计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190100172

WSNs 中基于信任度的节能机会路由算法

苏凡军　杜可怡
上海理工大学光电信息与计算机工程学院　上海 200093

摘　要　为了防止网络中存在的潜在恶意节点被加入到机会路由的候选转发集中，减少网络能量的消耗，并保证数据的可靠传输，提出了一种在无线传感器网络中基于信任度的节能机会路由(Trust Based Energy Efficient Opportunistic Routing in Wireless Sensor Networks，TBEEOR)算法。该算法根据网络的拓扑结构计算节点的代数连通度，进而计算节点的连通度诚意；再联合节点的转发诚意和 ACK 诚意，利用信息熵的概念计算综合信任度；最后，用节点的综合信任度来计算节点之间通信和协作造成的能量消耗，从而得到网络的预期成本。此外，该算法能够有效地识别和判断网络中的恶意节点，进一步减小了恶意节点对网络性能的影响。实验结果表明，TBEEOR 算法有效地保证了数据传输的可靠性，有助于延长网络生命周期，从而增加了网络吞吐量，减少了网络能量消耗。

关键词：机会路由；无线传感器网络；代数连通度；信任度；能量消耗
中图法分类号　TP393

Trust Based Energy Efficient Opportunistic Routing Algorithm in Wireless Sensor Networks

SU Fan-jun and DU Ke-yi
School of Optical-Electrical and Computer Engineering，University of Shanghai for Science and Technology，Shanghai 200093，China

Abstract　In order to prevent potential malicious nodes in the network from being added to the candidate forwarding set of opportunistic routing，reduce network energy consumption and ensure reliable data transmission，a trust based energy efficient opportunity routing in wireless sensor networks(TBEEOR)algorithm was proposed. The algorithm calculates the algebraic connectivity of nodes according to the topology of the network，then calculates the sincerity of the connectivity of the nodes，and then combines forwarding sincerity and ACK sincerity of nodes to calculate the comprehensive trust degree by using the concept of information entropy. Finally，comprehensive trust of nodes is used to calculate the energy consumption caused by communication and cooperation between nodes，thereby obtaining the expected cost of the network. In addition，the algorithm can effectively identify and judge malicious nodes in the network，further reducing the impact of malicious nodes on network performance. The experimental results show that the TBEEOR algorithm effectively guarantees the reliability of data transmission and helps to prolong the network life cycle，thereby improving the throughput of network，and reducing network energy consumption.

Keywords　Opportunistic routing，Wireless sensor networks，Algebraic connectivity，Trust，Energy consumption

1　引言

无线传感器网络是由部署在检测区域内的大量传感器节点以自组织和多跳的方式构成的无线网络，其主要目的是以协作方式对监控区域进行数据信息的采集、分析并将其传输到 sink 节点[1]，并且无线传感器节点常被用于大规模的无线传感器网络中，具有动态的拓扑结构和自组织等特性。但是，无线传感器节点容易受到功率、存储、带宽和能量等多方面因素的影响[2]；另外，无线网络中衰落、干扰和多路径效应等各种因素均有可能导致数据传输出现暂时性的严重数据包丢失[3-5]。因此，无线传感器网络路由协议的研究需要考虑可靠性和节点能耗等因素。

麻省理工学院(MIT)的 Biswas 等于 2004 年率先提出了机会路由(Opportunistic Routing)[6]。将无线信道的广播特性应用于机会路由，能很大程度地改善无线网络中数据传输的可靠性和端到端的吞吐量。因此，很多研究人员将机会路由引入传感器网络。文献[7]回顾了近年来一些重要的机会路由协议，并将这些路由协议按照不同标准进行更深层次的分类，充分对其进行了剖析和比较。但是，早期的一些机会协议(如 ExOR[6] 和 MORE[8])均没有考虑能耗问题。而 Mao 等提出的 EEOR[9] 路由算法，利用可调发送能量模型和不可调发送能量模型计算传感器节点的路由代价，并选择最优候选转发集，从而使得数据通过这些节点转发到 sink 节点时的总能耗最小。EEOR 路由协议中的无线节点按照能量优先级

到稿日期：2019-01-21　返修日期：2019-05-04　本文已加入开放科学计划(OSID)，请扫描上方二维码获取补充信息。
基金项目：国家自然科学基金(61703278)
This work was supported by the National Natural Science Foundation of China (61703278).
通信作者：苏凡军(sufanjun@126.com)

转发数据，若拥有高优先级的节点转发了数据，则拥有低优先级的节点就会丢弃监听到的数据包，从而减少造成节点能量浪费的可能性。AsOR[10]设计的分段路由方法，通过选择最优的段内节点个数使得平均能耗最小；但 AsOR 是从全局角度优化能耗，属于集中式的路由算法。Mandar 等提出的 CBEEOR[11]，是一种基于 EEOR 中可调节发送能量模型的改进算法，并且采用在同一时刻允许多个节点转发数据包的方式计算转发能量。CBEEOR 利用回退时间机制尽可能避免了数据在候选转发集中节点之间的重复传输，能量消耗较 EEOR 有所减少。

