第42卷 第2期 西 安 交 通 大 学 学 报 Vol.42 №2
2008年2月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Feb. 2008

无线传感器网络低时延能量均衡安全路由

郑杰，屈玉贵，郭淑杰，赵保华
（中国科学技术大学电子工程与信息科学系，230027，合肥）

摘要：提出了一种能量均衡的安全路由机制(LDEESR)，适用于周期性数据收集的传感器网络. LDEESR采用一种动态路由选择算法，该算法基于节点权值和高度值建立起一棵动态汇聚树，并利用类似于令牌传递的方式来选取树根，同时还用对称和非对称加密机制来保障路由的安全. 在这种机制下，LDEESR能够以很低的开销组织网络中所有的节点，健壮网络拓扑，防范多种攻击. 通过与基于群体的传感网络以及混合式高能效分布式聚类协议的仿真比较表明，LDEESR可降低和均衡所有节点的能耗，减小汇聚时延，延长网络的生命期.

关键词：无线传感器网络；能量均衡；安全路由；动态汇聚树；时延
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2008)02-0161-05

Low Delay Energy Equalizing Secure Routing in Wireless Sensor Networks

ZHENG Jie, QU Yugui, GUO Shujie, ZHAO Baohua
(Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230027, China)

Abstract: A low delay energy equalizing secure routing scheme (LDEESR) that is suitable for gathering data periodically in wireless sensor networks is proposed. LDEESR utilizes a dynamic route selecting algorithm based on weight-value and height-value of nodes to establish a dynamic gathered tree that is similar to the token passing to elect the root of the tree. LDEESR also uses symmetrical and asymmetrical encryption mechanisms to guarantee the routing security, under which LDEESR can organize all the nodes with low overhead and is perfectly robust against topology changes and many attacks. Simulation results show that compared with group-based sensor network (GSEN) and (hybrid, energy-efficient distributed (HEED), LDEESR can decrease and equalize the energy consume of all nodes, lessen data gathering delay, and extend the network lifetime as well.

Keywords: wireless sensor networks; energy equalizing; secure routing; dynamic gather tree; delay

无线传感器网络由大量能量受限且具有感知能力的传感器节点构成[1]，它是一种分布式自组织无线网络，部署后无需人为干预[2]，可广泛应用于环境监测、目标跟踪以及军事领域等[3].

充分地利用节点能源、尽量延长网络的生命期，是传感器网络研究的热点问题. 目前，很多基于簇和链的协议都是针对能量均衡这一问题提出来的，如：低能量自适应分簇(LEACH)协议[4]、混合式高能效分布式(HEED)聚类协议[5]，其每一个节点都以一定的概率成为簇头，簇头在每一轮需要进行轮换选举；传感信息系统高效聚类(PEGASIS)[6]协议、基于群体的传感网络(GSEN)协议[7]均采用链机制，其节点轮流充当汇聚点，以将数据发往基站. 又如，高效数据集中聚类协议(PEDAP)[8]并不适用

收稿日期：2007-05-23. 作者简介：郑杰(1982—)，男，博士生；赵保华(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60602016，60241004)；国家重点基础研究发展规划资助项目(2003CB314801)；国家高技术研究发展计划资助项目(2007AA01Z428)；华为基金资助项目(YJCB2006062WL，YJCB2007061WL).

于能量、计算能力受限制的分布式传感器网络.上述协议在构建网络拓扑和为基站收集数据时,要以牺牲时间延迟为代价,要么不考虑时延问题,而且均未涉及到路由安全问题.

本文针对上述协议问题,提出并验证了一种低时延的能量均衡安全路由协议(LDEESR),它通过时变动态树和多跳路由可灵活组织网络,同时基于对称和非对称加密机制来保障路由的安全.

1 系统模型与定义

1.1 网络模型

在一个由基站和100个随机分布于100 m×100 m区域的传感器节点组成的无线网络中,首先假定:①基站和节点放置后不再移动,基站位于节点监测区域以外;②每个节点均以大功率直接与基站通信;③所有节点是同构的,即具有相同的通信、处理能力和初始能量;④节点可以根据距离来调整发射功率,也可根据接收功率获知与邻居节点间的距离;⑤节点采用融合数据[9]以减少通信量.

另外,考虑到无线传感器网络的路由安全问题,本文基于静态密钥管理协议[10]和链路层加密算法,实现了节点认证和数据安全传输.

