# 无线传感器网络中基于网格信任度的可靠覆盖算法研究*

董书豪[1]，李小龙[1,2†]

(1. 桂林电子科技大学 计算机科学与工程学院，广西 桂林 541004；2. 曼尼托巴大学 电子与计算机工程学院，加拿大 温尼伯 R3T 2N2)

**摘 要**：针对节点的覆盖优化过程极易受到各种攻击的问题，通过从信任管理的框架内深入探索可靠覆盖技术，提出了一种基于网格信任度的可靠覆盖算法。该算法对节点进行可靠性筛选和轮换调度，以并行覆盖的方式对覆盖区域内的网格点实施基于信任度的覆盖。对节点信任阈值的取值进行讨论，分析得出信任阈值的大小对整个覆盖区域的安全性和覆盖质量有很大影响。经过仿真与传统的单一覆盖机制作比较，该算法能有效提高网络安全性和延长网络寿命。仿真结果验证了算法的有效性和分析的正确性。

**关键词**：信任管理；可靠覆盖；轮换调度；网格点；信任阈值

**中图分类号**：TP393.08 **文献标志码**：A **文章编号**：1001-3695(2014)01-0253-04

doi:10.3969/j.issn.1001-3695.2014.01.059

# Research on reliable coverage algorithm based on grid trust value for wireless sensor networks

DONG Shu-hao[1], LI Xiao-long[1,2†]

(1. *School of Computer Science & Engineering, Guilin University of Electronic Technology, Guilin Guangxi* 541004, *China*; 2. *School of Electronic & Computer Engineering, University of Manitoba, Winnipeg Canada R3T 2N2*)

**Abstract**: To solve the problem that nodes can easily suffer from various attacks during the process of coverage optimization, this paper discussed reliable coverage technology on the basis of the trust management system framework, and proposed a reliable coverage algorithm based on grid trust value. The algorithm performed the reliability screening and rotation scheduling on nodes, and the coverage based on the credibility of grid point by the way of parallel coverage. After discussing the value of the trust threshold, the paper found that it had a significant influence on the security of whole coverage area and the coverage quality. By comparing the new algorithm with traditional single coverage algorithms, the algorithm can improve the security and network lifetime effectively. Simulation experiments show the effectiveness of this algorithm and reflect the correctness of the analysis.

**Key words**: trust management; reliable coverage; rotation scheduling; grid point; trust threshold

## 0 引言

随着近几年来科学技术的进步，无线传感器逐渐向小型化、高效能、低功耗等方面发展，并且可以在无线电通信领域应用中实现高性价比的批量生产。伴随着无线传感器网络(wireless sensor network，WSN)在战场监测、环境和交通监测等领域越来越多的应用[1]，迫切需要在受到资源约束、WSN 脆弱性不可避免以及攻击和破坏行为客观存在的条件下，WSN 能提供可靠的服务质量。但迄今为止，很少有一个完整的可信 WSN 系统可以有效保障可靠的网络服务，极大地约束了 WSN 的发展[2,3]。为了节约能量，研究者们开始研究在传统的传感器中加入覆盖控制的功能，以便使用尽量少的节点完成覆盖要求。为了解决 WSN 易受到攻击而导致节点所覆盖区域不安全问题，研究者们又提出了信任的概念，以保证覆盖区域的安全性。目前，基于信任管理的安全路由技术[4]、安全融合技术[5]、安全定位技术[6]和安全时间同步技术[7]等已出现了一些有价值的研究成果，但还没有行之有效的基于信任管理的安全覆盖机制。传统的覆盖算法或是信任管理模型只是两个不同的研究方向，没有将两者结合起来研究。WSN 通过节点间的相互协作执行监测区域、目标跟踪的任务，但进行协作的前提和基础是参与节点是正常节点，而非恶意节点。为了提高网络覆盖质量的可靠性，屏蔽节点失效对覆盖质量造成的影响，研究者研究设计可靠的覆盖机制，取得了一定的研究成果。

文献[8]通过在网络中额外增加一些监测节点的办法来监测节点丢弃数据包的行为，帮助失效节点转发数据包，支持传感数据最终安全、准确地到达汇聚节点。文献[9]提出了一种基于 2-Coverage 的可靠覆盖机制，通过增加冗余覆盖来屏蔽单个节点的失效，达到容错效果。为了避免单个节点失效造成网络节点整体移动，文献[10]提出了基于虚拟坐标的节点调度方案。以上这些研究的可靠覆盖机制主要集中于解决减少

