WSN 中基于子博弈的节点能量优化算法研究*

张科峰，王改云
（桂林电子科技大学 电子工程与自动化学院，广西 桂林 541004）

摘 要：引用子博弈精炼模型对节点参与路由进行建模，基于安全度设计一个评价函数，对参与路由的节点进行合作度奖励而对没有参与路由的节点实施惩罚。避免了过度信任与使用某个节点，均衡了网络节点的能量消耗，优化了网络节点能量的利用率。实验结果表明，该算法与传统算法相比在相同的时间里具有较少的死亡节点，延长了网络寿命，并具有较强的鲁棒性。

关键词：子博弈纳什均衡；无线传感器网络；节点安全度；节点能量

中图分类号：TP393 **文献标识码**：A **文章编号**：1674-7720(2012)07-0054-04

Node energy optimization algorithm research based on subgame in WSN

Zhang Kefeng, Wang Gaiyun
(Institute of Electronic Engineering and Automation, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: The paper quotes the theory of subgame perfect nash equilibrium to model the reference node which is involved in routing. It designs an evaluation function based on safety, rewards or penalizes the routing nodes. This can avoid excessively trust and using one node, balance the network nodes energy consumption and optimize network node energy utilization. The experimental results show that there are less death nodes compared with the traditional method in the same time, and can prolong the life span of the network, and it also has strong robustness.

Key words: subgame perfect nash equilibrium; WSN; node safety; node energy

在无线传感器网络 WSN(Wireless Sensor Network)中，节点的能量非常有限，并且不能持续供电，节省能量就显得异常重要。由于传感器节点体积小，不可能带有很大的电池以供节点消耗，因此节点的电量是非常有限的。尽管节点结构简单、耗电量不大，但是目前的很多应用要求传感器网络可以长时间工作，更换电池或给电池充电是不可行的，因此，无线传感器网络设计的一个目标就是有效利用仅有的能量以延长网络寿命[1]。

WSN 中传统的最优可信路径算法(MTP)，节点能量选择的主要依据是从邻居节点发送询问报文来获取该节点的安全度。例如参考文献[2]采用的就是当节点 x 请求 y 节点路由时，y 节点发现 x 节点的路由请求中的能量存储值和本地存储的值不一致，就向邻居节点发送请求报文，从返回的请求报文中综合判断后，返回安全度的差异作为判断，从而作出接收请求与否的决策。参考文献[2]的算法没有考虑 P2P 技术中节点共谋存在的问题，并忽略了 WSN 中网络部署结构给其节点安全度判断带来的影响。而参考文献[3]通过对交互节点间的局部评价进行加权后得出评价可信度计算节点的全局信誉值，再采用基于局部评价标准差、局部评价集中度的方法识别和抑制共谋攻击，然后根据节点行为的变化更新其信誉值和评价可信度来抑制节点共谋行为的发生。参考文献[2]中忽略了节点安全度误判给整个路由路径带来的影响，最终导致网络节点能量选择效率降低。

本文将子博弈精炼模型引入到能量节点选择模型中，并就此提出一种最高安全度的能量节点选择算法 EOP (Energy Optimal Path)。本文设计了一个安全度评价函数，用来监测整个网络节点的安全度，并就节点安全度的返回值进行相似性分析，如果相似性超过一定的阈值就判断其存在节点共谋，并采用继任节点簇再次判断以确定节点的安全度。

1 传统基于节点安全度的能量选择模型

在传统基于节点安全度的能量选择模型[2]中，节点

* 基金项目：国家自然科学基金(61163059)

安全度的评价信息需要从其他节点收集，因此节点安全度的确认就需要一个参数模型进行评价。节点安全度判断是整个 WSN 网络可信判断的核心，本文也以节点安全度来判断节点能量值的有效性。

