基于梯度和能量捕获的无线传感网路由协议研究

郑志蕴 郭 芳 王振飞 张行进 王 飞
(郑州大学信息工程学院 郑州 450001)

摘 要 为解决无线传感网分簇协议中出现的节点能量消耗不均衡的问题,提出一种新的基于梯度和能量捕获的分布式无线传感网路由协议EGRP。该协议引入了距离梯度和能量捕获技术,在成簇阶段,以节点自身剩余能量、邻居节点平均剩余能量、节点距离梯度为参数构建成簇策略;在转发阶段,以簇头剩余能量和簇头梯度为参数构建簇间转发策略。理论推导与仿真实验结果均表明,EGRP协议的优化效果达到了预期,使单个节点的能耗下降10.9%,不同节点间的能耗更加均衡,从而延长了网络的生命周期。

关键词 无线传感网,分簇,距离梯度,能量捕获,路由协议
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.09.023

Research on Routing Protocol Based on Gradient and Energy Awareness in Wireless Sensor Networks

ZHENG Zhi-yun GUO Fang WANG Zhen-fei ZHANG Xing-jin WANG Fei
(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

Abstract To solve the problem of unbalanced energy consumption of wireless sensor network nodes, a new distributed routing protocol based on gradient and energy awareness (EGRP) was proposed. EGRP introduces 3 parameters to form clusters: the residual energy of the node itself, its distance gradient, and the average residual energy of its neighbors. Then according to inner cluster head's residual energy and distance gradient, every outer cluster head chooses one inner as the forward routing to build the routing tree. Theoretical derivation and simulation results show that EGRP can achieve ideal optimal effect, and it reduces single node's energy consumption by 10.9%, improves the balance of energy consumption between different nodes, and prolongs network's lifetime.

Keywords Wireless sensor network, Clustering, Distance gradient, Energy awareness, Routing protocol

1 引言

随着物联网被列入国家战略性新兴产业以及"感知中国"口号逐渐深入人心,无线传感网(Wireless Sensor Network, WSN)作为一种有效的信息获取和处理模式,在军事侦查、环境监测、智慧农业、抢险救灾和医疗救护等各个领域中得到广泛应用。由于传感器节点通常采用电池供电,不能得到及时补充或更换,其能量、通讯距离、计算和存储能力有限,因此如何设计高效的路由协议使得在保证数据传输质量的情况下尽可能减小能耗、延长网络生命周期成为国内外备受关注的研究热点[1]。分簇路由具有拓扑管理方便、能量利用高效、数据融合简单等优点,成为当前重点研究的路由技术[2]。

在簇结构生成方面,在LEACH协议[3]中提出了第一个经典的基于均匀分簇的路由算法。该协议将网络划分为大小均等的簇,在每个轮次开始时随机选择簇头,运行过程中不断循环执行簇的重构过程,但LEACH没有考虑能耗均衡问题[4]。文献[5]对LEACH进行改进,根据节点剩余能量来选择簇头,但不能保证簇头的负载均衡。文献[6]通过考虑节点剩余能量、节点间距离和簇内节点个数来选择簇头,并使用遗传算法优化分簇策略,但算法复杂度较高。文献[7]首次提出固定簇半径的分簇协议HEED,综合节点剩余能量和簇内通信代价来产生簇头。针对网络中簇头节点单位时间内能耗过大的问题,文献[8-9]通过不同的非均匀分簇策略来调节簇半径的大小以实现能耗均衡。文献[10]提出一种基于元胞自动机的非分簇拓扑控制算法,通过牺牲小部分拓扑联通度和覆盖度来换取更长的系统生存时间,但网络扩展性不强,其不适合大型网络。

在簇间数据传输方面,文献[11]将路径的跳数和节点剩余能量引入路径关键能量比的计算中,但未考虑节点间距离和数据传输的方向性。文献[12]利用网络的层次性和非均匀分区思想提出基于动态分区的非均匀分簇路由协议UCDP,但在路径建立时,簇内节点与簇头和簇头与簇头之间的通信

到稿日期:2016-08-30 返修日期:2016-12-12 本文受河南省科技攻关项目(142102310531,162102310616)资助。
郑志蕴(1962-),女,博士,教授,CCF会员,主要研究方向为大数据、分布式计算;郭 芳(1992-),女,硕士生,主要研究方向为无线传感网和智能信息处理;王振飞(1973-),男,博士,副教授,CCF会员,主要研究方向为移动计算、传感器网络技术;张行进(1973-),男,博士,讲师,主要研究方向为大数据、机器学习;王 飞(1987-),男,硕士,主要研究方向为无线传感器网络,E-mail:iewangfei@126.com(通信作者)。