由于无线传感器节点在复杂的网络环境中可能会遇到突发性的状况，比如传感器节点能量太低，受到恶意节点的攻击等，因此许多研究者着手研究节点的信任度[12-13]和识别恶意节点的技术[14]，提出了各种信任模型[15]，并将其应用于机会路由，以此来提高网络的安全性和数据的准确性。近年来，研究者们已经对 ad-hoc 网络、物联网和其他移动无线网络的信任管理协议和算法进行了改进，且提出的 RTOR，TORDP 和 GEOTOR 标准为机会路由协议计算信任值提供了支撑。文献[16]首次将信任模型应用于机会路由中，信任值的计算基于直接交互的直接信任度和与信任相似的推荐信任度；但是用于计算直接信任度的参数值大多依赖于专家经验，会在一定程度上影响对信任模型的客观评价。文献[17]利用无线节点服从 Beta 分布的理论基础进一步评估了节点的信任度，但该方法未考虑到失败交互中可能存在非恶意因素（如网络本身的不稳定）带来的数据包丢失引起的网络异常行为。文献[18]利用一种新的看门狗机制检测节点信息，将节点的链路投递率、节点的地理信息以及节点信任值整合为路由测度。这种机制在优化候选集的同时不仅会造成更多的网络开销，而且没有将其他节点的推荐信息作为计算节点信任值的重要参数，从而不能全面且准确地计算信任模型的信任值。NTA3D[19]路由算法将被监测区域分成网格，并在每个网格的中心放置吸引源，再联合节点的信任度综合计算吸引源的信任度，从而调度节点进行数据的转发；但该算法并没有考虑调配节点的能耗。以上文献虽然考虑了如何有效地计算节点的信任度，但没有将节点信任度作为衡量机会路由中能量消耗的标准。

针对上述问题，本文在对信任模型进行研究的基础上，提出了一种利用节点之间的连通度来衡量节点信任度的无线传感器网络节能机会路由协议。该协议通过使用节点的拉普拉斯矩阵来计算节点的代数连通度，根据节点的转发诚意、ACK 诚意以及连通度诚意，利用信息熵的概念计算节点的信任度，并创新性地将节点信任度作为选择候选转发集和计算网络能量消耗的主要参数，以保证网络的可靠性，并实现网络能量消耗的最小化，达到节能的目的。

本文利用 NS2 仿真工具对 TBEEOR 算法进行了仿真，并将其与 CBEEOR 和 EEOR 路由协议进行分析与对比。实验结果证明，TBEEOR 算法保证了整个网络的信任度，提高了网络端到端的吞吐量，延长了网络生命周期，并且能够大幅度地降低网络的能量消耗，从而实现节能。

第 2 节绍了无线传感器所组成的网络模型；第 3 节介绍了节点连通度的计算方式；第 4 节对节点信任度的计算方式进行了阐述；第 5 节详细介绍了 TBEEOR 算法；第 6 节对路由算法的实验结果进行了详细的分析；最后对全文进行总结。

2 网络模型

将无线传感器网络定义为一个无向简单有限图 $G=(V,E)$，其中 $V=\{v_1,v_2,\cdots,v_n\}$ 代表传感无线节点的顶点集合，E 代表节点之间的链路/边集合。无向图表示网络中所有存在的链路都是双向的并可以实现相互通信，即节点 v_i 能够到达节点 v_j 且节点 v_j 也能够到达 v_i；简单图表示节点中不存在自环，并且两个节点之间没有连接多条边；有限图表示节点和边的基数是有限的。假设参数 R 为无线节点 u 的通信范围，且将通信范围内的所有节点均称为节点 u 的邻居节点，表示为 $N(u)$。链路(u,v_i)表示在预定义的通信范围内节点 u 可以直接传输数据包到节点 v_i，且 $v_i\in N(u)$；$E_t(u,v)$和 $E_r(u,v)$分别表示无线节点发送和接收一个数据包所消耗的能量。e_{uv_i} 表示节点 u 利用链路(u,v_i)发送的数据没有被候选转发中节点 v_i 成功接收的概率。

3 节点连通度

节点连通度表示节点之间实现通信并进行数据传输的可能程度，可能程度越高说明节点的连通性越好，进一步加强了网络的连通性。此外，网络的连通性和流量的流通程度，对于保持节点之间的持续通信起到了重要的作用。节点之间只有保持连通的状态，才有可能实现数据传输和相互通信；相反，节点一旦因失效而不能正常工作，就会影响节点的通信和网络的连通性，导致数据包不能传输且出现网络延迟。因此，故本文引入代数连通度[20]的概念来计算节点的连通度属性。