1.2 能耗模型

采用文献[7]中的模型来计算节点能耗,评估节点性能,其中节点的发射能耗为

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

接收能耗为

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

式(1)、式(2)中:$E_{elec}=50$ nJ/b为模块电路能耗;k表示数据的位数;d表示发射距离,d_0为阈值.假设无线信道是对称的,即对同一数据包,A将其发送到B的能耗与B将其发送到A的能耗是相同的.另外,数据融合也需要耗能E_{da}.

传感器网络可以建模为一个无向图$G=(N,L)$,其中N是传感器的节点集合,L是节点间通信链路集合.若$l(i,j)\in L$表示连接节点i和节点j的无线链路,节点i在一定发射功率下能直接与节点j通信,则称节点j为节点i的邻居节点.设每个节点初始化能量均为$E_i(t=t_0)=E_0$,则$E_i(\tau)$是节点i在τ时刻的能量.

定义1 衡量运行协议的网络在时刻τ的能量均衡性可采用网络能量均值

$$m_E(\tau)=\frac{\sum_{i=1}^{M}E_i(\tau)}{M} \tag{3}$$

和网络能量方差

$$D_E(\tau)=\frac{\sum_{i=1}^{M}\{E_i(\tau)-m_E(\tau)\}^2}{M} \tag{4}$$

式中:$M=|N|$是节点数.

在时刻t,具有较高的网络能量均值和较低的网络能量方差的协议则具有更好的能量均衡性能.

定义2 整个网络的生命期定义为

$$T_L=\min\{T_{Li}:i\in N\} \tag{5}$$

T_L也是首个节点的死亡时间.

定义3 在时刻τ由节点i到节点j的数据传送时延为

$$t_{Delay}(i,j;\tau)=\text{random}\{1,2,\cdots,N_{neighbor}(i,j;\tau)\} \tag{6}$$

式中:$N_{neighbor}(i,j;\tau)$为τ时刻节点i和节点j的公共邻居数.在每一轮的动态路由拓扑中,最长路径的链路时延可作为网络的数据汇聚时延.

2 能量均衡路由算法

LDEESR协议以轮为单位运行,它分为3个阶段:快速建立阶段、拓扑调整阶段和数据收集阶段.

2.1 快速建立阶段

LDEESR在初始建立阶段分下面3个步骤.

(1)发现邻居.所有节点以一个默认的功率(覆盖半径为d_{cr})将信息广播到其邻居节点,使邻居节点获得自己的ID,同时每个节点计算与邻居节点的间距和共享密钥,并将结果存入邻居表.

(2)发现基站.基站用一个能覆盖全网的已知功率发送“Hello”信息,节点就此可以估算出其到基站的距离,以便于与基站直接通信.

(3)建立初始树.首先,ID为1的节点向周围节点发起一种类似的受控泛洪,每个节点都有一个高度值H,初始时均为一个大整数$X(X>3M)$,用它标记路由方向,以避免出现环路.节点1的H值设为0,它在广播的初始树建立报文中含有$H=0$的信息.邻居节点收到报文后,将报文中的H值加3,并取之作为自己的H值,然后再向邻居广播,以此类推.注意:每个节点只在第一次收到这种建立报文时将该报文发送一次,但需监听邻居节点H值的变化,并根据这种变化调整自己的邻居表.由于信道是双向的,所以按发送和接收报文的顺序、按H值

的高低就可建立起以节点 1 为根的一棵树.

2.2　拓扑调整阶段

拓扑调整阶段是一个过渡阶段,拓扑调整过程由根节点(节点 1)发起,逐步扩展到叶子节点.

用搜索标记法可调整 H 值,有以下 2 种方法.

(1)被动标记法. 由初始化树根节点发起,寻找离自己最近的邻居节点 k 并发送标记信息,邻居节点 k 收到信息后将自己的 H 值在根节点的基础上加 1,并确立链路. 被标记的邻居节点 k 又可将标记信息发送给最近的子节点,以此类推.

(2)主动标记法. 当节点收到或旁听到邻居节点的 H 值发生变化时,重新比较与邻居节点之间的距离和 H 值,并选 H 值较低的且离自己最近的邻居节点作为父节点,同时更改自己的 H 值. 经一段时间之后,除了个别链路外,标记过程应完成,每个节点均选择了最近的发送链路,这样一棵近似的最小生成树建成.

2.3　数据收集阶段

在数据收集阶段,数据沿着动态拓扑周期性地发往 H 值最小的节点(新选出的根节点). 根节点将汇集到的数据直接转给基站,然后选出下一轮的根节点. 该阶段有以下要点.