代价较大。文献[13]针对分簇传感器网络，提出一种求解最佳簇数的计算方法。文献[14]将协同进化思想引入到路由协议中，采用多路径数据分流策略，提出基于节点邻域空间划分的负载均衡路由算法 LRDNS。文献[15]基于目的节点的期望传输次数提出一种新的能量潜能机会路由算法，但其在节点能量变化时很难自适应。

以上协议针对降低节点能耗、促进网络负载均衡给出了不同的解决策略，但是都没有通过节点位置、剩余能量、簇间转发相协作的方式建立路由。本文引入距离梯度，利用能量捕获技术，提出一种基于梯度和能量捕获的分布式路由协议(Energy awareness and Gradient optimized Routing Protocol，EGRP)。EGRP 协议以节点自身剩余能量和邻居节点平均剩余能量为主要参数，以节点所处的距离梯度为辅助参数进行节点分簇和簇间数据转发。它不仅考虑了节点到基站的方向和距离，而且对网络中的能量变化进行实时感知，在不同簇之间形成转发路由，从而有效解决了网络中心“热区”问题，延长网络生命周期。

2 网络模型

本文假设 N 个无线传感器节点随机均匀分布在 $m\times m$ 的正方形检测区域 S 内，并假设该网络具有如下特性：

1)传感器网络为高密度均匀分布的静态网络，传感器节点部署后不再移动，具有唯一的网络标识 ID，所有节点时间同步。

2)网络中只存在一个基站标记为 sink，基站位置一旦确定后不可移动；基站能量无限大，距离梯度为 0。

3)节点能量不可补充，不能获知自身位置信息，但可以根据接收信号强度计算相对距离，节点的通信半径可以在合理的范围内根据需要进行调整。

本文参考文献[3]的能耗模型：根据距离阈值 d_0 的不同，在距离 d 上传输 $k$bit 信息时，发送能耗为：

$$E_{Tx}(k,d)=E_{Tx\text{-}elec}(k)+E_{Tx\text{-}amp}(k,d)=\begin{cases}kE_{elec}+k\varepsilon_{fs}d^2, & d<d_0\\ kE_{elec}+k\varepsilon_{mp}d^4, & d\geqslant d_0\end{cases}\tag{1}$$

接收能耗为：

$$E_{Rx}(k)=E_{Rx\text{-}elec}(k)=kE_{elec}\tag{2}$$

其中，

$$E_{Tx\text{-}elec}(k)=E_{Rx\text{-}elec}(k)=kE_{elec}\tag{3}$$

阈值 d_0 的计算公式为：

$$d_0=\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}\tag{4}$$

其中，kE_{elec} 为无线电路发送或接收 $k$bit 数据消耗的能量；ε_{fs} 和 ε_{mp} 分别为自由空间模型和双线地面反射模型的信号衰减因子；当收发节点之间的距离小于阈值 d_0 时，无线信号传播采用自由空间模型，信号能量衰减与距离的平方成正比；当收发节点之间的距离大于或等于阈值 d_0 时，无线信号传播采用双线地面反射模型，信号能量衰减与距离的四次方成正比。

3 基于距离梯度的能量捕获路由协议

3.1 协议架构

EGRP 协议按轮次运行，工作流程可分为 4 个阶段：梯度标记阶段、成簇阶段、转发路由建立阶段、数据传输阶段。运行流程如图 1 所示。

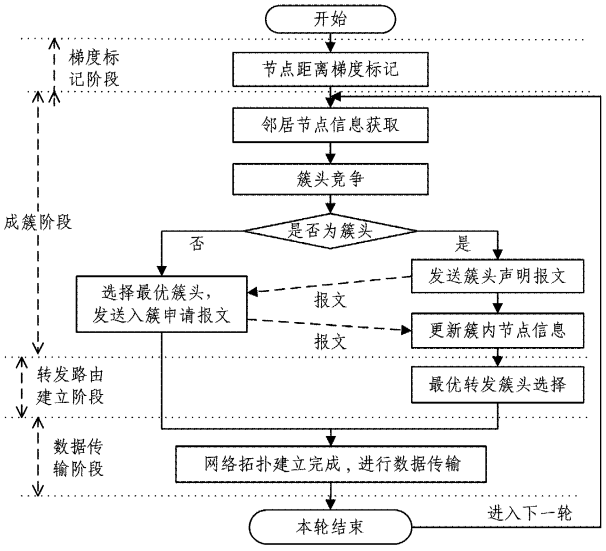

图 1 EGRP 协议运行流程图

首先根据节点到基站的距离划分距离梯度，然后按照轮次循环执行成簇阶段、转发路由建立阶段和数据传输阶段。在每一轮次过程中，在成簇阶段，各个节点根据策略进行簇头竞争和节点入簇；在转发路由建立阶段，各簇头根据距离梯度和剩余能量选择下一跳转发簇头，构建路由树。转发路由确定之后，则完成对本轮整个网络的数据传输拓扑结构的构建，网络进入一段时间的稳定期，各个传感器节点将本轮采集到的数据按照构建好的路由进行汇聚和转发，最终送达基站，本轮结束。然后自动进入下一轮，迭代执行上述 3 个阶段直到网络失效。下面将对 EGRP 协议进行详细描述。

