模型还能用于区分网络受到何种攻击方式[4]; Awad A 等利用虚拟坐标提高传感器网络的路由性能, 从而隐藏恶意节点的攻击目标[5]; Naser A 等在研究过程中以两跳邻居信息为基础提出了一种新的算法来对选择性的转发攻击来进行检测[6]. 段正飞等针对虫洞攻击对节点定位过程的影响, 提出了一种距离矢量跳安全定位算法. 通过改进冲突集建立方法,选出最合适的信标节点广播睡眠信息, 提高了虫洞检测成功率和定位精度[7]. 付翔燕等建立了以最优转发为基础的随机路由算法, 利用可信任的邻居节点进行监听, 可对恶意节点做到有效的防御和处理[8]. 齐全等提出一种基于信誉机制的认知 ad hoc 网络分簇协作感知方法, 将权值应用为节点信誉值的基础上实现了数据之间的融合, 然后对融合值和实际值进行了比较分析, 判断数据节点的可疑性, 并利用惩罚系数来降低数据信誉值, 筛选恶意节点[9]. 与有线网络相比较, 无线传感器网络在开放环境下, 能量、带宽、计算能力、存储空间受到一定限制, 这就决定了传统的入侵检测技术难以直接应用到无线传感器网络中. 因此, 针对无线传感器网络的特点, 金鑫等提出了针对无线传感器网络的入侵检测模型, 它由邻居节点监听、历史行为记录、数据采集融合、拓扑和路由追踪等搭建[10]. 为提升无线网络传感器的安全性和使用时间, 本文在对前人相关研究进行分析和借鉴的基础上, 引入信任以及信誉系统, 针对的节点类型主要有两种, 分别是转发节点和传感节点, 提出了一种以随机并行为基础的簇头选举算法, 该算法以安全数据的融合为基础, 可以均匀地选举节点, 对恶意节点进行识别清除, 加密通信数据, 从而有效地实现无线网络通信的安全.

1 算法设计

1.1 簇头节点的可信选举

假定全网时间同步并且各节点有独一无二的身份标志. 网络的簇结构如图 1 所示不考虑具体的密钥分布策略, 但假设各节点拥有 3 种密钥: 公钥、密钥以及私钥. 公钥被网络中的全部节点拥有, 主要作用为收获基站广播. 密钥主要作用为簇结构内部的组播或广播, 每一个簇结构拥有其内部特有的密钥. 因此, 可以通过簇内密钥实现基站和其它簇之间的通讯, 还可以使得邻居节点的簇头内部信息交换相互不影响. 私钥一般是被某一个节点存放, 以便于节点间的数据通讯.

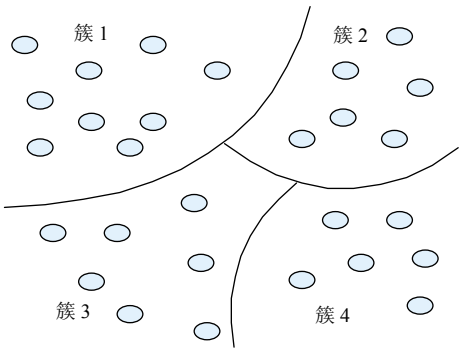


图 1 无线传感网层次路由的拓扑结构

在路由层级中, 簇头节点扮演着核心的角色, 如数据采集融合、信息转送、密钥转存等. 在相对繁杂的网络背景下, 层级路由急需改善的核心问题是如何采取适当的方式来保证簇头的可信任度. 在对簇头节点进行可信选举的过程中不应该对太多的因素进行考量, 而是应该把其当作一个最优化的选举方式, 仅须对可信度、距离和密度之间的最优化进行考量分析. 节点密集度是指在某节点附近的邻居节点密集程度, 可以直接表示为邻居节点的数量; 距离 D 指的是簇头节点和成员节点间相隔的距离. 对距离和密集程度进行设置的主要目的是为了能够以节点的信任评估为基础来实现路由主干节点选择的均匀性. 如果密集度越高, 那么簇头间数据信息的融合率就会越大, 如果距离越近, 那么节点间的通讯代价就会越小[11].

