法来寻找簇头到汇聚节点的最优路径.但是,由于 CRPCTMAS 算法引入了簇可信度因子,在其最佳路径的寻找过程中,仅仅要选择可信度高的簇,所以,与 BLEACHAR 算法相比,CRPCTMAS 算法的可选路径较少.因此,CRPCTMAS 算法的收敛速度较快.但是,同时也导致 CRPCTMAS 算法找到的并非最短路径,路径长度大于 BLEACHAR 算法的路径长度.

图 3 描述两种算法在具有恶意节点情况下的有效发包率.当恶意节点在第 3 个时间段上开始出现以后,BLEACHAR 算法只是靠信息素浓度来进行路由选择,没有对恶意节点采取防护措施,最佳路径没有变化.因此,当恶意节点对数据进行破坏时,有效发包率降低.在恶意节点出现以后,CRPCTMAS 算法能够在一段时间后发现恶意节点,并根据簇可信度重新选择最佳路径,保证网络有较高的有效发包率,杜绝恶意节点的破坏.

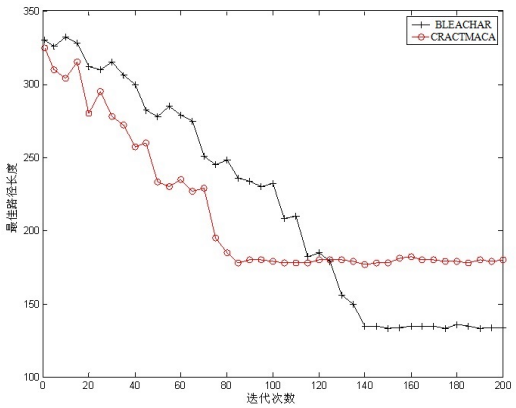


Fig.2 Comparison of algorithm convergence

图 2 算法收敛性的比较

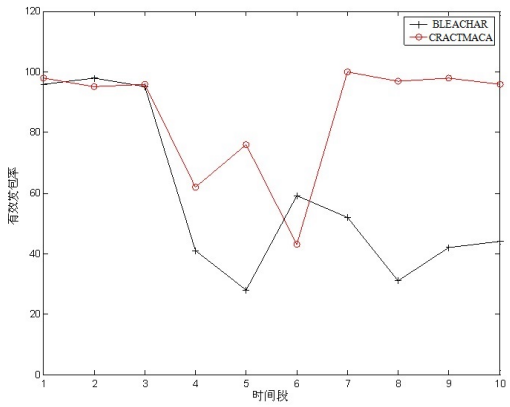


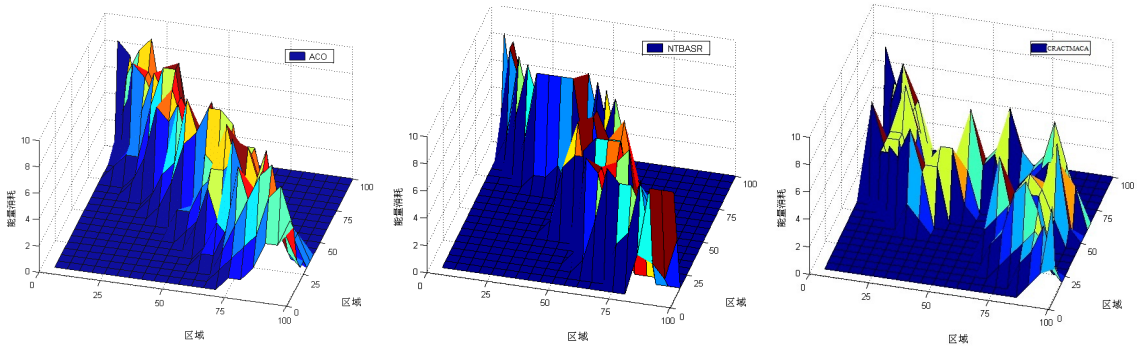
Fig.3 Comparison of effective packets sending rate of algorithm

图 3 算法有效发包率的比较

图 4 描述了网络中存在恶意节点时 CRPCTMAS 算法与基于节点可信度的蚁群安全路由算法 NTBASR (nodes' trust based ant secure routing)[16]以及普通的蚁群(优化)(ant colony optimization,简称 ACO)算法迭代 100 次后能量消耗分布.ACO 算法只依靠信息素浓度计算转移概率,无法识别恶意节点,最优路径上存在着恶意节点.恶意节点不断要求其邻居节点重传数据,造成其他节点能量消耗较大.NTBASR 算法在转移概率中加入节点可信度,最优路径将绕过恶意节点保证路由的安全性.以节点为单位进行可信度的计算和路由选择,各个节点的能耗保持在一个范围内,差异不大.由于要收集和处理簇内各类节点的可信度,并向簇内广播下一跳簇的簇号,CRPCTMAS 算法的簇首节点能量消耗相对较高,而簇内其他节点任务相对简单,能量消耗也相对较低.