节点安全度的内容如下：节点能量和合作度等参数存储在本地节点上，节点安全度的评价信息却需从邻居节点的回复结果来计算自身的安全度。然而这种安全度收集方式存在数据作假问题，如节点被俘且进一步对数据造假或者恶意节点伪造自身安全度。这些问题可以通过图 1 提出的安全度检查来进行验证。传统的节点安全度模型如图 1 所示。

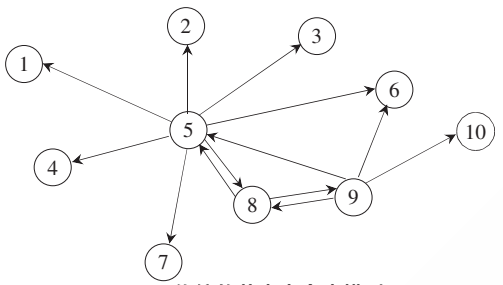

图 1 传统的节点安全度模型

假设节点 1 发送路由请求节点 5，那么在传统的节点安全度模型中，节点 5 会将节点 1 的安全度与本地保存的安全度进行比较，如果有误差，节点 5 就会向其所有的邻居节点（即节点 2、3、4、6、7、8、9）发送一个验证报文，这样节点 5 所能依赖的验证节点有 7 个；再假设节点 5 向节点 8 发送请求，那么按照节点安全度模型，节点 8 也会向其所有的邻居节点发送验证报文，然而节点 8 就只能依赖 5、7、9 这 3 个节点来判断。

该节点安全度模型的缺点如下：

（1）每个节点所能依赖的验证节点固定，完全存在节点共谋作假的可能，从而导致网络能量过度消耗的现象。

（2）每个节点所依赖的验证节点个数和安全度对应的加权不一致。路由节点对其依赖节点返回安全度的值是完全不一致的，因此存在误判断的情况。

（3）在此路由中可能存在对某几个节点的过度信任与依赖，从而导致某些节点能量过度消耗，过早出现死亡节点的情况。

2 子博弈纳什均衡机制的节点能量选择判定

在传统的节点安全度模型中，节点的安全度的评价方案还不够完善。特别是节点的安全度由节点所有的邻居节点来评价，由此带来了节点共谋的问题，并使得安全度值的数据不完全可信，最终导致节点能量消耗增加。本文提出了一种新方案，将子博弈纳什均衡理论引入到节点安全度最优路径的判断策略中来。对每个节点返回的安全度值进行分块处理，并剔除节点安全度值较低的节点，最终得出一个可信的安全度值。如果节点安全度高的一簇节点返回的评价值误差在 ε 范围之内，就接受该节点作为路由节点。

子博弈纳什均衡是将纳什均衡中包含的不可置信的威胁策略剔除出去，它要求参与者的决策在任何时间点上都是最优的。子博弈纳什均衡的定义如下：

定义 1 子博弈纳什均衡（Subgame Perfect Nash Equilibrium）中的动态博弈是指各参与者行动有先后，后行动者根据先行者所作的选择来决定自己的选择。其中，完全信息博弈表示每个参与者对其他参与者的特征、战略空间和评价函数都了解，子博弈是指整个博弈过程中某一阶段以后的博弈。它具有初始信息和进行博弈分析所需的全部信息[4]。

定义 2 对于扩展式博弈的策略组合 $S^*=(S1^*, \cdots, Si^*, \cdots, Sn^*)$，其中，每个参与者所选择的战略都是最优的，并且如果它是原博弈的纳什均衡，则它在每一个子博弈上也都构成纳什均衡，即它是一个子博弈精炼纳什均衡。

子博弈精炼纳什均衡是基于每个参与者自身角度来考虑所选择策略的不同收益程度，在此收益程度的基础上建立一个策略选择的过程，这种过程用图来表示就是一棵“与或树”。对于不同的参与者，这种“与或树”是不一样的，这样的一棵“与或树”就是博弈树（Game Rree）。建立起博弈树之后求解的一个解集合就是子博弈精炼纳什均衡的解集合。现在假设一棵博弈树[5]结构如图 2 所示，其中，坐标分别代表的是根节点的进退策略收益值。