定义 1 节点 u 的连通度属性被量化为不包括节点 u 及其相关联边的图的代数连通度，表示为 $a(G)$。图 G 的代数连通度 $a(G)$是拉普拉斯矩阵 $L(G)$的第二小特征值，且 $L(G)=D(G)-A(G)$[20]。其中，$D(G)$为图 G 的度矩阵，$A(G)$为图 G 的邻接矩阵。

对于图 $G_1=(V,E_1)$和 $G_2=(V,E_2)$，只要$|E_1|\leqslant|E_2|$，$a(G_1)\leqslant a(G_2)$，就表明图 G_2 的连通性比图 G_1 的连通性好，故节点 v_2 的连通度比节点 v_1 的连通度大，节点 v_2 对于维持网络连通性的能力就比节点 v_1 的能力好。因此，$a(G)$的值越大，图 G 的连通性就越好。由图 1 可得，各节点的代数连通度 $a(G_{v_1})=2$，$a(G_{v_2})=1$，$a(G_{v_3})=2$，$a(G_{v_4})=2$。

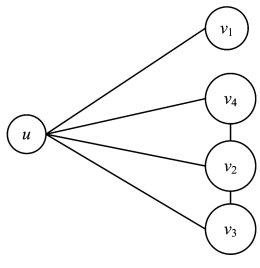

图 1 网络图

Fig. 1 Network diagram

4 节点信任度的计算

节点信任度 T 是评估节点对被评估节点关于信任程度的量化。因此，本文利用节点的转发诚意、ACK 诚意和连通

度诚意对节点信任度进行综合评估。此外，考虑到各个参数在信任度评估中所占的比重和节点影响网络性能的程度，不能直接从逻辑的层面上判断节点信任度。为了克服个人主观方面对权重分配的影响，增强各参数的自适应性，本文引入信息熵的概念来综合性地计算节点信任度。信息熵反映了多个评价指标对待评价事务的影响程度，即各指标在评价过程中提供有效信息的多寡程度[21]。因此，利用信息熵来对节点的转发诚意、ACK 诚意和连通度诚意进行权值的分配。节点信任度的计算如下：

$$T_{v_i}=W_{v_i}^{F}*F_{v_i}+W_{v_i}^{ACK}*ACK_{v_i}+W_{v_i}^{Con}*Con_{v_i} \tag{1}$$

其中，F_{v_i}，ACK_{v_i} 和 Con_{v_i} 分别为节点 i 的转发诚意、ACK 诚意和连通度诚意；$W_{v_i}^{F_i}$，$W_{v_i}^{ACK}$ 和 $W_{v_i}^{Con}$ 分别为节点 i 转发诚意、ACK 诚意和连通度诚意的自适应权重。

4.1 转发诚意

转发诚意表示候选节点成功转发数据包次数与失败转发数据包次数的关系。其计算方式如下：

$$F_{v_i}=\frac{FS_{v_i}}{FS_{v_i}+FF_{v_i}},F_{v_i}\in[0,1] \tag{2}$$

其中，F_{v_i} 表示节点 i 的转发诚意，FS_{v_i} 表示节点 i 转发数据包成功的次数，FF_{v_i} 表示节点 i 转发数据包失败的次数。

4.2 ACK 诚意

ACK 诚意表明节点之间发送和接收确认信息的诚意，且记录了确认信息传输成功与失败的次数。此度量对于计算重传数据包的概率非常有用，其计算方式如下：

$$ACK_{v_i}=\frac{SACK_{v_i}}{SACK_{v_i}+FACK_{v_i}},ACK_{v_i}\in[0,1] \tag{3}$$

其中，ACK_{v_i} 表示节点 i 的 ACK 诚意，$SACK_{v_i}$ 表示节点 i 发送成功的 ACK 包数量，$FACK_{v_i}$ 表示节点 i 发送失败的 ACK 包数量。

4.3 连通度诚意

连通度诚意用于衡量节点与节点之间的连通程度，是衡量节点信任度必不可少的参数。其计算方式如下：

$$Con_{v_i}=\frac{a(G_{v_i})}{\sum\limits_{i\in N(u)}a(G_{v_i})},Con_{v_i}\in[0,1] \tag{4}$$