3.2 节点数据结构和报文设置

EGRP 对传感器节点的数据结构的定义如表 1 所列，对协议工作过程中的各类报文的定义如表 2 所列。

表 1 节点数据结构

Parameter	Description
ID	The id set of WSN, ID={1,2,…,N}.
IE	(Initial Energy) Define the initial energy of every node.
RE	(Residual Energy) Define how much energy the node left.
AE	(Average Energy) Define the average energy of neighbor nodes.
DG	(Distance Gradient) Define the distance gradient of node, default value is 0.
TN	(Total Number of Nodes) If it's cluster head, TN defines how many nodes this cluster contains; default value is 1.
NS	(Node State) Define if the node has been chosen as a header this round, default value is IS(Initial State), CS means it's a cluster header, and MS means a member node.
NL	(Neighbor Nodes List) Define the first pointer of the list storing all the neighbor nodes' information which including their ID, RE, DG and NS.
NR	(Next Route) Define the next route of the node.

表 2　消息报文参数及作用描述

Message Type	Parameter	Description
Gradient_Msg	DG	Sent by the base station, is used to define each node's gradient.
Broadcast_Msg	ID, DG, RE, NS	Sent by each node, to broadcast their attribute information to neighbor node. s.
Head_Msg	ID, DG, RE, NS	Send by the chosen cluster head, to tell its neighbors it is a cluster header.
Join_Msg	ID, NS	Member nodes send Join_Msg to the cluster header, to join this cluster.
Forward_Msg	ID, RE, DG, TN	Sent between cluster headers, is used to construct the forward routing.

3.3　梯度标记阶段

在节点距离梯度标记阶段，基站依次以 HR_0 为半径广播 Gradient_Msg 报文（其中 R_0 是成簇半径；H 是距离梯度值，取值是区间$\lfloor 1, |0.5+\sqrt{2}M/2R_0| \rfloor$上的整数递增序列）。节点收到 Gradient_Msg 报文后，查询本节点的 DG 值，如果是默认值 0，则修改 DG 为报文中对应的 H 值；否则，忽略本次 Gradient_Msg 报文。基站依次发送完 Gradient_Msg 报文后，所有节点的距离梯度标记完毕；然后对网络中的节点进行时间同步，以保证所有节点同时开始执行后续的各个阶段。

3.4　成簇阶段

本阶段包含 3 项子任务：邻居节点的信息获取、簇头竞争和节点入簇选择，对应的时间段长度分别是：T_{NA}，T_{HC} 和 T_{CS}，三者的值根据网络规模提前给定。

(1)邻居节点的信息获取

各节点以 R_0 为半径广播 Broadcast_Msg 报文，将自身 ID、所处梯度和剩余能量等信息发送给邻居节点。邻居节点收到该报文后首先查询自身邻居节点信息表 NL 中是否包含该节点，若不包含，则先添加该节点为邻居，然后记录该节点的属性信息；若已包含该节点，则只更新表中该节点的信息。所有节点的邻居表 NL 在 T_{NA} 时段内建立完毕，进入簇头竞争阶段。

(2) 簇头竞争

所有节点计算邻居节点的平均剩余能量 AE，按照式(5)计算自身发送簇头声明报文 Head_Msg 所需的等待时长 T：

$$\begin{cases} T=t_1=\dfrac{AE}{RE}\times\dfrac{1}{DG+1}\times T_{HC}\times\rho, & RE>AE \\ T=t_2=\dfrac{T_{HC}}{2}+(1-\dfrac{RE}{IE})\times\dfrac{T_{HC}}{2}\times\rho, & RE\leqslant AE \end{cases} \tag{5}$$