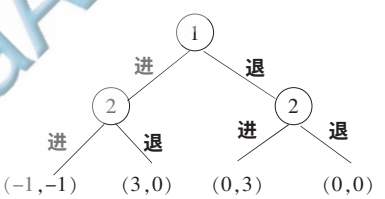

图 2 博弈树求解图

该博弈树求解的过程如下：

（1）若 2 在右，2 将选择进（0，3），因为（0，3）>（3，0）。

（2）若 2 在左，2 将选择退（3，0），因为（3，0）>（-1，-1）。

（3）在 2 的选择中，1 的最大收益是选择进，因为（3，0）>（0，3），所以纳什均衡为（进（进，退）），均衡解为（进，退），均衡收益为（3，0）。

2.1 节点安全度选择模型的建立

基于子博弈精练纳什均衡理论，引入子博弈精炼纳什均衡的节点安全度模型建立在如下两个定义的基础上。

定义 3 深安全度节点：它的影响因素包括能量因素和合作度因素。两组因素加权处理后共同描述一个节点的信任度，深信任度是信任度的前 n 位值。

定义 4 深安全度节点簇：M 个深信任度节点组成一个深信任节点簇。

基于以上两个定义建立的安全度模型如图 3 所示。

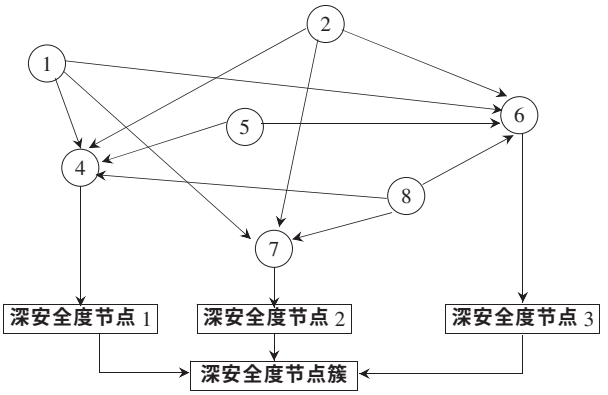

图3 子博弈机制安全度模型

集合 S 用来描述一个深安全度节点簇，它取自所有网络节点中的前 n 个节点，而在每一次的路由过程中，全网络都需要刷新每个节点的安全度值，并对网络节点依据安全度值进行分簇，对所有的分簇进行递归求解子博弈纳什均衡，并从纳什均衡集中选取最优结果集作为路由请求节点的仲裁节点集，此集作为上任节点选择该节点安全度的值是否成为路由节点的依据。使用该集合中的元素返回的报文信息作为判断依据。假设节点 x 向节点 y 发送路由请求，当 y 收到 x 的节点请求之后判断本地的存储的 x 安全度值，如果误差范围存在且超过阈值£，就向本次路由中深安全度节点簇发送询问报文。当所有深安全度节点返回的关于此节点的安全度值后，对这些安全度值进行分簇，并建立博弈树。对此博弈树进行递归求解，得出一个最优解集。对解集中的值进行相似度判断，如果相似度高于某阈值 a，就认为该数据不合理，并继续之前阐述的子博弈选择过程。节点安全度最优解集处理步骤如图4所示。