**收稿日期**：2013-03-28；**修回日期**：2013-05-03 **基金项目**：国家自然科学基金资助项目(61063040)；广西可信软件重点实验室开放课题(kx201305)；桂林市科学研究与技术开发项目(20100104-1)

**作者简介**：董书豪(1989-)，男，硕士研究生，主要研究方向为自组织网络；李小龙(1981-)，男(通信作者)，湖南常德人，副教授，博士，主要研究方向为传感器网络、Mesh 网络(xlli@guet.edu.cn).

节点失效对覆盖质量的影响。然而在现实应用中,除了节点失效造成网络覆盖质量下降以外,网络攻击等都会对覆盖质量造成影响。例如,若网络中的监测节点被敌方俘获,成为恶意节点,监测节点辅助的加强机制将失去效用。对于“贪吃蛇”节点替换方案,若网络中的个别节点或者部分节点老化,传感数据严重偏离现实数据,这些虚假的数据将会引发错误警报,干扰用户决策,消耗有限的网络资源,造成严重的后果。

文献[11]虽然提出了一种基于信任管理的节点覆盖调度方案,但是该调度方案只是简单地把信任管理模型加入到节点中,具体调度时仅仅把不可信的节点剔除,而没有把它与实际的覆盖算法相结合。该调度方案不能保证节点所覆盖区域的覆盖质量,一旦节点在工作过程中突然失效,其覆盖区域会陷入部分瘫痪。

信任管理模型的提出是传统安全机制的有效补充,已经应用于 Internet 网络安全中的方方面面。由于上述原因,信任管理模型的应用已经成为当今的研究热点。当前,通用的信任管理模型有很多种,其中由 Ganeriwal-Srivastava 提出的 RFSN[12] 就是一种典型的基于声望的通用信任管理系统。为了减少信任管理造成较高的能量和存储开销,Shaikh 等人[13]提出一种基于分组的轻量级信任管理系统,Ho[14]提出了基于区域块的信任管理系统。本文所提出的基于网格信任度的可靠覆盖机制,并不是局限于某种特定的信任管理模型,任何有效的模型都可以应用到该机制中。因此,具有更好的通用性。

本文在对以上文献研究的基础上,提出了一种基于网格信任度的节点自适应轮换调度算法。在基于节点信任调度的基础上,对可信任节点进行自适应轮换调度。之后通过对虚拟网格划分形成的网格点进行量化,若经过量化的信任度无法达到安全覆盖的要求,则苏醒相关节点重新调度。本文算法的目的是在高覆盖的基础上尽量提高覆盖区域的安全性,从而通过对网格点的安全覆盖基本满足这一要求,同时保证了网络的覆盖质量和安全性。

## 1 基于信任管理的模型

### 1.1 网格点信任模型

网格点是虚拟网格剖分目标区域形成的,即划分网格时的横纵坐标的交叉点。通过以网格点为圆心,以节点通信半径为半径内的活跃节点(信任度超过节点信任阈值的节点)对网格点进行并行覆盖,经过量化,最终得到网格点的信任度。本模型基于以下假设:a)通过某种定位算法可以得到无线传感器节点和网格点的位置,即这些点的坐标值;b)虚拟网格的尺寸限制于 $\min(\sqrt{2}/4Rc,\sqrt{2}/2Rs)$,即每个网格的边长;c)节点的信任度是基于某个信任管理模型量化出来的,相关过程具体内容本文不再讨论。

为了接下来对模型的描述更加方便,本文定义了一些符号:

$T_{\min}$:节点信任度阈值,信任度低于该阈值的节点被判定为恶意节点(该阈值是由所选信任管理模型、节点数量等因素决定)。

$T_{\max}$:网格点联合信任阈值,若网格点信任度量化后低于该阈值则不能保证覆盖区域的质量和安全性(该阈值由周围工作节点的数量以及它们的信任度等因素决定)。