其中，ρ 是均匀分布在[0.9,1]上的随机数，引入该随机数是为了避免两个节点具有相同的等待时长 T，以保证在任意时刻最多只有一个节点发送簇头声明。t_1，t_2 满足：$0<t_1<\dfrac{T_{HC}}{2}<t_2<T_{HC}$，在$[0,\dfrac{T_{HC}}{2}]$时间段内，大部分簇头将从梯度和剩余能量都比较合适的节点中选出；在$[\dfrac{T_{HC}}{2},T_{HC}]$时间段内，少量簇头将从尚未被簇头覆盖的空白区域和剩余能量较多的节点中选出；T_{HC} 时间段内簇头竞争完成。

在本节点的等待时长 T 结束之前，若收到其他节点发送的 Head_Msg 报文，则立即退出本轮簇头竞争。若 T 结束时仍未收到 Head_Msg 报文，则以 R_0 为半径广播 Head_Msg 报文，声明自己成为本轮簇头。

(3)节点入簇选择

当 T_{HC} 时间段结束时，本轮网络中的所有簇头已经诞生。被标记为 MS 的节点需要选择一个合适的簇头加入该簇。这一阶段的持续时间为 T_{CS}。

MS 节点首先按照式(6)计算周围所有簇头的 K 值。

$$K=\frac{CRE\times CDG}{CDG+1} \tag{6}$$

其中，CRE 为簇头节点剩余能量，CDG 为簇头节点所在梯度。

MS 节点选择邻居表中 K 值最大的簇头，向其发送入簇申请报文 Join_Msg，同时修改自身参数 NR 的值为该簇头 ID。当簇头收到发给自己的 Join_Msg 报文后，在邻居表 NL 中将对应节点的状态由 IS 改为成员状态 MS。至此，EGRP 协议成簇阶段完成，这一策略的伪代码如图 2 所示。

```
1. NS=IS
2. //Neighbor information Acquisition stage
3. every node broadcast Broadcast_Msg
4. receive Broadcast_Msg
5. update neighbor nodes list NL
6. //Head Competition stage
7. T=the delay time to broadcast Head_Msg
8. while (currentTime < THC){
9.    while (the delay time T is not run out){
10.      if (receive a Head_Msg from neighbor list NL[i]){
11.         NS=MS
12.         NL[i]. NS=CS
13.      }
14.      else continue
15.   }
16.   if (NS==IS){
17.      broadcast Head_Msg
18.      NS=CS
19.   }
20.}
21.//Cluster Selection stage
22.while (THC<currentTime<TCS){
23.   if (NS==MS && have not sended Join_Msg)
24.      send (Join_Msg to the max K cluster head)
25.   else
26.      receive (Join_Msg from its neighbor MS nodes)
27.}
```

图 2　EGRP 协议成簇策略的伪代码

3.5　转发路由建立阶段

EGRP 协议采用簇头间由外向内逐层转发的簇间路由策略。首先每个簇头（包括基站）以 $2R_0$ 为半径广播 Forward_Msg 报文，周围簇头收到后更新转发列表。所有簇头发送完毕后，按照如下 4 个原则在收到的簇头中选择一个最优的作为转发簇头，建立转发路由。

原则 1　只能选择 DG 小于自身值的内层簇头；

原则 2　存在多个小于自身 DG 值的簇头时，优先选择 DG 值最小的簇头；

原则 3　存在多个拥有最小 DG 值的簇头时，按照式(7)计算各个簇头的 h 值，选择 h 值最大的作为转发簇头。

$$h=\lambda CRE/TN \tag{7}$$

其中，CRE 为簇头剩余能量，TN 为簇内节点个数，λ 为转发修正因子，本文取值为 20。

原则 4　如果在 $2R_0$ 半径内找不到内层簇头，则簇头将直接与基站通信。

3.6 数据传输阶段

在该阶段，各个传感器节点持续工作，不断采集数据，并将数据按照协议生成的路由逐级转发，即先发送给簇头，簇头融合本簇内的数据后发送给下一跳转发簇头，以此类推，直至所有数据都传输到基站。本阶段的持续时长、传感器采集数据频率以及数据包的大小等需要根据网络的实际应用场景设定，本文不作具体限定。

4 EGRP 协议性能分析

与现有协议相比，EGRP 引入新的参数——距离梯度 DG，结合能量感知技术来改进传统的路由生成策略。

通过式(5)，构造等待时长 T 关于 AE 和 DG 的减函数，使得能量相同的情况下梯度大的节点更有可能当选簇头。通过式(6)，构造 K 关于 CRE 和 CDG 的增函数，使得距离基站较近的内层簇的规模相对较小，簇头的能量主要用来进行簇间数据转发；而距离基站较远的外层簇规模相对较大，簇头的能量主要用来进行簇内数据融合和发送，通过式(5)和式(6)可以实现内外层簇数量和规模的自适应变化，从而更简便地促进不同簇头节点的能耗均衡。