图4 节点安全度最优解集流程图

2.2 安全度描述算法

每个节点的安全度值在每次路由过程完成之后刷新，本文每个节点的安全度值用一个变量 t 来描述，每个节点的安全度值与其节点自身存储的能量值以及其合作度相关联。t 表示节点当前的安全度，e 表示节点自身存储的能量值，c 表示节点的合作度（节点通过一次路由，合作度值加1）。每个节点存储一个集合 $S(e,c)$，即当前节点的（能量，合作度），对相应的节点还存在一个集合 $W(W1,W2)$，即相应的权值，它们的关系式为：

$$t=s\times W=(e,c)\times(W1,W2) \quad (1)$$

其中，$W1+W2=1$ (2)。

假设 m 为每个节点参与总路由过程中的成功百分比，那么有如下2个变量定义：

$$\alpha=(1-e^{-0.5\times m}) \quad (3)$$

其中，0.5为修正因子。

$$\beta=\begin{cases}\beta\times(1-m) & m<50\% \\ \beta\times e^{0.8\times m} & m>50\%\end{cases} \quad (4)$$

其中，0.8为修正参数。

则有：$W1=\alpha/(\alpha+\beta)$；$W2=\beta/(\alpha+\beta)$

针对不同的应用需求，对W1和W2进行不同的权重选择，相应得出不同安全度。参数范围与适用的网络环境关联表如表1所示。

表1 参数范围与适用的网络环境关联表

	W1	W2	应用
W1>W2	>0.5	<0.5	适合于能量要求更高，且网络环境不太复杂的环境
W1=W2	=0.5	=0.5	适合于能量要求与网络复杂要求相同的环境
W1<W2	<0.5	>0.5	适合网络环境比较复杂，且能量相对充足的环境

如果是普通节点全部发送报文进行咨询，显然不能消除一些恶意节点和不可置信节点带来的威胁，因此需要剔除不可置信节点。本文采用深安全度节点簇来描述一个高安全度节点的集合，它集合了一个WSN网络节点中的前 n 位安全度高的节点。每次依据节点安全度进行路由的流程如图5所示。

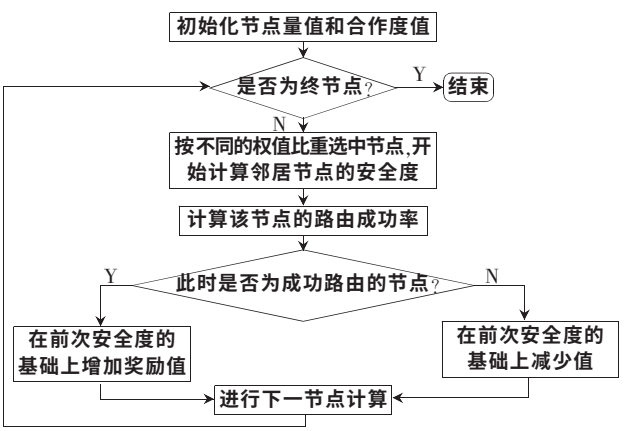

图5 节点安全度计算流程图

3 实验方案及仿真

本实验的目的是将传统最优路径选择算法(MTP)[2]与本文提出的EOP算法在网络能量空洞以及节点能量消耗两个方面进行对比。

实验中,设定传感器节点区域大小为[10,10],随机生成网络节点数为100。子博弈选择出的安全度优化集的相似度阈值为0.7,每个节点的合作度初始值在30~100之间随机取,网络中的节点能量在20~100之间随机取。为了验证本文算法在网络节点能量优化上的优越性,在随机生成的100个网络节点中进行了2 000次的路由过程记录,并提取路由过程中出现的死亡节点个数以及每次路由的节点能量数据,基于提取出的数据来分析网络中出现能量空洞以及网络节点能量优化效率的问题,通过系统仿真实验数据进行如下分析。