图 5 描述了 3 种算法都迭代 100 次时,计算的平均能耗.由于路径上存在恶意节点,ACO 算法的平均能耗较高.由于簇首与簇内节点的频繁交互,CRPCTMAS 算法的能耗略高于 NTBASR 算法.

图 6 和表 2 分别描述了 3 种算法迭代 100 次后,死亡节点的数量以及分布情况.由于 ACO 算法的最优路径中存在恶意节点,节点的能量消耗较大.因此,随着网络中传输数据增多,死亡节点在恶意节点周围出现的机率越大.NTBASR 算法选择的最优路径能够绕过恶意节点,保证了网络没有被恶意节点破坏.但是,由于根据节点独自计算可信度来进行路由选择,有时无法正确判断恶意节点,造成在恶意节点没有被判断出的路径上节点死亡机率大.CRPCTMAS 算法以簇为单位进行可信度的计算和路由选择,簇首相对能耗较大.由于簇内其他节点利用剩余能量进行选择路由选择,所以簇内能耗相对均衡,只有部分簇首节点死亡,死亡节点数量少于其他算法.



(a) ACO 算法 (b) NTBASR 算法 (c) CRACTMACA 算法

Fig.4 Network energy distribution in three kinds of algorithm

图 4 3 种算法的网络能耗分布

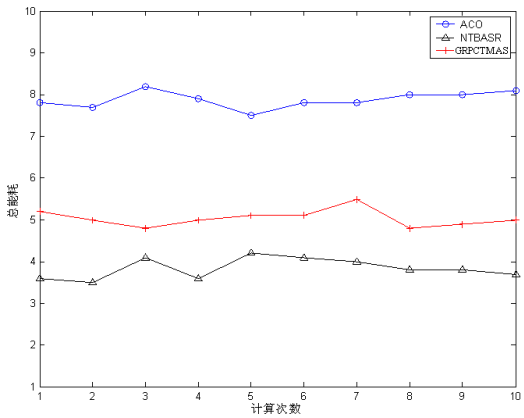
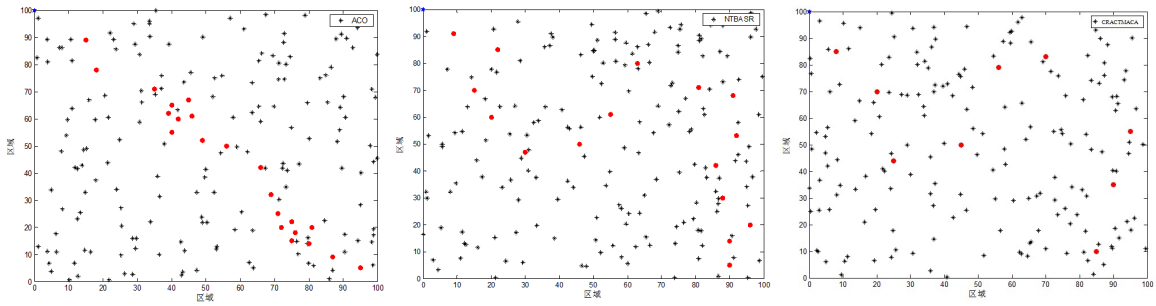


Fig.5 Three algorithms total network energy consumption comparison chart

图 5 3 种算法的总网络能耗比较图



(a) ACO 算法 (b) NTBASR 算法 (c) CRACTMACA 算法

Fig.6 Death nodes distribution

图 6 死亡节点的分布

Table 2 Three death number of nodes in three algorithms

表 2 3 种算法的死亡节点数

算法名称	死亡节点数
ACO	22
NTBASR	15
CRPCTMAS	9

5 结 论

在基于云理论的簇可信度的研究基础上,本文将基于云理论的簇可信度作为蚁群算法转移概率的计算因子,提出了 CRPCTMAS 算法.CRPCTMAS 算法将在簇间以簇可信度作为路由选择的限制因素,在簇内以剩余能量作为限制因素来保证网络安全性和平衡能量的消耗.研究表明,与已有的基于蚁群算法的相比,CRPCTMAS 算法能够准确地判定簇内节点的可信度,建立了安全有效的路由,保证了路由的高有效发包率,延长了网络的生命周期.

References:

[1] Sun LM, Li JZ. Wireless Sensor Network. Beijing: Tsinghua University Press, 2005. 135−155 (in Chinese).

[2] Li T, Feng Y. Survey on secure routing research in wireless sensor networks. Application Research of Computers, 2012,29(12): 4412−4419 (in Chinese with English abstract).

[3] Deng J, Han R, Mishra S. INSENS: Intrusion-Tolerant routing in wireless sensor networks. Computer Communications, 2006, 29(2):216−230.