在转发路由建立阶段，EGRP 借助距离梯度 DG，以 4 个原则为基础构建一种新的簇间数据转发策略，可实现以下几个目标：1)数据每转发一次都更靠近基站；2)距离基站小于 $2R_0$ 的簇头直接向基站转发数据，进一步减少内层簇头的转发能耗；3)DG 值相同时，式(7)能够选出剩余能量更大或簇内节点更少的簇头来进行转发；4)在网络生命的中后期，部分节点和簇头能量耗尽，采用原则 4 可以尽可能地延缓网络失效时间，延长整个网络的生命周期。

与已有协议相比，EGRP 简单合理地控制了不同位置上簇的规模和簇间转发路径，更好地平衡了整个网络的能量能耗，有效地缓解了“网络中心热区”和内层节点死亡过快的问题。

5 实验仿真与结果分析

本文选择网络仿真方面的主流平台 OPNET 作为实验平台，仿真验证 EGRP 协议运行时的实际效果与理论分析的关系；并在相同条件下与成熟的 UCDP，LRDNS 作对比，验证 EGRP 协议的性能和效果。

5.1 仿真参数设置

本实验中对网络模型参数的设置如表 3 所列。

表 3 仿真参数设置

Parameter	Value	Parameter	Value
Network size	100m×100m	Sink position	(50m,100m)
Initial energy	2J	d_0	87.7m
ε_{mp}	0.0013pj/bit/m^4	E_{elec}	50nj/bit
E_{DA}	5nj/bit	ε_{fs}	100pj/bit/m^2
Node number	300	Cluster radius	20,25,30,35,40

在每一轮数据传输阶段，一个普通传感器节点一次发送的数据包长度为 250byte，其中控制信息数据占 36byte，一轮共发送 10 个数据包。

根据文献[11]，在网络模型和节点部署密度相同的条件下，无线传感器网络中实际产生的簇头数量的理论值的计算公式如式(8)所示，最优簇半径的计算公式如式(9)所示。

$$K_{\exp}=\frac{4S}{3\sqrt{3}R_0^2},K_{\max}=\frac{2\sqrt{3}S}{3R_0^2},K_{\min}=\frac{2\sqrt{3}S}{9R_0^2} \tag{8}$$

$$r_{opt}=2\sqrt[4]{\frac{2\pi S[(\alpha-1)E_{elec}+\alpha E_{DA}]}{27N\varepsilon_{fs}}} \tag{9}$$

其中，$K_{\exp}$ 为网络中簇头个数的理论期望值，$K_{\max}$ 为理论最大值，$K_{\min}$ 为理论最小值，R_0 为成簇半径，r_{opt} 为簇半径最优值，α 为每个簇头需要承担转发任务的外层簇个数的平均值，本文中设置 $\alpha=2$。

5.2 实验结果分析

5.2.1 簇半径对网络寿命的影响

为了更准确地衡量协议性能，对网络寿命选用两种不同定义：1)严格网络寿命(Strict Network Fife，SNL)，即网络中任一节点的能量耗尽时认为网络失效；2)宽松网络寿命(Loose Network Life，LNL)，即网络中一半节点能量耗尽时认为网络失效。

根据表 3 和式(9)，计算得到最佳簇半径的理论值 $r_{opt}=29.37$m。图 3 给出了在不同簇半径下，EGRP 协议遵循两种网络寿命定义得到的运行效果图。从图 3 中可以看出，当簇半径取值为 30m 时，网络寿命达到最大值 1300 轮和 952 轮，此时每轮中网络内部用于数据传输所消耗的能量最小。显然，这一实验结果较好地印证了理论值的分析结果。

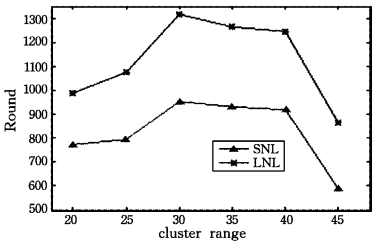

图 3 成簇半径和网络寿命关系图(300 nodes)

5.2.2 簇半径对簇头数量的影响

根据表 3 和式(8)，计算得到网络中簇头数量的理论值为 $K_{\exp}=8.55\approx9$，$K_{\max}=12.82\approx13$，$K_{\min}=4.27\approx5$。图 4 示出了簇半径 R_0 取最优值 30m 时 EGRP 运行过程中某一时段内簇头个数的统计结果。从图 4 中可以清楚地看出，在实际仿真中簇头数量 $K\in(9,11)$，与理论分析值完全相符。