其中，Con_{v_i} 表示节点 i 的连通度诚意，$a(G_{v_i})$ 表示发送 v_i 节点的连通度。

通过对转发诚意、ACK 诚意和连通度诚意的计算，得到转发诚意、ACK 诚意和连通度诚意的信息熵，分别表示为 $H(F_{v_i})$，$H(ACK_{v_i})$ 和 $H(Con_{v_i})$；进一步得到转发诚意、ACK 诚意和连通度诚意的自适应权重，分别表示为 $W_{v_i}^{F}$，$W_{v_i}^{ACK}$ 和 $W_{v_i}^{Con}$。相关计算公式如下：

$$H(F_{v_i})=-F_{v_i}\log_2 F_{v_i} \tag{5}$$

$$H(ACK_{v_i})=-ACK_{v_i}\log_2 ACK_{v_i} \tag{6}$$

$$H(Con_{v_i})=-Con_{v_i}\log_2 Con_{v_i} \tag{7}$$

$$W_{v_i}^{F}=\frac{H(F_{v_i})}{H(F_{v_i})+H(ACK_{v_i})+H(Con_{v_i})} \tag{8}$$

$$W_{v_i}^{ACK}=\frac{H(ACK_{v_i})}{H(F_{v_i})+H(ACK_{v_i})+H(Con_{v_i})} \tag{9}$$

$$W_{v_i}^{Con}=\frac{H(Con_{v_i})}{H(F_{v_i})+H(ACK_{v_i})+H(Con_{v_i})} \tag{10}$$

综上所述，节点信任度 T_{v_i} 是通过节点的转发诚意 F_{v_i}、ACK 诚意 ACK_{v_i} 和连通度诚意 Con_{v_i} 3 个参数进行有机融合而得到的。信任度越高的节点，参与数据可靠传输和通信的可能性就越大，进一步加强了节点之间的协作、通信的稳定性及数据的安全性，减少了内部节点之间因为节点信任度不过关而造成的链路不可靠传输问题。

5 TBEEOR 算法的实现

TBEEOR 路由协议的设计包括预期成本的计算和算法描述两部分，从而有效地选择候选转发集和下一跳中继节点以减少能量的消耗。

5.1 预期成本的计算

源节点通过下一跳中继节点转发数据包到 sink 节点的预期成本包括传输数据的成本和维持节点之间信任度的通信成本。节点 u 的候选转发集 $Fwd(u)$ 是邻居节点集 $N(u)$ 的一部分，即 $Fwd(u)\subseteq N(u)$。由于是将节点本身的能量作为选择候选转发集的标准，因此根据节点的预期成本将节点 u 的候选转发集 $Fwd(u)$ 进行非降序排列，即 $Fwd^*(u)=\{v_1,v_2,\cdots,v_{|Fwd(u)|}\}$，其中 $i<j\Rightarrow C_{v_i}<C_{v_j}$。因此，其预期成本由 3 部分组成：1）源节点发送的数据包至少被候选转发集中的一个节点成功接收到的预期成本，表示为 $C_u^h(Fwd^*)$；2）候选转发集中的一个节点转发数据包到 sink 节点的转发成本，表示为 $C_u^f(Fwd^*)$；3）为了保持网络的稳定性和节点之间的可靠传输而形成的通信成本，表示为 $C_u^a(Fwd^*)$。因此，源节点广播数据包通过候选转发集中的节点转发数据到 sink 节点的预期成本 $C_u(wd^*)$ 为：

$$C_u(Fwd^*)=C_u^h(Fwd^*)+C_u^f(Fwd^*)+C_u^a(Fwd^*) \tag{11}$$

节点 u 发送的数据包被候选转发集中至少一个节点 v 成功接收到所消耗的能量取决于发送、接收一个数据包的固定能量和传输概率，故发送的预期成本 $C_u^h(Fwd^*)$ 如下：

$$C_u^h(Fwd^*)=\frac{w}{\rho}=\frac{E_t(u,v)+E_r(u,v)}{1-\prod\limits_{i=1}^{|Fwd^*|}e_{uv_i}} \tag{12}$$

其中，e_{uv_i} 表示源节点 u 发送的数据包没有被候选转发集中任何节点 v 成功接收到的概率。

节点 v_1 成功转发数据包的概率是 $1-e_{uv_1}$，且其预期成本是 C_{v_1}；节点 v_2 成功转发数据包的概率是 $e_{uv_1}\times(1-e_{uv_2})$），且其预期成本是 C_{v_2}。理论上，$Fwd^*(u)$ 中的节点在同一时刻只允许一个节点转发数据，从而避免了数据包的重复传输，故转发预期成本的计算如下：

$$\beta=(1-e_{uv_1})*C_{v_1}+\sum_{i=2}^{|Fwd^*|}\left(\prod_{j=1}^{i-1}e_{uv_j}\right)*(1-e_{uv_i})*C_{v_i} \tag{13}$$

由机会路由的广播特性可知，候选转发集中的所有节点都有接收到源节点广播数据包的可能性。想要候选转发集中的节点在同一时刻只有一个节点转发数据，需要节点之间进行协调和合作；一旦没有这种协调，候选转发集中的多个节点就会同时转发同一个数据。在这种情况下，传输同一个数据包到 sink 节点所产生的能量消耗，计算方式如下：

$$\beta=\sum_{i=1}^{|Fwd^*|}\left(\prod_{j=1}^{i-1}e_{uv_j}\right)*(1-e_{uv_i})*C_{v_i} \tag{14}$$