*Na*:表示为恶意节点,节点的信任度低于 $T_{\min}$。

*Nb*:表示为休眠节点,节点的信任度虽然高于 $T_{\min}$,但是经过轮换调度算法最终被判定为冗余的节点。

*Nc*:表示为工作节点,节点的信任度高于 $T_{\min}$,并且经过轮换调度算法活跃的节点。

*Rc*:节点通信半径。

*Rs*:节点感知半径。

网格点信任模型选择节点的结果如图 1 所示。

具体的选择工作节点的过程将在接下来基于网格信任度的节点自适应轮换调度算法的描述中讲到。如图 1 所示,以网格点为圆心,*Rs* 为半径范围内的活跃的工作节点对网格点进行量化处理,得到该网格点的联合信任度。如果所有网格点的信任度都高于信任度阈值 $T_{\max}$,说明该覆盖区域已经达到了高覆盖度和安全度的要求。如果有网格点的信任度低于阈值 $T_{\max}$,说明达不到安全的高覆盖度要求,则需要重新对达不到要求的网格点进行调度。

### 1.2 网格点信任度数学模型

为了使网格点的感知半径内能够具有更好的安全性,要求感知半径内一半以上的工作节点正常工作的概率大于网格点信任度阈值 $T_{\max}$,这样才能保证网络的正常运作。

假设网格点 $W_{ij}$ 的感知半径内有 $n$ 个比较可信任的节点(超过节点信任阈值 $T_{\min}$ 的节点),信任度分别为 $T_1,T_2,T_3,\cdots,T_n$,即信任度集合 $S=\{T_1,T_2,T_3,\cdots,T_n\}$。$S_{mk}$ 表示所有感知错误节点信任度组成的集合,其中 $m$ 表示感知错误节点数量,$k$ 表示其中的一种可能性。例如,$S_{21}=\{T_1,T_2\}$ 代表感知错误节点有两个,$\{T_1,T_2\}$ 是错误节点的其中一种可能性。网格点的信任度数学模型为

$$Tw_{ij}=\sum_{m=1}^{\frac{n-1}{2}}\{\sum_{k=1}^{C_n^k}[\prod_{T\alpha\in S_{mk}}(1-T\alpha)\prod_{T\varepsilon\in(S-S_{mk})}T\varepsilon]\}+\prod_{\sigma=1}^{n}T\sigma \quad (1)$$

其中:$T\alpha$ 表示感知错误节点的信任度;$T\varepsilon$ 表示正常工作节点的信任度;$\prod_{T\varepsilon\in(S-S_{mk})}T\varepsilon$ 为所有感知正确节点的信任度的乘积;$S-S_{mk}$ 为该网格点感知半径内正常工作节点的信任度组成的集合。

只有所有覆盖目标区域网格点的信任度都达到阈值 $T_{\max}$,才能表明这是一个安全的覆盖,即

$$\begin{cases}\text{success} & Tw_{ij}\geqslant T_{\max}\\ \text{fail} & Tw_{ij}<T_{\max}\end{cases} \quad (2)$$

### 1.3 信任阈值的分析与讨论

节点信任度阈值 $T_{\min}$ 的大小对信任模型有很大影响,下面对可能出现的几种情况进行讨论:

a)节点信任度阈值 $T_{\min}$ 过低。信任度过低的节点加入到模型中,会导致需要加入更多的高信任度节点以保证网络的安全性。这样不仅要额外增加大量的节点,还造成了能量浪费。阈值过低还可能导致永远无法达到模型要求的 $T_{\max}$ 的标准。

b)节点信任度阈值 $T_{\min}$ 过高。阈值 $T_{\min}$ 过高,可能导致可以选择的工作节点过少,或者在网格点的感知半径甚至没有一个达到 $T_{\min}$ 标准的节点。

由此可见,节点信任度阈值在选择上要经过多方考虑,过高或过低都会对整个网络带来不利的结果。

## 2 基于网格信任度的节点自适应轮换调度算法描述

本章首先了分析算法需要满足的条件,然后设计了一种基于网格信任度的覆盖算法来调度传感节点,使得监控区域能够达到安全的高覆盖率。

### 2.1　算法需要满足的条件

a)尽可能选取最少的工作节点来保证网络的高覆盖度,延长整个网络的寿命。

b)算法应该是完全分布式,在信任管理的基础上,基于邻居节点的信息进行决策。

c)选取工作节点的过程应该考虑到节点的信任度,尽量调度信任度高的节点,有利于提高整个网络覆盖的安全度。

d)所选取的工作节点应该在覆盖区域内均匀分布。

### 2.2　算法思想

基于网格信任度的可靠覆盖机制,要求虚拟网格中存在着若干个处于正常状态的活动节点监控着目标区域,而让其余节点进入休眠状态,达到既保持覆盖质量又能延长网络生存时间的效果。网络的生存时间被划分为多个不同的时间段,每一个时间段内又分为节点调度阶段和工作两个阶段,调度阶段也是通过与邻居节点交换信息,根据信任度和节点位置来选择节点。