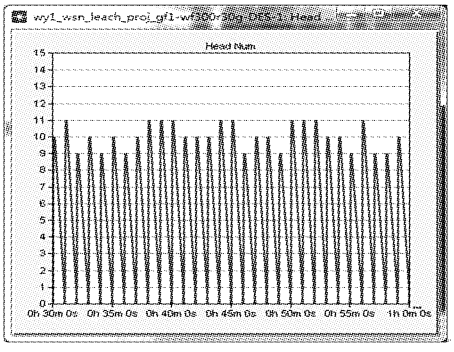

图 4 簇头数量统计图($R_0=30$m)

当协议运行稳定时，在不同簇半径下求取簇头数量的平均值，结果如图 5 所示。从图 5 中可以看出簇头的实际数量与理论值基本一致。随着簇半径的增大，簇与簇之间出现空白区域的可能性增大，为了保证网络全覆盖，空白区域中的节

点需要声明成为簇头，因此实际簇头数量要略大于理论分析值，并且两者的差距会随着簇半径的增大而增大。

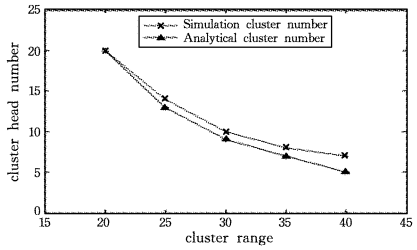

图 5　簇头数量理论值与实验值对比

5.2.3　EGRP 协议与其他协议的对比

在表 3 设置的仿真场景下，分别按照 EGRP，UCDP 和 LRDNS 协议的最佳簇半径进行多次仿真，选择每个协议的最佳运行状态进行对比，得到网络中存活节点数量的变化趋势，如图 6 所示。

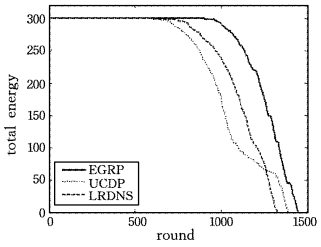

图 6　不同协议的网络寿命对比图

从图 6 可以看出，无论是严格网络寿命 SNL，还是宽松网络寿命 LNL，EGRP 协议的网络生存时间都要比 UCDP 和 LRDNS 协议长。从第一个节点的死亡时间来看，EGRP 出现在第 826 轮，而 LRDNS 和 UCDP 分别出现在第 745 和 701 轮，说明 EGRP 运行时单个节点的能量消耗更慢，分别下降了10.9%和17.8%；从节点全部死亡的时间来看，EGRP 与 UCDP 相差不大，都长于 LRDNS 协议，说明 EGRP 协议运行时网络的生存时间更长；从第一个节点死亡到全部节点死亡的持续时间来看，EGRP 协议的最短，说明 EGRP 运行时节点的能耗更均衡，更好地做到了所有节点“同生共死”。

网络中总能量的变化趋势如图 7 所示。

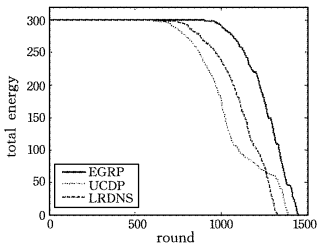

图 7　不同协议的网络中总能量对比图

从图 7 中可以看出，在 3 个协议的最佳运行状态下，EGRP 协议的网络中总能量一直明显高于 UCDP 和 LRDNS。在网络中没有节点死亡之前，EGRP 的总能量呈匀速下降趋势，说明每一轮次协议运行时的能耗大致均衡，且均小于 UCDP 和 LRDNS。当网络中存在死亡节点时，EGRP 的簇间转发策略避免了节点与基站的直接长距离通信，防止能量剧烈消耗而使节点过早死亡。总体来说，EGRP 协议在收敛性、网络生命周期和能量负载均衡方面优于其他两种协议。

结束语　本文针对分簇无线传感网协议中存在的节点能量消耗不均衡的问题进行研究，引入距离梯度和能量感知技术，提出一种新的基于梯度和能量捕获的分布式路由协议 EGRP。以节点自身剩余能量、邻居节点平均剩余能量和节点距离梯度为主要参数构建了成簇策略，以簇头剩余能量和簇头梯度为主要参数构建了簇间转发策略。仿真结果表明，本文提出的 EGRP 协议充分考虑了节点位置、实时剩余能量、网络能耗等因素，达到了理论预期的优化效果，能有效降低节点能量消耗，促进负载均衡，延长网络生命周期。

参 考 文 献

[1] DENG Y P, CHEN Z. Group clustering protocol based on energy balance for wireless sensor networks[J]. Journal of Computer Applications, 2011, 31(6): 1465-1468. (in Chinese)
邓亚平，陈铮. 能量负载均衡的无线传感网分组成簇协议[J]. 计算机应用，2011，31(6)：1465-1468.