为了维持无线传感器网络的正常运行和数据转发过程的井然有序，该文允许候选转发集中的多个节点对数据包进行

转发。因此，TBEEOR 路由算法利用式(14)计算转发数据的预期成本。考虑到节点之间成功传输的概率，转发数据包的预期成本为 $C_u^f(Fwd^*)$：

$$C_u^f(Fwd^*)=\frac{\beta}{\rho}=\frac{\sum_{i=1}^{|Fwd^*|}(\prod_{j=1}^{i-1}e_{uv_j})*(1-e_{uv_i})*C_{v_i}}{1-\prod_{i=1}^{|Fwd^*|}e_{uv_i}} \quad (15)$$

在 TBEEOR 路由协议中，虽然节点之间是否连通是衡量节点进行通信的必要条件，但是单凭连通度这一个参数不能对网络进行可靠通信和保证网络的连通起到决定性作用。因此，将节点信任度作为计算节点通信和协作所需能量消耗的重要参数，称其为通信成本，即 $C_u^a(Fwd^*)$。分别用发送节点和接收节点的信任度来衡量两个节点之间的通信成本 $C_u^a(Fwd^*)$，计算如下：

$$C_u^a(Fwd^*)=\frac{E_t(u,v)}{T_u}+\frac{E_r(u,v)}{T_v} \quad (16)$$

其中，T_u 和 T_v 分别表示源节点和接收节点的信任度。

5.2 算法描述

基于信任度的节能机会路由算法的具体步骤如下：

Step1 随机部署传感器节点到 100 m×100 m 的目标区域中，且选择 5%～20%的节点作为恶意节点集，表示为 S。

Step2 传感器节点根据其通信半径 R 决定邻居节点 $N(u)$。

Step3 根据传感器节点的分布情况计算每个节点的代数连通度。

Step4 充分利用式(1)综合计算节点的信任度 T。

Step5 假设 $C_u=\infty$，$Fwd=\emptyset$，$S\neq\emptyset$，且根据预期成本对节点进行非降序排序。

Step6 如果节点的预期成本低于总的预期成本，且该节点不属于恶意节点集 S，则将该节点添加到候选转发集，并根据式(11)计算预期成本；如果节点的预期成本高于总预期成本，无论节点是否属于恶意节点集 S，都不能将节点添加到候选转发集。

Step7 循环执行 Step6，直到遍历完邻居节点为止，从而得到候选转发集。将预期成本最低的节点作为下一跳中继节点，进行数据包的转发。

假定 $E_t(u,v)=0.7$，$E_r(u,v)=0.3$，并且 $N(u)=\{v_1,v_2,v_3,v_4\}$，$S=\{v_2\}$。简单起见，让 e_i 表示 e_{uv_i}，让 c_i 表示节点 v_i 的预期成本。首先，根据图 2 和式(1)－式(10)，可以算出候选转发集中各节点的信任度，即 $T_{v_1}=\frac{1}{2}$，$T_{v_2}=0$，$T_{v_3}=\frac{1}{2}$，$T_{v_4}=\frac{1}{2}$。其次，根据式(11)计算预期成本，将节点 v_1 加入候选转发集即 $Fwd(u)=\{v_1\}$ 的预期成本被计算为 $(E_t(u,v_1)+E_r(u,v_1)+(1-e_1)\times c_1)/(1-e_1)+E_t(u,v_1)/T_u+E_r(u,v_1)/T_{v_1}=4.6$；虽然节点 v_2 的预期成本为 1 且会减小，但是 $v_2\in S$，故不能加入候选转发集；节点 v_3 的预期成本为 1.5，故节点 v_3 会减少预期成本，即 $Fwd(u)=\{v_1,v_3\}$ 的预期成本计算式为 $(E_t(u,v_3)+E_r(u,v_3)+(1-e_1)\times c_1+e_1\times(1-e_2)\times c_2+e_1e_2(1-e_3)\times c_3)/(1-e_1\times e_2\times e_3)+E_t(u,v_3)/T_u+E_r(u,v_3)/T_{v_3}=4.1$；节点 v_4 的预期成本为 5，节点 v_4 将会增加预期成本，假如 $Fwd(u)=\{v_1,v_3,v_4\}$，则预期成本计算为 $((1-e_1)\times c_1+e_1(1-e_2)\times c_2+e_1e_2(1-e_3)\times c_3+e_1e_2e_3(1-e_4)\times c_4)/(1-e_1\times e_2\times e_3\times e_4)+(E_t(u,v_4)+E_r(u,v_4))/(1-e_1\times e_2\times e_3\times e_4)+E_t(u,v_4)/T_u+E_r(u,v_4)/T_{v_4}=4.45>4.1$，故 v_4 不能加入候选转发集。因此，候选转发集是 $Fwd(u)=\{v_1,v_3\}$，且源节点转发数据包到目的节点的预期成本是 4.1，节点 v_3 最终被选作转发数据包到目的节点的转发节点。