若节点 p 在等候选择的信任簇节点集 s 之中, 那么 $THSp$ 命令为表示节点 p 的簇头选举函数. 如果对概率形式的信任值进行利用, 那么对簇头选举进行无约束优化的问题表达式就如式 (1) 所示:

$$\mathrm{Max}\left(THS_p\right)=\omega*\alpha*OT+\beta*C_P-\gamma*D \tag{1}$$

式中, OT 表示的是普通成员节点对候选的可信簇头节点 p 表现出的总体信任值, α、β、γ 分别代表的是节点处的信任值、密集度以及距离的权重, 且存在 $\alpha+\beta+\gamma=1$ 的现象, 表示信任值的调整系数. 如果使用理论基础上的信任值, 那么基本表达式如式 (2) 所示:

$$\mathrm{Max}\left(THS_p\right)=\varpi*\alpha*(m(T))+\lambda*M(T,-T)+\beta*C_P-\gamma*D \tag{2}$$

其中, $m(T)$ 指普通成员对可信节点 p 总体信任值的信任分量, $M(T,-T)$ 指不确定分量.

由式 (2) 可得出簇头选举函数具有这种特性: 随着可信值和密集度的提高, 函数值增大; 随着距离的增加,

函数值减小. 此可以表为一个组合优化问题, 若 p 要成为可信簇头, 则 p*必须为簇头选举函数的一个解, 即:

$$p^* = f(\alpha,\beta,\gamma) \tag{3}$$

可得出式 (3) 的解并不是唯一存在, 是 3 个参数 α、β、γ 的不同函数; 因此, 须依据实际情境, 拟定 3 个参数的值, 最后对其进行迭代优化. 通过分析节点发送和接受的消息使每个节点的行为得到监督, 从而自动检测识别恶意节点并清除, 实现对无线网络的保护.

1.2 算法优化

在传统的层次路由之中, 一般会对全网节点的安全可信性进行肯定假设. 但是在实际操作和工作环境之中, 层次路由经常会受到威胁. 威胁的来源和种类主要分为以下两个方面: (1) 恶意节点有时会充当簇头节点对网络流量产生一定的误导影响, 从而对网络的安全产生一定的威胁; (2) 恶意节点有时会加入到正常的簇结构中, 通过发送某些错误信息而对监测结果产生相应的影响. 传统 HRBNT 算法主要解决单一网络威胁, 忽略了信任路由自身功能漏洞, 并没有对信任整体进行充分考虑, 如簇结构不稳定导致恶意节点不能及时排除、关键节点防御能力不足等问题[12], 为了实现上述问题的有效解决, 确保簇结构工作过程中的安全可靠, 本文以簇头可信选举和节点信任值为基础, 对无线传感器网络层次路由协议 HRBNT 进行优化. 改进算法基于节点行为分析, 综合信任度、密集度等参数选举簇头, 根据邻居节点建立高效稳定的簇结构, 与原算法在预防恶意节点方面更加优秀, 保证网络高安全性. 算法优化和建立过程主要为:

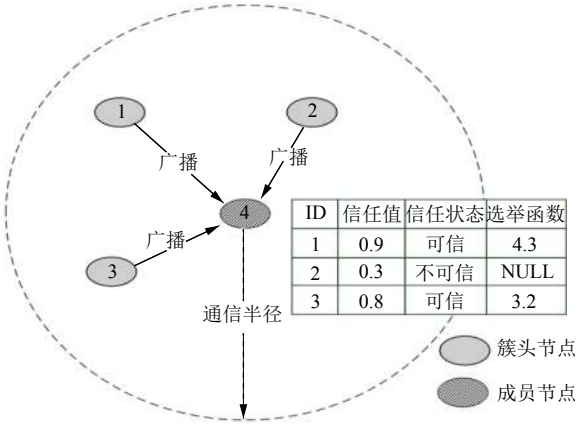
① HRBNT 之运行过程呈周期性, 其可分为数次循环. 如簇头的能量小于一定阈值或该轮运行操作即将结束时, 当前簇头发布重新选择信息, 进入后面的循环运行操作, 并选举新的簇头.