[4] Perrig A, Szewczyk R, Tygar J, Wen V, Culler DE. SPIN: Security protocols for sensor networks. Wireless Networks Journal, 2002,8(5):521−534.

[5] Traynor P, Choi H, Cao G, Zhu S, Porta T. Establishing pair-wise keys in distributed sensor networks. In: Proc. of the 10th ACM Conf. on Computer and Communication Security. 2003. 22−46.

[6] Tanaehaiwiwat S, Dave P, Bhindwale R, Helmy A. Location-Centric isolation of misbehavior and trust routing in energy-constrained sensor networks. In: Proc. of the IEEE Workshop on Energy Efficient Wireless Communications and Networks in Conjunction with IEEE IPCCC. 2004. 57−75.

[7] Zhou Q, Zhou XD. Trusted routing protocol based on cluster head for wireless sensor network. Transducer and Microsystem Technologies, 2008,27(10):42−47 (in Chinese with English abstract).

[8] Shaikh R, Jameel H, d'Auriol BJ, Lee H, Lee S, Song Y. Group-Based trust management scheme for clustered wireless sensor networks. IEEE Trans. on Parallel and Distributed Systems, 2009,20(11):1698−1712.

[9] Zeng MM, Jiang H, Wang X, Liu WQ. Reputation evaluating model and security routing protocol of wireless sensor networks based on grey Markov model. Application Research of Computers, 2013,30(12):3758−3766 (in Chinese with English abstract).

[10] Hou YY, Liang JZ. Cluster-Based wireless sensor networks secure routing protocols. Electronic Component and Device Applications, 2012,14(10):30−32 (in Chinese with English abstract).

[11] Cai SB, Fang W, Zhao J. Research of interval-based cloud similarity comparison algorithm. Journal of Chinese Computer Systems, 2011,32(12):2457−2460 (in Chinese with English abstract).

[12] Pathan A, Lee H, Hong C. Security in wireless sensor networks: Issues and challenges. In: Advanced Communication Technology, Proc. of the 8th ICACT 2006. 2006. 149−158.

[13] Li DY, Liu CY, Gan WY. A new cognitive model: Cloud model. Int'l Journal of Intelligent Systems, 2009,3(24):357−375.

[14] Heinzelman W, Chandrakasan A, Balakrishnan H. An application specific protocol architecture for wireless microsensor networks. IEEE Trans. on Wireless Communications, 2002,1(4):660−670.

[15] Hang HC, Guo AH, Shu WJ. Performance analysis of WSN routing scheme based on LEACH and ant algorithm. Chinese Journal of Sensors and Actuators, 2008,21(10):1375−1380 (in Chinese with English abstract).

[16] Wang C, Jia XY, Lin Q. Trust based secure routing algorithm for wireless sensor network. Journal of Communications, 2008, 29(11):106−115 (in Chinese with English abstract).

附中文参考文献:

[1] 孙利民,李建中.无线传感器网络.北京:清华大学出版社,2005.135−155.

[2] 李挺,冯勇.无线传感器网络安全路由研究综述.计算机应用研究,2012,29(12):4412−4419.

[7] 周权,周小东.基于簇首节点的可信传感器网络路由.传感器与微系统,2008,27(10):42−47.

[9] 曾梅梅,蒋华,王鑫,刘伟强.一种基于灰色马尔可夫模型的信誉评测模型及其安全路由协议.计算机应用研究,2013,30(12):3758−3766.

[10] 侯媛元,梁京章.基于分簇的无线传感器网络安全路由协议研究.电子元器件应用,2012,14(10):30−32.

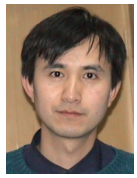
[11] 蔡绍滨,方伟,赵靖,赵蕴龙,高振国.基于区间的云相似度比较算法的研究.小型微型计算机系统,2011,32(12):2457−2460.

[15] 杭海存,郭爱煌,舒文杰.基于 LEACH 与蚁群算法的 WSN 路由机制及性能分析.传感器技术学报,2008,21(10):1375−1380.

[16] 王潮,贾翔宇,林强.基于节点可信度的无线传感器网络安全路由算法.通信学报,2008,29(11):106−115.

蔡绍滨(1973－),男,辽宁辽中人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为无线传感器网络,水声传感器网络.

E-mail: caishaobin@hrbeu.edu.cn

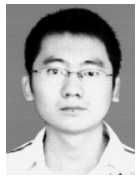


姚念民(1974－),男,博士,教授,博士生导师,CCF 会员,主要研究领域为无线传感器网络,网络存储.

E-mail: yaonianmin@hrbeu.edu.cn

潘虹杞(1990－),女,硕士生,主要研究领域为无线传感器网络.

E-mail: panhongqi@hrbeu.edu.cn



方伟(1986－),男,硕士,主要研究领域为无线传感器网络.

E-mail: fangwei@hrbeu.edu.cn