本文所提出的覆盖算法是一种完全分布式算法,要求把对整个覆盖区域的覆盖拆分成对覆盖区域内每一个网格点的覆盖,最终达到相同的或者更高的覆盖效果。该覆盖算法不仅要解决信任管理和覆盖相结合的问题,还要考虑活动节点的信任度变化对覆盖区域的影响,以及基于信任度的退避机制设计问题。

在对网络覆盖过程中,每经过一个周期,相关工作节点的信任度都可能出现变化。如果有节点的信任度变小,会导致对网格点的信任覆盖达不到 $T_{\max}$ 的标准。需要在新的周期开始直接增加工作节点,以保证网络可靠性。如图 2 所示,当(a)中的其中一个节点的信任度由 0.8 下降到 0.7 时,在新的运行周期(b)内,经过调度算法,网格点的感知区域内增加了一个新的信任度为 0.9 的节点,以达到要求的标准。

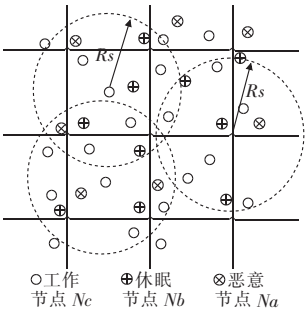


图 1　网格点信任模型选择节点结果

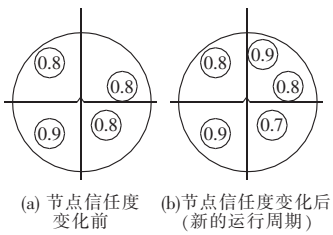


图 2　工作节点信任度变化对网格点感知区域的影响

在图 3(a)中,节点 $n_5$ 和 $n_6$ 的整个传感区域都可以被相邻的邻居节点所代替覆盖。如果两者分别都感知到自身满足休眠条件后,进入休眠状态会导致覆盖区域内出现盲点。为了避免出现覆盖盲点的状况,本文提出了基于信任度的退避算法。以图 3 为例,经过一段随机的时间后(算法设计中介绍随机时间选择方法),如果该随机时间相同,说明两者信任度相同,选择编号高的节点;如果随机时间不同,直接选择时间短的,即为信任值高的节点。图 3(b)为选择后的情况。

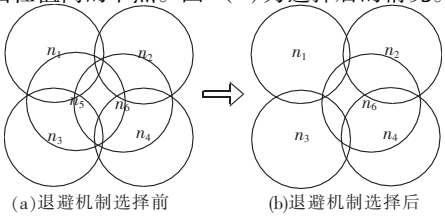


图 3　基于信任度的退避机制选择示意图

### 2.3　算法设计

**定义 1**　无线传感器节点的通信模型和感知模型都是圆盘模型。

**定义 2**　以网格点 $W_{ij}$ 为圆心,半径为传感器节点感知半径 $Rs$ 的圆形区域,称为该网格点的感知区域 $R$。称处于网格点感知区域内的传感器节点为相关节点,其他为不相关节点。即

$$\Omega_{ij} = \{n / d(n, W_{ij}) < Rs\} \quad n \in N$$

其中:$\Omega_{ij}$ 表示网格点相关节点的集合;$N$ 为覆盖区域内所有节点;$d(n, W_{ij})$ 表示节点到网格点的距离。距离小于 $Rs$ 的节点放入到集合 $\Omega_{ij}$ 中。