[2] LV T. Research on Cluster-based Routing Protocol and Its Application for Wireless Sensor Networks[D]. Chengdu: University of Electronic Science and Technology, 2013. (in Chinese)
吕涛. 无线传感器网络分簇路由协议及其应用研究[D]. 成都：电子科技大学，2013.

[3] HEINZELMAN W R, CHANDRAKASAN A, BALAKRISHNAN H. Energy-Efficient communication protocol for wireless microsensor networks [C] // Proc. of the 33rd Hawaii Int'l Conf. on System Science (HICSS 2000). 2000: 3005-3014.

[4] CHEN H N, LIU G C, WU X G, et al. Clustering Protocol Based on Genetic Algorithm and Probabilistic Forwarding[J]. Computer Science, 2015, 42(3): 71-73. (in Chinese)
陈海南，刘广聪，吴晓鸽，等. 一种基于遗传算法与概率转发的分簇协议[J]. 计算机科学，2015，42(3)：71-73.

[5] KHEDIRI E S, NASRI N, WEI A, et al. A new approach for clustering in wireless sensors networks based on LEACH [C]// Proceedings of the International Workshop on Wireless Networks and Energy Saving Techniques, Amsterdam. Swedish: Procedia Computer Science, 2014: 1180-1185.

[6] SHOKOUHIFAR M, JALALI A. A new evolutionary based application specific routing protocol for clustered wireless sensor networks[J]. International Journal of Electronics and Communications, 2015, 69(1): 432-441.

[7] YOUNIS O, FAHMY S. Heed: A Hybrid, Energy Efficient, Distributed Clustering Approach for Ad-Hoc Sensor Networks[J]. IEEE Trans. on Mobile Computing, 2004, 3(4): 660-669.

[8] JIANG C J, SHI W R, TANG X L, et al. Energy Balanced Unequal Clustering Routing Protocol for Wireless Sensor Networks [J]. Journal of Software, 2012, 23(5): 1222-1232. (in Chinese)
蒋畅江，石为人，唐贤伦，等. 能量均衡的无线传感器网络非均匀分簇路由协议[J]. 软件学报，2012，23(5)：1222-1232.

[9] ZHANG R B, CAO J F. Uneven Clustering Routing Algorithm for Wireless Sensor Networks Based on Ant Colony Optimization[J]. Journal of Xi'an JiaoTong University, 2010, 44(6): 33-38. (in Chinese)
张荣博，曹建福. 利用蚁群优化的非均匀分簇无线传感器网络路由算法[J]. 西安交通大学报，2010，44(6)：33-38.

（下转第 147 页）

belle验证逻辑完整，不存在任何未证明的子目标。

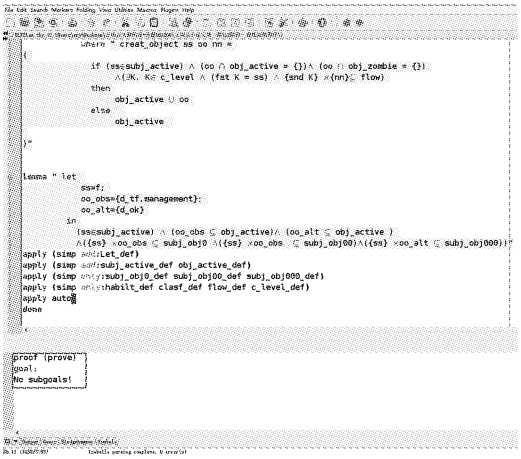

图 4　Isabelle 验证结果(二)

结束语　针对传统上依靠经验设计的安全网关缺乏严格安全模型的不足，本文提出了一种典型安全网关的形式化设计和证明方法。首先利用 BLP 模型对典型安全网关的安全策略进行形式化建模，然后使用定理证明器 Isabelle/HOL 对安全网关的功能规约和安全模型的一致性进行验证，保证了安全网关顶层设计的安全性。

本文仅给出了典型安全网关简化的逻辑结构，在项目的整个设计过程中，涉及到的模块有 20 多个，需要形式化证明的定理有 80 多条，通过采用形式化方法对其进行分析验证，避免了复杂情况下传统设计过程中人为错误的引入，增强了安全网关的可靠性。本文采用的 BLP 模型可以实现对安全网关及其功能模块的描述。接下来的工作将继续利用这种形式化设计和证明的方法对各个功能模块进行形式化设计和验证研究，最终得到采用形式化方法开发的典型安全网关。

参 考 文 献

[1] VIAPLANA A R. IpsecVPN[EB/OL]. [2017-4-10]. http://upcommons. upc. edu/handle/2099. 2/2117.