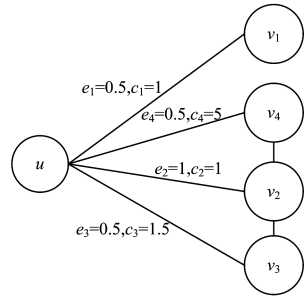

图 2 计算预期成本

Fig. 2 Calculate expected cost

6 仿真实验

6.1 实验参数设置

利用 NS2 仿真工具对本文提出的 TBEEOR 算法进行实验。将 50×250 个传感器节点随机部署在 100 m×100 m 的区域内，并在所有的无线节点中随机选择 0～20%的节点作为降低网络信任度的恶意节点。实验中具体参数的设置如表 1 所列。

表 1 实验参数

Table 1 Experimental parameters

参数	描述
区域/m^2	100 * 100
节点数目	50～250
节点传输范围/m	30
恶意节点百分比/%	0,5,10,15,20
数据包大小/bytes	50
发送能量/J	0.660
接收能量/J	0.395
初始化能量/J	10
仿真时间/s	500

本文将对信任度变化趋势、吞吐量、能量消耗、生命周期这 4 个方面的性能进行比较和分析，并将其与 CBEEOR 算法和 EEOR 算法进行对比。

6.2 实验分析

6.2.1 网络信任度分析

在网络信任度的评估中，恶意节点所占百分比分别为 0，5%，10%，15%和 20%的情况下，网络信任度的变化情况如图 3 所示。由图 3 可知，网络中没有部署恶意节点时网络信任度最高，能够最大限度地保证网络中的节点实现数据的可靠传输。当网络中的传感器节点数目一定且部署的恶意节点所占比例越来越高时，3 种路由算法的网络信任度逐渐下降。其中，CBEEOR 算法和 EEOR 算法由于没有直接判断和识别网络中恶意节点的机制，因此其网络信任度会随着恶意节点所占比例的增加而大幅度下降，几乎与恶意节点所占比例成正比；而本文提出的 TBEEOR 路由算法可以识别候选转发集中潜在的恶意节点，虽然一开始遇到恶意节点时其网络的信任度迅速下降，但是当网络中恶意节点所占比例在 10%左右

时，网络信任度的下降趋势慢趋于平缓。因此，TBEEOR 算法在网络信任度方面的性能比 CBEEOR 算法和 EEOR 算法好，并且能够有效地识别和剔除候选转发集中的恶意节点，尽可能地保证网络的可靠性和数据的可靠传输。

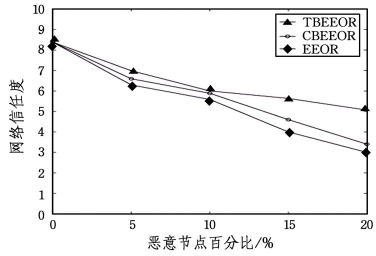

图 3 网络信任度

Fig. 3 Network trust

6.2.2 网络能耗分析

本文将通过计算预期成本方式来验证 TBEEOR，CBEEOR 与 EEOR 3 种路由算法在能量消耗方面的性能。当网络节点数目一定且恶意节点百分比不同时，TBEEOR，CBEEOR 和 EEOR 3 种路由算法的网络能量消耗如图 4 所示。在网络传感器节点数目一定时，随着恶意节点百分比的增加，TBEEOR 算法的网络能耗呈现上升的趋势，但增加的幅度非常小，说明网络中恶意节点的数目会随着监测机制的运行而减少，对网络能量消耗的影响也减小。相反，CBEEOR 和 EEOR 算法消耗的能量都随着恶意节点的增多而大幅度上升，但 CBEEOR 算法的能量消耗并没有 EEOR 算法消耗的能量多，因为 CBEEOR 算法利用了节点的连通度属性来衡量网络的连通性，对于维护网络的稳定性起到了重大的作用，导致恶意节点对网络的影响较 EEOR 算法小，从而使网络中节点消耗的能量更小。综上，本文提出的计算预期成本的方式能够大幅度地降低网络的能量开销，有助于延长网络的生命周期。