**定义 3**　对于传感器节点 $n_1$、$n_2$,它们所覆盖的区域分别为 $S_1$、$S_2$,如果 $S_1 \cap S_2 \neq \varnothing$,则传感器节点覆盖相关。

**定义 4**　对处于网格点感知区域 $R$ 内且不参加调度的休眠节点,用 $X$ 表示这些节点的集合。同时用 $G$ 表示参与覆盖任务的节点集合。

为了更好地说明算法实现的过程,现将算法的具体步骤作如下描述:

a)对目标区域进行虚拟网格划分,同时确定目标区域内所有网格点 $W_{ij}$ 的位置$(x,y)$。通过定义 2,可以找到网格点相关节点的集合 $\Omega_{ij}$。

b)判断网格点目标区域内所有相关节点的信任度 $T$。若 $T < T_{\min}$,则节点被判定为恶意节点,从网格点相关节点集中剔除,不参与任何调度;若 $T \geqslant T_{\min}$,则节点被判定为活跃节点,放入活跃节点集中,活跃节点集合记为 $H$。

c)为了保证覆盖过程中使用尽可能少的节点和保持更高的安全性,延长生命周期。把集合 $H$ 中的节点按照数量从少到多、信任度从高到底的顺序放入待工作节点集合 $G_1$ 中。例如,首先把集合 $H$ 中信任度最高的节点放入 $G_1$ 中,如果该节点的信任度能达到 $T_{\max}$ 标准,则该网格点的待工作集合即为此节点;否则,继续把集合 $H$ 中最高的节点放入集合 $G_1$,判断网格点的联合信任度是否达到要求。依此类推,最终确定所有网格点的待工作节点集合 $G_1$,同时把剩余活跃节点放入待休眠集合 $X_1$ 中。

d)在节点选择阶段,各个待工作节点还要向感知半径内的所有邻居节点广播 $P_{im}$ 消息(包括节点的编号、位置以及信任度)。当收集完信息后,若判断自己是冗余覆盖节点,为了避免出现覆盖盲点,引入了一个基于信任度的退避机制,每个待工作节点是否休眠还要等待一个随机时间 $t$,时间结束后才能确定是否进入待休眠状态。

对于覆盖相关节点 $n_1$、$n_2$,如果其信任度为 $Tn_1$、$Tn_2$,则设置定时器 $T_{tb}^{(n1)} = k|1 - \dfrac{T_{n1}}{T_{\max}}| \cdot t_{n1}$ 和 $T_{tb}^{(n2)} = k|1 - \dfrac{T_{n2}}{T_{\max}}| \cdot t_{n2}$。其中 $t_{n1}$、$t_{n2}$ 为节点的当前时间,$k$ 为系统的调节参数,可以根据实际情况设定。

具体的退避机制如下:(a)如果 $T_{tb}^{(n1)} = T_{tb}^{(n2)}$,则工作节点的选择以该节点的编号为准;(b)如果 $T_{tb}^{(n1)} \neq T_{tb}^{(n2)}$,则选择节点信任度高的作为工作节点。

所有待休眠节点确定后先不进入休眠状态,而是等待其覆盖范围内网格点的信任度确定后,根据网格点信任度的大小,才最终决定待休眠节点是进入休眠状态还是重新调度成为工作节点。将最终确定休眠的节点放入休眠节点集 $X$ 中,最终确定工作的节点放入节点集 $G$ 中。

e)网格点感知区域内的所有相关工作节点对网格点进行量化处理,得到其信任度 $Tw$。

接下来的节点调度分为两种情况:(a)信任度 $Tw \geqslant T_{max}$,表明网格点感知区域内完成了可信的高覆盖度要求,待休眠节点正式成为休眠节点;(b)信任度 $Tw < T_{max}$,表明网格点感知区域内的覆盖度没有达到信任的高覆盖要求,此时激活网格点感知区域内信任度最高的待休眠节点成为工作节点。将该工作节点加入到网格点信任度的量化过程中,重新计算信任度。如果信任度达到 $Tw \geqslant T_{max}$ 的标准,最终确定休眠节点和工作节点;否则重复该过程,直到网格的信任度达到上述要求为止。

f)选定好工作节点,节点调度进入第二个阶段,即工作阶段。执行相关监控任务,直到该周期结束。

整个网络的生存周期就是重复以上过程,直到该网络彻底无法工作。

本文所提出的算法中,首先从网络内的 $N$ 个节点中选出信任值较高节点,然后从中选出节点参与到覆盖 $M$ 个网格点中去,算法的时间复杂度为 $O(N \times M)$。