[2] PHIFER L. Tunnel Vision: Choosing a VPN-SSL VPN vs IPSec VPN[EB/OL]. http:/search security. techtarget. com/feature/Tunel-vision-Choosing-a-VPN-SLL-VPN-vs-IPSec-VPN.

[3] WU T, KUANG X H, FU Z L. Analysis and Suggestion of the Heartbleed [J]. National Defense Science & Technology, 2014, 35(5): 27-30. (in Chinese)
吴彤，匡兴华，傅中立. “心脏出血”漏洞的特点分析和对策建议[J]. 国防科技，2014，35(5)：27-30.

[4] BIEBER P. Formal techniques for an ITSEC-E4 secure gateway [C]// Computer Security Applications Conference, 1996. IEEE, 1996: 236-245.

[5] BELL D E, LAPADULA L J. Secure computer system: mathematical foundation: MTR2527 [R]. Belford: Mitrecorp, 1973.

[6] ABRIAL J R. Modeling in Event-B: System and Software Engineering[M]. Cambridge university Press, 2010.

[7] COMMUNITY E E. Information Technology Security Evaluation Criteria (ITSEC)[R]. Commission, 1990.

[8] 沈晴霓. 操作系统安全设计[M]. 北京：机械工业出版社，2013.

[9] BIBA K J. Integrity Considerations for Secure Computing Systems: Mitre Report MTR 3153[R]. Belford: Mitrecorp, 1975.

[10] DENNING D E. A lattice model of secure information flow[J]. Communications of the ACM, 1976, 16(5): 236-243.

[11] GOGUEN J A, MESEGUER J. Unwinding and Inference Control [C] // 1984 IEEE Symposium on Security and Privacy. IEEE, 1984: 75.

[12] NIPKOW T, PAULSON L C, WENZEL M. Isabelle/HOL: A proof assistant for higher-order logic[M]. Springer, 2002.

[13] CHAPMAN D B, ZWICKY E D. Building Internet firewalls [M]// O'Reilly & Associates, Inc., 1995.

[14] COMER D E. Internetworking with TCP/IP[M]. Beijing: Posts & Telecom Press, 2002.

(上接第 119 页)

[10] ZHANG W Z, LIU J, ZHANG L, et al. Non-cluster Based Topology Control Method in Wireless Sensor Networks[J]. Comptuer Science, 2010, 37(2): 44-47. (in Chinese)
张文铸，刘佳，张林，等. 无线传感器网络的非分簇拓扑控制方法研究[J]. 计算机科学，2010，37(2)：44-47.

[11] FAN Z P, XIE D Q, JIN Z Z. Energy-efficient and load-balancing multipath routing scheme for wireless sensor networks[J]. Journal of Chinese Computer Systems, 2013, 34(2): 253-257. (in Chinese)
樊志平，谢冬青，金政哲. 无线传感网络能量有效负载均衡的多路径路由策略[J]. 小型微型计算机系统，2013，34(2)：253-257.

[12] SUN Y Q, PENG J, LIU T, et al. Uneven clustering routing protocol based on dynamic partition for wireless sensor network [J]. Journal on Communications, 2014, 35(1): 199-206. (in Chinese)
孙彦清，彭舰，刘唐，等. 基于动态分区的无线传感器网络非均匀成簇路由协议[J]. 通信学报，2014，35(1)：199-206.

[13] FENG C X, LIU Z, LUO Y S. Optimal Cluster Numbers in Clustered Wireless Sensor Networks[J]. Journal of Huazhong University of Science and Technology, 2013, 41(10): 49-53. (in Chinese)
冯成旭，刘忠，罗亚松. 分簇传感器网络中最佳簇数的研究[J]. 华中科技大学学报，2013，41(10)：49-53.

[14] REN X L, WANG C. Load-balancing Routing Protocol Based on Dividing Node Neighboring Space in Wireless Sensor Networks [J]. Journal of Chinese Computer Systems, 2016, 6(6): 1222-1227. (in Chinese)
任秀丽，王冲. 基于节点邻域空间划分的无线传感网负载均衡路由协议[J]. 小型微型计算机系统，2016，6(6)：1222-1227.

[15] TIAN X Z, XIAO Y. Algorithm of Opportunistic Routing Based on Energy Harvesting Wireless Sensor Networks[J]. Comptuer Science, 2016, 43(6A): 288-290. (in Chinese)
田贤忠，肖赟. 一种能量捕获无线传感网络机会路由算法[J]. 计算机科学，2016，43(6A)：288-290.