② 每一次运行过程中, 各个节点会依据本身的运行状态考虑是否成为候选簇头: 每一个节点会生成一个[0, 1]间的随机数, 假设阈值 $T(n)$ 大于随机数, 那么此节点可选作候选簇头, 然后邻居节点会收到它选作候选节点的广播. 在每一次循环过程中, 若节点曾经被选取为簇头, 则需要设置 $T(n)$ 为 0, 如此当选过簇头的节点就不会再一次成为簇头, 从而实现提高其他节点当选概率的目标; 在当选过簇头的节点个数逐渐增多时, 其他节点当选为簇头的阈值 $T(n)$ 也会增长, 节点生成比 $T(n)$ 小的随机数的概率随之提高, 因此其他节点当选的概率就会增大. $T(n)$ 的基本计算式 (4) 如下:

$$T(n) = \begin{cases} \dfrac{P}{1-p\left[r \bmod \left(\dfrac{1}{p}\right)\right]} \dfrac{er}{ei} \\ 0 \end{cases} \tag{4}$$

其中, P 指簇头在全部节点中所占的比值, r 指循环次数, G 指还没当选过簇头的节点的集合, er 代表节点当前能量, ei 代表节点初始化能量.

③ 若节点生成的随机数大于 $T(n)$ 或者其已被选作簇头, 那么可作为成员节点, 等候接收候选簇头的广播讯息. 如果此节点接收到了若干候选簇头节点的广播讯息, 那么就查找本地相关的纪录, 对拥有较低信任值的节点进行排除, 收集信任值较高的节点. 成员节点在选择加入某簇结构之后会发送相应的请求包, 告知该候选簇头. 候选簇头的选举过程如图 2 所示, 其中的 1、2 和 3 号节点为候选簇头节点, 4 号节点为成员节点, 虚线表示成员节点的通信半径. 4 号节点排除信任值较低的 2 号节点, 计算 1 号节点和 3 号节点的簇头选举函数, 并向选举值最大的 1 号节点发送请求包, 请求加入该簇.

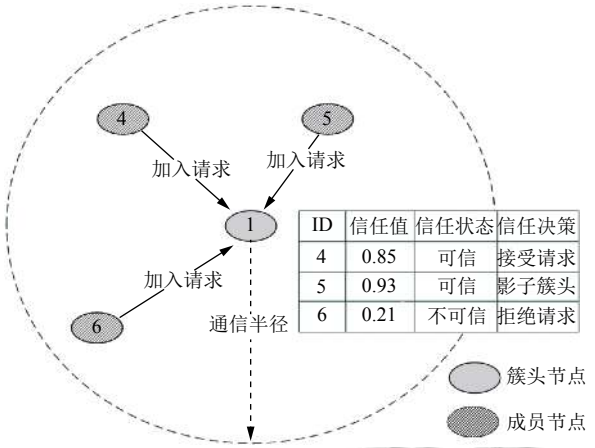


ID	信任值	信任状态	选举函数
1	0.9	可信	4.3
2	0.3	不可信	NULL
3	0.8	可信	3.2

图 2 实际网络联机情形

④ 候选簇头发送广播消息后, 等候接收其他节点的请求包. 在簇头接收到来源于全部节点发出的加入申请之后, 它就会对本地的信任纪录加以运用, 对具有恶意节点的请求进行排除, 从而确保簇的全部成员是安全可信的. 同时, 经过等待接收簇头的考察, 仅行为良好的节点才能和簇头节点连接, 预防恶意节点频繁的加入簇导致过多消耗簇头能量. 簇结构的形成过程如图 3 所示, 其中 4、5 和 6 号节点为成员节点, 都向

1 号候选簇头发送请求包, 虚线圆表示簇头节点的通信半径. 由于 6 号节点信任值较低, 所以只接受 4 和 5 号节点的请求, 且信任值最大的 5 号为影子簇头节点[13].



ID	信任值	信任状态	信任决策
4	0.85	可信	接受请求
5	0.93	可信	影子簇头
6	0.21	不可信	拒绝请求

图 3 簇结构的形成过程

⑤ 簇头首先利用 TDMA 时分复用给其余节点提供方案, 通过广播把方案信息转发给簇结构中的全部节点, 以告诉节点什么时隙可以发送数据, 杜绝节点间互相共谋或者互相影响. 簇组员收到 TDMA 信息时, 立刻为对应的时隙转发消息. 全部簇节点的信息传送完成之后, 数据信息会被融合转化为其它信号, 再次发给其它簇头和基站. 节点间的数据通信可选用最短路径、泛洪广播和列分层级等不同协议, 实现形式须依据现实情况、网络功能和规格等确定, 在此不做深入讨论[14,15].