## 3 实验结果与分析

为了验证本文所提出算法的有效性和分析的正确性,使用 MATLAB7.5 作为仿真实验平台对其进行实验和分析。仿真实验环境为监控区域大小 100 m × 100 m,40 ~ 200 个节点随机分布在目标区域内,节点的感知半径 10 m 和通信半径为 30 m。假设该算法信任度的值是文献[12]中由 Ganeriwal-Srivastava 提出的基于信誉的信任管理模型(RFSN)所决定的。

将本文提出的基于网格信任度的节点自适应轮换调度算法与文献[11]中的基于信任模型的节点覆盖调度算法以及文献[15]中的 node self-scheduling(NSS)覆盖算法进行性能比较。其经过仿真结果如图 4 ~ 6 所示。

图 4 反映了三种不同算法随网络运行时间各自覆盖率的变化。随着时间的增加,本文算法的覆盖率变化不大,达到第 280 轮时,覆盖率依然能达到 80% 以上,而另外两种算法都低于 80%。文献[11]未采用轮换调度算法,节点没有很好地调度,能量消耗过快,所以导致了覆盖率下降的速度最快。NSS 覆盖算法虽然开始时节点利用率和覆盖率都很高,但是节点在工作过程中容易遇到突发状况,导致整体的覆盖质量下降。本文覆盖算法基于信任管理,对网格点的覆盖必须达到信任阈值才能确定,所以节点在工作过程中不容易出状况。由于对网格点采用的是并行覆盖方式,即便节点出状况,还有其他相关节点来保证覆盖质量。

图 5 反映的是三种不同算法随着整个网络运行时间的增加,各自覆盖区域安全程度的变化。定义节点安全行为是指不发生恶意伪装攻击和节点老化等问题的正确行为。从图中可以看到,随着时间的增加,本文算法和文献[11]算法覆盖区域的安全度并没有多大的变化,但是本文算法的安全度更高,这是由于采用了基于网格信任度的联合覆盖机制,提高了节点发生安全行为的概率,从而要求覆盖区域必须要有更高的安全度。经过综合考虑,本文提出的基于网格信任度的可靠覆盖算法在保证较高的覆盖质量的前提下,更加安全可靠。

图 6 反映的是三种不同算法随网络运行时间各自剩余总能量的变化。可以看出,文献[11]的网络寿命最短,这是由于所有节点都处于工作状态,能量消耗过快。其他两种节点都采用了节点轮换调度的方法,防止了能量的过快消耗。本文算法考虑了节点可能重复覆盖的问题,从而总体的能量消耗更慢,网络寿命更长。

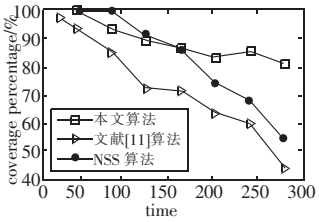

图 4 网络覆盖质量比较

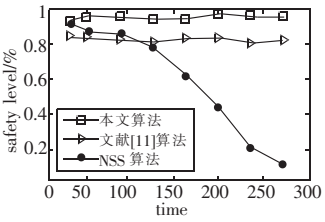

图 5 安全程度随时间的变化

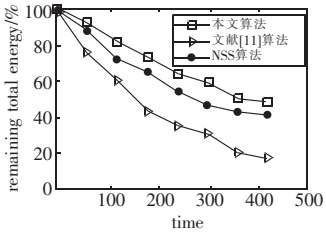

图 6 网络剩余总能量与运行时间的关系

## 4 结束语

本文针对区域覆盖的信任管理问题,提出了一种基于网格信任度的节点自适应轮换调度算法。在对信任管理框架深入了解的基础上,首先提出了网格点信任模型。在节点可信的基础上,网格点通信范围内的节点对其进行量化,以便达到高覆盖区域信任度的要求。同时在算法中采用一种新的基于信任度的退避机制,在避免出现盲点和节约能量的同时,对工作节点进行准确的选择。仿真实验表明,基于网格信任度的节点自适应轮换调度算法,不仅能够较为精确地保证要求的覆盖质量,而且能够有效地减少网络通信中的出错率,实现了网络环境的安全,为传感器网络高可靠覆盖技术和在信任管理框架内的可信传感器网络技术进一步研究提供了新思路和理论依据。

**参考文献:**

[1] 唐秋玲,杨柳青,覃团发,等. 无线传感器网络中 PPM 节能调制方案[J]. 中国科学 E 辑:信息科学,2007,37(12):1583-1596.