(1)选择路由. 每一轮均从叶子节点开始收集数据,每个叶子节点先将感知到的外界信息进行初步处理,然后打包发送到其父节点,父节点应在 H 值低于自己的邻居节点中选择,选择权重 $w_{ij}(\tau)=E_j(\tau)/(2k_{ij}E_{\mathrm{elec}}+k_{ij}\xi_{\mathrm{fs}}d_{ij}^2)$,最终数据将汇聚到 H 值最低的根节点之上.

(2)选择根节点. 首轮根节点由 ID 为 1 的节点担当,根节点在将数据发往基站之后,选择邻居节点中剩余能量最大的节点 r 作为动态树的下一个根节点. 前一根节点可将消息发送给节点 r,告知节点 r 将作为下一个树根节点. 节点 r 在收到信息应修改自己的 H 值,即在当前根节点 H 值的基础上减 1.

(3)交互信息. LDEESR 采用 2 种方式进行邻居信息交互:捎带与旁听信息、周期性地广播信息. 前者是节点在发送数据时捎带着自己的 H 值和剩余能量信息,而邻居节点可以接收或旁听到这些信息(采用安全机制时无法旁听),后者则向邻居表示自己存在. 在节点收到更新报文之后,首先更新自己的邻居表,如果其父节点的 H 值发生变化,则应调整自己的 H 值,即在父节点 H 值的基础上加 1,由此根节点的 H 值不断减小,随着轮数(时间)的增加,将带动全网节点的 H 值不断减小.

(4)加入节点、应对失效. 节点间的通信是局部化的,所以 LDEESR 需应对节点的加入和失效. 加入的节点只要构建自己的邻居表即可运行 LDEESR 算法,失效的节点则经一段时间后将被邻居节点从各自的列表中删除即可.

在网络生命的末期,LDEESR 可采用以下措施维护网络:当邻居节点得知节点死亡信息时(由于得不到该节点的无周期性广播),就将死亡节点从自己的列表中删除. 当节点的所有邻居节点均死亡时,它将增大发射功率以进一步寻找邻居节点或直接与基站通信.

3　安全保证机制

3.1　节点密钥共享方案

本文利用文献[10]的 Blom 密钥预分布模型,在有限域 $F(q)$ 上形成对称的密钥对 $\boldsymbol{K}=\boldsymbol{A}\times\boldsymbol{G}$ 来定义所有节点之间的共享密钥对,每个节点 i 根据自己的编号拥有 $\boldsymbol{A}$ 的第 i 行和 $\boldsymbol{G}$ 的第 i 列. 在快速建立阶段,节点与其相邻的所有节点通过交换 $\boldsymbol{G}$ 的列,并按照矩阵乘法计算各自的密钥 $k_{i,j}$ 和 $k_{j,i}$,因为 $k_{i,j}=k_{j,i}$,所以可获得共享密钥 $k_{i,j}$. 在网络中,即使节点妥协或对网络安全性影响有限,节点 n ($n\neq i$, j)仍无法计算 $k_{i,j}$. 密钥共享方案见表 1.

表 1　密钥共享方案

密钥	密钥持有者	用途
K_{BS}	基站和所有节点	为基站广播的消息加密
K_i	基站和节点 i	保障节点-基站安全通信
$k_{i,j}$ 或 $k_{j,i}$	节点 i 或节点 j	保障节点 i、节点 j 安全通信

3.2　节点认证

当需加入新节点或失效节点再次被加入时,要对它们进行认证. 每个节点在部署前应分配一个私钥 K_1,K_1 对应的公钥由基站管理. 在数据通信之前,若需要进行身份认证,节点可从基站直接获取邻居节点的公钥 K_2,为认证时解密所用. 考虑到节点的计算能力,认证计算过程可由基站替代完成,此时节点需要与基站进行二次保密通信.

3.3　恶意节点防范

LDEESR 安全路由还包括保护汇聚树拓扑. 节点在广播时是无法进行加密的,为了防止恶意节点发布虚假信息(H 值或 $E_i(\tau)$),造成数据无法到达根节点,可以将广播改为多次单播或者采用 H 值或 $E_i(\tau)$ 预估机制. 根据 2.3 节所述机制,邻居节点的 H 值是单调不增的,即在每一轮 H 值最多减 1 或不

减，同样 $E_i(\tau)$ 也是不断减少，所以在节点中只需缓存2轮的 H 值，即可预估当前 H 值和剩余能量的范围. 对异常，可追加认证，这样就能抵御恶意节点通过增大 $E_i(\tau)$ 和减小 H 值来吸引邻居的数据流.