1.3 阈值的确定

假设网络中簇头节点的数目是特定的, 所有节点的初始能量相同. 由于簇头节点比成员节点耗费的能量更多, 为了避免某些簇头节点比其它成员节点先耗尽能量, 造成网络生命周期的缩短, 需要每个节点轮流充当簇头节点以平均分配能量负载.

假设某个节点 i 在第 r+1 轮循环中自主决定它以 $T(n)$ 的概率当选为簇头节点. 阈值 $T(n)$ 的确定应该使得当前轮数期望的簇头节点数目为 k. 因此, 如果整个网络中共有 N 个节点, 则有:

$$E[CH]=\sum_{i=1}^{N}T(n)*1=k \tag{5}$$

为确保全部节点在相同的时间段内成为簇头的几率同等, 则需要每一个节点平均在N/k轮中作为簇头节点一次. 用指示函数 $C_i(t)$ 表示节点 i 在最近的 $r*\mathrm{mod}(N/k)$轮是否成为簇头节点, 如果节点 i 已经当选过一次簇头节点或者一次以上, 则$C_i(t)$=0, 否则 $C_i(t)$=1. 于是每个节点在 r+1 轮应当以 $T(n)$ 的概率当选为簇头节点, 则:

$$1*T(n)*\left[N-k*r*\bmod\left(\frac{N}{k}\right)\right]+0*k*r*\bmod\left(\frac{N}{k}\right)=k \tag{6}$$

因此, 只有当节点 i 在最近$r*\mathrm{mod}(N/k)$轮中没有当选过簇头节点, 它才有可能在 r+1 轮中当选为簇头节点. $C_i(t)$为 1 表示节点 i 在 t 时刻有资格当选为簇头节点, $C_i(t)$为 0 则表示没有资格. 那么$\sum_{i=1}^{N}C_i(r+1)$表示在 r+1 轮有资格当选为簇头的所有节点数目, 则:

$$E\left[\sum_{i=1}^{N}C_i(r+1)\right]=N-k*\left(r*\bmod\frac{N}{k}\right) \tag{7}$$

由此可保证通过每个N/k环循环后, 全部节点的能量近似相等. 得出每一轮循环期望的簇头数目是:

$$\begin{aligned}E[CH]&=\sum_{i=1}^{N}T(n)*1\\&=\left(N-k*\left(r*\bmod\frac{N}{k}\right)\right)*\frac{k}{N-k*\left(r*\bmod\frac{N}{k}\right)}=k\end{aligned} \tag{8}$$

式中, 全部节点都自主决定其以 $T(n)$ 的概率当选为簇头节点, 但是某些节点由于本身能量较低, 作为簇头节点或会造成其过早的死亡. 为延长网络生命周期, 可根据节点能量情况, 对 $T(n)$ 的算法进行调整:

$$T(n)=\begin{cases}\dfrac{k}{N-k\left[r\bmod\left(\frac{N}{k}\right)\right]}\dfrac{er}{ei}\\0\end{cases}=\begin{cases}\dfrac{k}{N-k\left[r\bmod\left(\frac{1}{p}\right)\right]}\dfrac{er}{ei}\\0\end{cases} \tag{9}$$

其中, er 为节点当前能量, ei 为节点初始化能量.

但是, 对于经过长时间运行的网络来说, 其全部节点的现有能量较之前都会有所降低, 阈值 $T(n)$ 也自然会变小, 而这些节点成为簇头的基本概率也会有所降低, 从而使每一轮循环被选为簇头的节点个数有所减少, 最终甚至会影响网络能量消耗的均衡性, 缩短网络的生命周期. 因此, 进一步改进后的 $T(n)$ 的计算方法如下:

$$T(n)=\frac{P}{1-P\left[r\bmod\left(\frac{1}{P}\right)\right]}\left[\frac{er}{ei}+\left(r_s\mathrm{div}\frac{1}{P}\right)\left(1-\frac{er}{ei}\right)\right] \tag{10}$$

其中, *rs* 指节点连续没有被选为簇头的选举次数. 如果节点被选为簇头, 则将 *rs* 重置为 0. 上式对节点能量、阈值在选择簇头时的影响方面进行了综合考量, 改进算法更具公平性.