两种方法分别在路由过程中出现首节点死亡情况对比如图6所示。

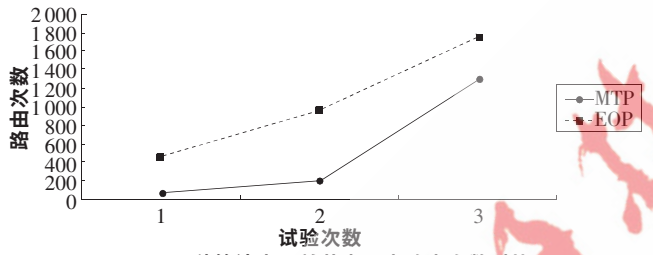

图6 两种算法出现首节点死亡路由次数对比

由图6可知,基于安全度算法的无线传感器网络在第443、964和1 750次时出现首节点死亡,SOP算法出现首节点死亡的路由次数比MTP算法的路由次数要多,从而可以看出基于子博弈安全度算法在路由安全鲁棒性上要优于传统算法。

实验结果取的是单组实验中的50轮实验结果,以轮为单位取单轮实验中所有路径的路径安全度平均值,从图7中可以看出,与传统算法相比,节点安全度算法在平均路径能量值上性能明显较优。在实际的传输过程中,假定节点的安全度以100为单位计算,当节点的安全度少于$100\times\pounds(\pounds<1)$时,路由节点传输被判断为路由失败,那么从图7可以看出,基于子博弈的安全度算法节点路由成功的概率明显大于传统算法。这是由于传统算法没有考虑路径中安全度的信任问题,因此安全性能较差。而更新后的算法中的可信度融入了安全的因素,因此更新后的算法的安全性较优。

本文引入子博弈机制来实现节点能量优化算法,首先引入节点安全度评价概念,在此基础上判断某个具体节点是否可以参与本次路由,有效降低了路由过程中选

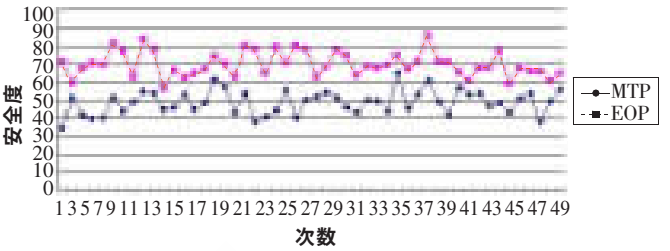

图7 两种算法中节点路由成功概率对比

择低能量节点的现象,从图6中关于死亡节点出现的情况可以得知,路由网络的鲁棒性有一个明显的改善。同时,从图7可以得出该算法优化了网络的能量管理。每次路由过程中重新选择不同的节点安全度进行安全度判断,有效防止了节点共谋,解决了对某一个节点过度依赖的问题。本方案也有待解决的问题和不足之处。本文主要通过计算节点安全度来判断某节点是否可以参与路由的过程,这会使得路由节点过多从而导致计算复杂。如何选择一个参数来适配计算复杂度、网络鲁棒性以及高能量节点,同时对本文给出的其他两种环境的研究,都是后续研究的方向。

参考文献

[1] KANNAN R, SARANGI S, IYENGAR S S. Sensor-centric energy-constrained reliable query routing for wireless sensor networks [J]. Journal of Parallel and Distributed Computing, 2004,64(7):839-852.

[2] 陈作汉,任旭鹏,卢鹏丽.对抗共谋及节点行为动态性的P2P信任模型[J].计算机应用,2011,31(2):308-312.

[3] 王江涛,陈志刚,邓晓衡.WSN中基于完全信息动态博弈的可信路由研究[J].小型微型计算机系统,2010,31(8):1478-1483.

[4] 吴广谋,王文平,尤海燕,等.数据,模型与决策[M]北京:石油工业出版社,2003.

[5] 王骐,孙建伶.基于优化迭代的博弈树算法[J].计算机应用与软件,2008,25(2):228-230.

[6] 孙利民,李建中,陈渝,等.无线传感器网络[M].北京:清华大学出版社,2005.

(收稿日期:2011-12-14)

作者简介:

张科峰,女,1986年生,硕士研究生,主要研究方向:可信计算、无线传感网络。

王改云,女,1964年生,副教授,硕士生导师,主要研究方向:智能控制、数据融合、故障诊断等。