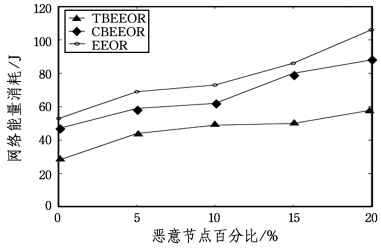

图 4 网络能量消耗

Fig. 4 Network energy consumption

6.2.3 网络吞吐量分析

当网络节点数目一定时，随着恶意节点百分比的增加，TBEEOR，CBEEOR 和 EEOR 3 种路由算法吞吐量的变化趋势如图 5 所示。由图 3 可知，网络中恶意节点所占比例的增加，导致 3 种路由算法的网络信任度均逐渐降低，对网络中数据的可靠传输和网络端到端的吞吐量造成了巨大的影响。由图 5 可知，受网络中恶意节点的影响，TBEEOR，CBEEOR 和 EEOR 3 种路由算法的吞吐量均呈现下滑的趋势，但是 TBEEOR 算法的吞吐量始终比 CBEEOR 和 EEOR 算法的吞吐量大。最主要的原因是：在网络中节点数目一定时，随着恶意节点数目的逐渐增多，CBEEOR 和 EEOR 两种路由算法没有在网络中设置检测恶意节点的机制，导致恶意节点对网络的连通性造成破坏，从而使网络的吞吐量呈现大幅度下降的趋势；而本文提出的 TBEEOR 算法可以利用设置的检测机制有效地识别网络中的恶意节点，且高效地将恶意节点从候选转发集中剔除，选择符合信任度条件的传感器节点，增加了网络中数据传输的可靠性，从而进一步提高了网络端到端的吞吐量。

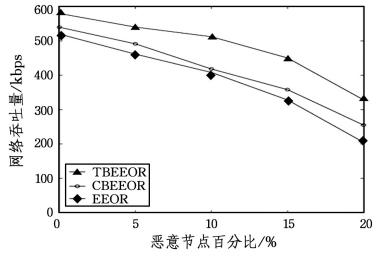

图 5 网络吞吐量

Fig. 5 Network throughput

6.2.4 网络生命周期分析

当网络中恶意节点百分比不变时，随着传感器节点数目的逐渐增加，网络生命周期变化的基本情况如图 6 所示。基于能量消耗的评估过程可知，文中计算预期成本的方式相较于其他两种路由算法可以在一定程度上降低网络的能量开销，能够有效地帮助网络中的节点实现能量的充分利用，从而延长网络的生命周期。从图 6 可知，TBEEOR 的网络生命周期会随着网络中节点数目的增加而延长，且均比 CBEEOR 和 EEOR 两种路由算法的网络生命周期更长。此外，随着网络中传感器节点数目的增加，TBEEOR 与其他两种算法的差距变大，优势更加明显。CBEEOR 算法利用了节点的连通度属性，一方面对于减小节点受到攻击与破坏的可能性是不可或缺的，另一方面有效地提高了网络中正常节点的性能，故 CBEEOR 算法的生命周期明显长于 EEOR 算法的生命周期。根据以上的分析结果，改善网络能量消耗的计算方法不仅增加了节点多次利用的次数，而且减少了节点早死或失效的可能性，从而改善了整个网络的生命周期。

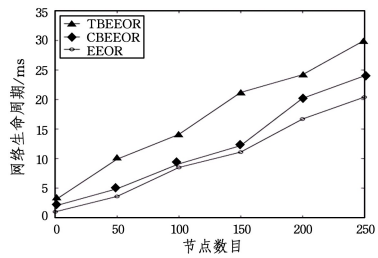

图 6 网络生命周期

Fig. 6 Network life cycle

6.2.5 时间复杂度和空间复杂度分析

TBEEOR 算法与 CBEEOR 和 EEOR 两种算法最大的不同在于选择候选转发集中节点的标准不同。CBEEOR 和 EEOR 两种算法在选择候选转发集的时候都将节点的预期成本作为选择的标准，两者没有本质上的区别，故两者的时间复杂度都是 $O(n^2)$，空间复杂度都是 $O(1)$；TBEEOR 算法不仅将节点的预期成本作为选择候选转发集的标准，而且还考虑了节点的信任度。TBEEOR 算法虽然设置了检测恶意节点的机制，但仅是对节点信任度的一种判断，并没有增加算法的

时间复杂度，故 TBEEOR 算法的时间复杂度也为 $O(n^2)$ 且空间复杂度为 O(1)。由以上的分析可以，虽然 TBEEOR 算法与 CBEEOR 和 EEOR 两种算法的空间复杂度和时间复杂度是相同的，但是 TBEEOR 算法比其他两种路由算法的性能更好。

从以上 5 个方面的分析可知，本文提出的 TBEEOR 算法能够提高网络的信任度，以保证网络数据的可靠传输，并且基于节点信任度和预期成本最小化的标准选择转发节点，有效地降低了网络中节点能量的开销，从而减少了整个网络消耗的能量，对于延长网络的生命周期有着相辅相成的作用。

结束语 本文根据节点信任度的评估模型和网络中节点能量消耗的情况，创新性地提出了一种基于信任度的节能机会路由算法。该算法将节点连通度作为衡量节点信任度的主要参数，并将节点信任度用于计算节点的通信成本和作为选择候选转发集的评判标准，以减少能量消耗为目的选择出下一跳中继节点；此外，利用恶意节点监测机制在保证网络信任度的同时减小了恶意节点对网络性能的影响，进一步提高了网络端到端的吞吐量并延长了网络的生命周期，减小了无线节点不工作或失效的可能性。但是，该算法在计算节点信任度的时候并没有进行实时更新，会让节点的信任度不能够完全地反映出当前网络的真实情况。因此，在今后的研究中会考虑节点信任度动态的实时变化，降低对网络性能的影响。

参 考 文 献

[1] HOLGER K, ANDREAS W. Protocols and Architectures for Wireless Sensor Networks [M]. New York: John Wiley & Sons, 2007.