2 算法实验与结果分析

使用 Matlab 进行仿真实验, 我们把节点信任值的计算参数设为 $\alpha=\beta=\gamma=1/3$. 实验范围是参照节点 *i* 和 *i* 通讯区间的全部节点, *i* 的坐标定为 (50, 50). 试验范围内全部簇头节点会将选举信息进行广播, 节点 *i* 在收到相应的广播之后会对两者之间的相互距离进行计算, 并且对历史记录信任过的节点以及候选簇头节点的密集程度进行查找, 最后以最优原则为依据对可信簇头进行选择.

具体结果如表 1 所示, 依据可信任簇头选取方法, 对等候选举的节点可信数值、数据采集融合率、信息传输耗损和簇结构的负载均衡进行综合考量. 由于 18 号节点选举值最大, 则让参照节点选取其为簇头节点, 然后朝簇头节点发出入列申请.

表 1 参照点 *i* 的信任节点选举数据

ID	坐标	可信度	密度	距离	簇头	状态	函数值
1	(32,15)	0.16	30	13.6	否	恶意	NULL
6	(51,50)	0.21	33	21.1	否	恶意	NULL
10	(32,37)	0.08	29	18.6	是	恶意	6.11
11	(22,51)	0.94	32	18.2	是	信任	6.98
13	(50,40)	0.90	25	10.5	是	信任	14.25
18	(39,63)	0.92	33	24.2	是	信任	17.33
20	(65,63)	0.85	29	12.7	是	信任	7.28
25	(57,79)	0.88	30	15.8	否	信任	10.75

实验对 HRBNT 算法和改进算法路由层级的建立采取了仿真模拟, 模拟结果如图 4 和图 5 所示. 在原算法中, 无线网的全部节点会以收到广播的次数和频率为标准来对较近的簇进行选择; 但在改进算法中, 成员节点通常会选择选举函数值最大的簇, 并且会向簇头发出加入请求, 候选的簇头在收到请求之后会对本地的信任记录进行查询, 然后根据成员节点信任值的高低来决定允许或拒绝其加入.

据仿真结果数据得到, 原算法不能对恶意节点进行及时地识别和排除, 有时还会将一部分恶意节点误认为是网络流量, 从而导致破坏网络正常结构的后果; 而改进算法则可对恶意簇头与节点进行有效的清除, 并且还可在最大程度上对簇结构的布局进行优化整合. 这其中的原因主要在于, 建立路由层级时, 原算法在一定程度上缺乏恰当的信任机制, 但改进算法对可信度、密集度进行了充分考量并利用节点之间的协同合作检测恶意节点, 使网络更加安全可信.