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

[3] QIN Ya-juan, ZHANG Si-dong, ZHENG Tao, *et al*. Issues of trust management for mobile wireless sensor networks[C]//Proc of the 7th International Conference on Wireless Communications, Networking and Mobile Computing. Piscataway: IEEE Press, 2011: 1-4.

[4] AGARATHNA K, MALLAPUR J D, HIREMATH S. Trust based secured routing in wireless multimedia sensor networks[C]//Proc of the 4th International Conference on Computational Intelligence, Communication Systems and Networks. Piscataway: IEEE Press, 2012: 53-58.

[5] 马守明,王汝传,叶宁. 基于信誉度集对分析的 WSN 安全数据融合[J]. 计算机研究与发展,2011,48(9):1652-1658.

[6] ZENG Ying-pei, CAO Jian-nong, HONG Jue, *et al*. Secure localization and location verification in wireless sensor networks[C]//Proc of the 6th International Conference on Mobile Ad hoc and Sensor Systems. Piscataway: IEEE Press, 2009: 864-869.

[7] YANG Ya-feng, SUN Yan. Securing time-synchronization protocols in sensor networks: attack detection and self-healing[C]//Proc of Global Telecommunications Conference. Piscataway: IEEE Press, 2008: 1-6.

(下转第 260 页)

a) 当网络结构处于单链状态下，从上文中第一段的分析论述可以看出，此时算法的时间复杂度是 $O(n^3)$，也就是该算法此时的适应程度最差。

b) 当网络中的路由排列处于完全图时，两两路由能够进行一次性的直接交互，即同一时间内完成了信息的传递，此时深度优先遍历次数的时间复杂度为 $O(1)$，那么算法的总体时间复杂度是 $O(n^2)$。

c) 通过 a) b) 看出，算法的整体时间复杂度要么存在于 $O(n^2)$ 与 $O(n^3)$ 之间，要么仍处于 $O(n^3)$。然而对于后者，每增加一个环路，算法的遍历次数有所下降，并且在算法执行的过程中，大多数路由都是成对脱落。基于这两点因素，即便算法的深度优先遍历次数的时间复杂度仍处于 $O(n)$，但很大程度上提高了收敛速度，因此同样具有良好的优越性。

事实上，网络中设备的变动、增加减少，或者线路逻辑上、物理上的断开，都会造成网络动荡，从而改变了网络的拓扑结构。这种情况下，路由需要重新计算，以保证达到路由的一致性。路由重新计算，即执行本文算法，在深度优先搜索过程中，随着遍历次数的增加，某些路由编号开始脱落，这样，后面就不必花费时间遍历这些路由了，很大程度上缩减了整个深度优先搜索的时间。以图 1 为例，最优禁位排列之后，就出现了路由 2 和 3 脱落的现象，那么在执行第一次深度优先搜索时，只需对路由 1、4 和 5，而不再需要对全部的路由进行算法。第一次优先搜索之后，路由 4 脱落，那么在执行第二次深度优先搜索时，只需对路由 1 和 5 执行算法。如果不引用路由脱落办法，整个深度优先搜索过程中，要对 1 号到 5 号路由遍历 2 次，共 10 次；引用路由脱落策略，第一次深度优先搜索遍历 1 号、4 号、5 号路由，第二次深度优先搜索遍历 1 号、5 号路由，仅需要 5 次，相比 10 次而言，大大提高了算法的收敛速度，这在实际复杂多变的网络结构中具有较强的适应性。

### 3.4 本文算法较之 Dijkstra 算法的主要优越性

Dijkstra 算法是基于路径代价的一种算法，而本文算法是基于消息直接互传的一种算法。本文算法抛开了路径代价，省略了路径之间的代价加和，引入了禁位排列，将路由虚拟编号，进行多次禁位排列，在每次排列当中，路由都是直接交互的，从而简化了算法的形式。

## 4 结束语

路由决策是当前网络消息互传的关键技术，一个好的路由决策算法能够很快地使网络消息达到一致性。本文从数学原理中的禁位排列问题出发，将排列数看做网络拓扑中的路由。路由在网络中进行信息交换，等同于排列数在各个禁位排列之后的不断变化。这种基于禁位排列的路由决策算法能够满足网络的基本需求，较快地使网络链路状态达到一致。