[2] MASSAYUKI O A, AUGUSTO F A. Ant-based Dynamic Hop Optimization Protocol: a Routing Algorithm for Mobile Wireless Sensor Networks [C] // 2011 IEEE Globecom Workshops. IEEE, 2011: 1139-1143.

[3] RAJU J, GARCIA-LUNA-ACEVES J J. A new approach to on-demand loop-free multipath routing [C] // International Conference on Computer Communications & Networks. IEEE, 1999.

[4] NASIPURI A, CASTANEDA R, DAS S R. Performance of multipath routing for on-demand protocols in mobile ad hoc networks [J]. Mobile Networks & Applications, 2001, 6(4): 339-349.

[5] RAPPAPORT T. Wireless Communications: Principles and Practice[M]. Electronic Industry Press, 2011.

[6] BISWAS S, MORRIS R. ExOR: Opportunistic multi-hop routing for wireless networks [J]. Acm Sigcomm Computer Communication Review, 2005, 35(4): 133-144.

[7] AZZEDINE B, AMIR D. Opportunistic Routing in Wireless Networks: Models, Algorithms, and Classifications [J]. ACM Computing Surveys, 2014: 47(2): 1-36.

[8] SZYMON C, MICHAEL J, SACHIN K, et al. Trading structure for randomness in wireless opportunistic routing [J]. Acm Sigcomm Computer Communication Review, 2007, 37(4): 169-180.

[9] MAO X F, TANG S J, XU X H, et al. Energy-Efficient Opportunistic Routing in Wireless Sensor Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(11): 1934-1942.

[10] CHEN W, CHEN Z, FAN P Y, et al. AsOR: An Energy Efficient Multi-Hop Opportunistic Routing Protocol for Wireless Sensor Networks over Rayleigh Fading Channels [J]. IEEE Transactions on Wireless Communications, 2009, 8(5): 2452-2463.

[11] KARYAKARTE M S, TAVILDAR A S, KHANNA R. Connectivity Based Energy Efficient Opportunistic Robust Routing for Mobile Wireless Sensor Networks [J]. Wireless Personal Communications, 2015, 84(1): 729-744.

[12] HAN G J, JIANG J F, LEI S, et al. Management and applications of trust in Wireless Sensor Networks: A survey [J]. Journal of Computer and System Sciences, 2014, 80(3): 602-617.

[13] JIANG J F, HAN G J, FENG W, et al. An Efficient Distributed Trust Model for Wireless Sensor Networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 26(5): 1228-1237.

[14] CAI S B, HAN Q L, GAO Z G, et al. Research on Cloud Trust Model for Malicious Node Detection in Wireless Sensor Network [J]. Acta Electronica Sinica, 2012, 40(11): 2232-2238.

[15] LIU T, XIONG Y, HUANG W C, et al. Trust Computation Model of Nodes Based on Bayes Estimation in Wireless Sensor Networks [J]. Computer Science, 2013, 40(10): 61-64.

[16] WANG B, HUANG C H, LI L Y, et al. Trust-based minimum cost opportunistic routing for Ad hoc networks [J]. Journal of Systems and Software, 2011, 84(12): 2107-2122.

[17] THORAT S A, KULKARNI P J. Opportunistic Routing in Presence of Selfish Nodes for MANET [J]. Wireless Personal Communications, 2015, 82(2): 689-708.

[18] MAHMOOD S, AZZEDINE B, AMIR D, et al. Towards a novel trust-based opportunistic routing protocol for wireless networks [J]. Wireless Networks, 2015, 22(3): 1-17.

[19] DANG X C, WANG H M, HAO Z J. Three dimensional coverage algorithm based on node trust degree in wireless sensor networks [J]. Application Research of Computers, 2016, 33(12): 3794-2796.

[20] FIEDLER M. Algebraic connectivity of graphs [J]. Czechoslovak Mathematical Journal, 1973, 23(23): 298-305.

[21] YIN X Q, WU J, MO W W, et al. Improved Opportunistic Routing Algorithm Based on Node Trustworthiness for WMNs [J]. Computer Science, 2017, 44(8): 151-156.

SU Fan-jun, born in 1976, Ph.D, lecturer. His main research interests include wireless sensor networks, data center network and recommendation algorithm.

DU Ke-yi, born in 1992, postgraduate. Her main research interests include wireless sensor networks and opportunistic routing.