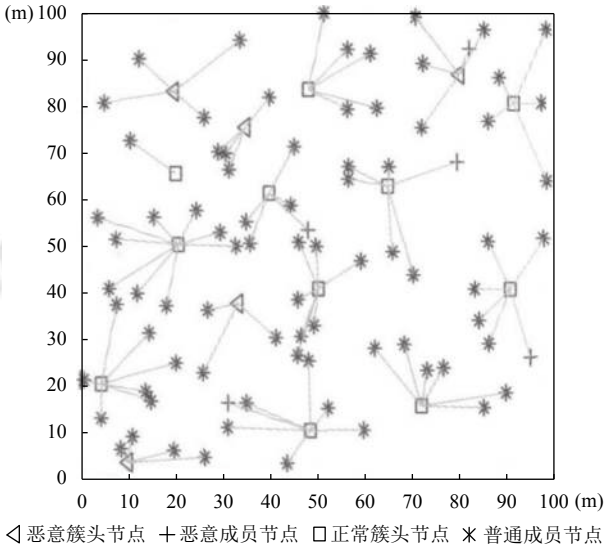


图 4 HRBNT 算法在网络攻击下的簇结构

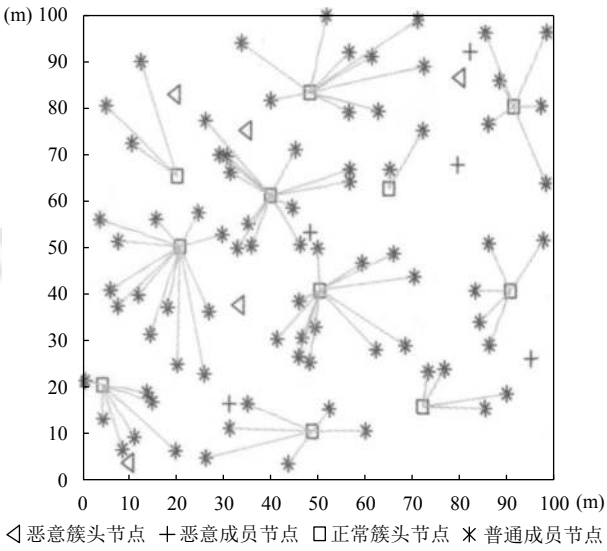


图 5 改进算法在网络攻击下的簇结构

3 结语

本研究提出了一种基于节点信任值的无线传感网路由算法, 其以节点信任评估为基础, 对节点距离与密集度进行分析考量, 并使用局部最优化和分布式策略, 经过对路由节点的可信选举, 预防恶意节点参与数据

通信, 保证了层次路由的安全性和可信性, 可对无线传感网节点失效和被俘获所导致的路由安全问题进行有效的解决.

参考文献

1 祝凯捷, 蔡权伟, 林璟锵, 等. 密钥安全及其在虚拟化技术下的新发展. 密码学报, 2016, 3(1): 12–21.

2 王栋, 熊金波, 张晓颖. 面向云数据安全自毁的分布式哈希表网络节点信任评估机制. 计算机应用, 2016, 36(10): 2715–2722. [doi: 10.11772/j.issn.1001-9081.2016.10.2715]

3 李明明, 乐光学, 代绍庆, 等. 无线 mesh 网络中可信协同信道资源分配策略. 电信科学, 2017, 33(5): 62–74.

4 刘志锋, 陈凯, 李雷, 等. 一种多种攻击并发下的 WSN 生存性评估模型. 计算机科学, 2017, 44(8): 129–133, 161. [doi: 10.11896/j.issn.1002-137X.2017.08.023]

5 Awad A, German R, Dressler F. Exploiting virtual coordinates for improved routing performance in sensor networks. IEEE Transactions on Mobile Computing, 2011, 10(9): 1214–1226. [doi: 10.1109/TMC.2010.218]

6 Alajmi N, Elleithy K. Multi-layer approach for the detection of selective forwarding attacks. Sensors (Basel), 2015, 15(11): 29332–29345. [doi: 10.3390/s151129332]

7 段正飞, 冯军焕. 一种抵御虫洞攻击的安全定位方法. 传感器与微系统, 2019, 38(4): 51–54.

8 付翔燕, 李平, 吴佳英. 无线传感器网络选择性传递攻击的检测和防御机制. 计算机应用, 2012, 32(10): 2711–2715, 2718.

9 齐全, 王可人, 杜奕航. 基于信誉机制的认知 Ad hoc 网络分簇协作频谱感知. 计算机科学, 2017, 44(10): 103–108. [doi: 10.11896/j.issn.1002-137X.2017.10.020]

10 金鑫, 胡平. 无线传感器网络入侵检测系统模型. 传感器与微系统, 2016, 35(5): 46–48, 59.

11 闫海云, 吴韶波. 基于能量和节点密集度的 WSN 路由算法. 物联网技术, 2015, 5(7): 42–45. [doi: 10.3969/j.issn.2095-1302.2015.07.018]

12 徐世武. 无线传感器网络分级成簇路由算法. 计算机系统应用, 2017, 26(2): 129–133. [doi: 10.15888/j.cnki.csa.005569]

13 吴银锋, 周翔, 冯仁剑, 等. 基于节点信任值的无线传感器网络安全路由. 仪器仪表学报, 2012, 33(1): 221–228. [doi: 10.3969/j.issn.0254-3087.2012.01.033]

14 刘金鑫. 无线传感器网络信任评估模型与方法研究[硕士学位论文]. 北京: 北京交通大学, 2015.

15 胡向东, 蔡东强. 无线传感器网络安全加密成簇算法的设计及研究. 重庆邮电大学学报 (自然科学版), 2009, 21(3): 421–424.