然而，由于本文算法是一个全新的算法，因此有些问题一时半会尚未得到解决，如兼并考虑模式 1 和 2 两种禁位排列时，其满足条件的排列数是多少。笔者查阅了大量的文献资料，并没有现成的理论支持，因此只是通过编程实现而并未给出相关的数学证明。另外，虽然从理论上说明了算法的时间复杂度存在于 $O(n^2)$ 和 $O(n^3)$ 之间，但毕竟对多链状态的仿真实验做得不够充分。在以后的工作中，笔者将沿着这两个方向继续探究，找到某个阈值范围内的路由排列链路数，使得该算法的时间复杂度低于 Dijkstra 算法的时间复杂度。

**参考文献：**


[1] 谢希仁. 计算机网络[M]. 5 版. 北京：电子工业出版社，2008：144-156.

[2] 彭中君，魏永林. 基于无线自组网的多接口路由协议[J]. 计算机工程与应用，2010，46(19)：113-116.

[3] 徐佳，王汝传. 基于效用的容迟网络路由技术研究[J]. 计算机研究与发展，2011，28(4)：1211-1215.

[4] 岐世峰，李艳华，梅大成. 蚁群算法在 QoS 单播路由中的应用研究[J]. 电子科技大学学报，2010，39(2)：271-274.

[5] 胥小波，郑康锋. 基于并行 BP 神经网络实现的路由查找算法[J]. 通信学报，2012，33(2)：61-67.

[6] 孙侠，殷志祥. 全错位排列问题的基于芯片的 DNA 计算模型[J]. 大学数学，2010，26(5)：79-81.

[7] 李三燕，徐允庆. 二重错排与拉丁矩的计数[J]. 宁波大学学报：理工版，2011，24(2)：51-55.

[8] GOBJAKA H，BREITHART Y. Discovering network topology of large multisubnet Ethernet networks[C]//Proc of IEEE INFOCOM. 2007：428-434.

[9] 李琼琳. 容斥原理及应用[J]. 中国科技信息，2012，20(8)：58-59.

[10] GOLDA A F，ARIDHA S，ELAKKIYA D. Algorithmic agent for effective mobile robot navigation in an unknown environment[C]//Proc of International Conference on Intelligent Agent & Multi-Agent Systems. 2009：1-14.

[11] 张德富，彭煜，张丽丽. 求解三维装箱问题的多层启发式搜索算法[J]. 计算机学报，2012，35(12)：2553-2560.


(上接第 256 页)


[8] WANG Jiong，MEDIDI S. Topology control for reliable sensor-to-sink data transport in sensor networks[C]//Proc of IEEE International Conference on Communications. Piscataway：IEEE Press，2008：3215-3219.

[9] 徐强，汪芸. 容错节能无线 WSN 中可靠覆盖问题的解决方案[J]. 软件学报，2006，17(11)：184-191.

[10] 李小龙，林亚平，易叶青，等. 传感器网络中基于虚拟坐标的节点调度方案[J]. 软件学报，2008，19(8)：2089-2101.

[11] YIN Zhen-yu，ZHAO Hai，LIN Kai，*et al*. A coverage-preserving node scheduling scheme based on trust selection model in wireless sensor networks[C]//Proc of the 1st International Symposium on Pervasive Computing and Applications. Piscataway：IEEE Press，2006：696-698.

[12] GANERIWAL S，SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks[C]//Proc of the 2nd ACM Workshop on Security of Ad hoc and Sensor Network. New York：ACM Press，2004：66-77.

[13] SHAIKH R A，JAMEEL H，D' AURIOL B J，*et al*. Group-based trust management scheme for clustered wireless sensor networks[J]. IEEE Trans on Parallel and Distributed Systems，2009，20(11)：1698-1712.

[14] HO J W. Zone-based trust management in sensor networks[C]//Proc of IEEE International Conference on Pervasive Computing and Communications. Piscataway：IEEE Press，2009：1-2.

[15] TIAN D，GEORGANAS N D. A node scheduling scheme for energy conservation in large wireless sensor networks[J]. Wireless Communications and Mobile Computing，2003，3(2)：271-290.