4 协议安全性能分析

采用动态树路由能够在节点受到攻击时改选路由，提高鲁棒性. 动态拓扑可使得攻击者难以把握和预测网络的运行状况，这也是一种反攻击机制. 基于安全保证机制，LDEESR 协议在收集阶段能抵御窃听、注入、篡改、重放、哄骗模仿等攻击，防范发布虚假路由信息、创建路由环、选择转发、Sybil 攻击、sinkhole 攻击，但不适用于 HELLO flood 攻击，因为网络模型②、④假设了节点需改变功率并利用信号强度估距. 对广播报文一般是无法进行加密的，所以广播时报文有可能被窃听、篡改，正常建立路由拓扑将受到影响，虽然可以采用邻居身份认证技术解决这一问题，但会增加报文的计算复杂度. 所以，消息加密将影响协议的运行效率.

安全机制可以保证网络的安全性，但对基站和节点的处理、存储能力要求很高，同时还影响到路由算法的性能. 节点需要存储 $\boldsymbol{A}$、$\boldsymbol{G}$ 矩阵的相关列、K_{BS}、K_i 以及私钥 K_1，邻居节点列表还需要加入通信共享密钥，所以加解密计算和认证通信需要时间，同时会增大节点能耗，甚至可缩短网络的生命期. 为此，安全机制仅为一个可选项，它取决于应用需求. 从上述分析看出，安全机制与路由算法有关，在设计时应充分考虑.

5 实验模拟及结果分析

用C++编写模拟程序，以分析、评估 LDEESR 协议的能效性能. LDEES 协议属于网络层协议，为了简单起见，假定 MAC 层协议是理想的且忽略信道差错，并在仿真中不加入安全机制. 同时，将 LDEESR 与 GSEN[7]、HEED[5] 进行比较（文献[7]中已经验证了 GSEN 算法的能效优于 PEGASIS[6] 和 LEACH[4]，同时它的平均数据汇聚时延仅为 PEGASIS 的 40%），以证明 LDEESR 的优势.

通过若干次随机节点分布场景的模拟实验得到平均抽样结果，并统计了节点在每一轮的能耗，计算了数据汇聚时延，记录了网络生命期. 模拟中所用密钥方案见表1，其中与能耗模型相关的参数与文献[7]相同. 数据和消息长度是协议在真实情况下估计所得. 节点初始能量 E_0 为 0.5 J，当节点剩余能量低于 0.002 J 时可认为节点死亡，其他参数如表2所示.

表2 仿真参数

基站位置/m	(50,150)	E_{elec}/nJ·b^{-1}	50
通信半径/m	20	ξ_{fs}/pJ·b^{-1}·m^{-2}	10
门限距离/m	75	ξ_{amp}/pJ·b^{-1}·m^{-4}	0.001 3
数据长度/b	4 000	消息长度/b	80

在仿真中，主要对网络生命期、网络能量、网络能量方差、每一轮的数据汇聚时延进行了评估. 图1给出了存活节点随时间变化的情况. 从中看出，由于 GSEN 中存在过长链路，所以第1个死亡节点较早出现，即 $T_L=510$ 轮. 与 GSEN 和 HEED 相比，LDEESR 的网络生命期（$T_L=883$ 轮）可分别提高 72%和34%，同时也验证了性质2. 在 HEED 中，所有节点都在 90 轮之间死亡，可见 HEED 节点的能耗较为平均，但高于 LDEESR. GSEN 的全部节点死亡时间持续了 500 轮，这是因为链式协议本身存有缺陷.

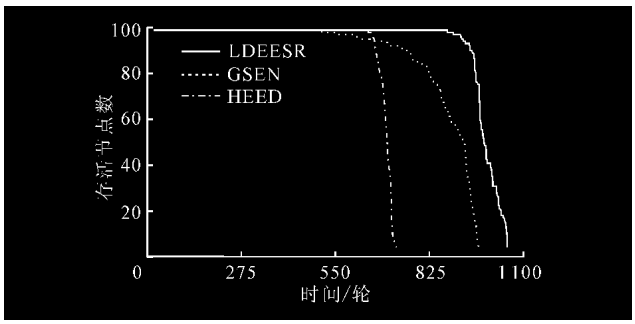

图1 不同协议的网络生命期

图2给出了3种协议的能量均衡性能比较. 从中可以看到，LDEESR 的网络能量均值高于 GSEN、HEED. 图3给出了3种协议能量方差随时间的变化情况. 从中看出，前 510 轮（未出现死亡节点），LDEESR 的能量方差低于 GSEN. 尽管 HEED 的能量方差最小，但它的能量均值（图2）下降得最快. 所以，LDEESR 的能量均衡性能最好.

图4描述了3种协议的数据汇聚时延的变化情况. 可以看到，LDEESR 的时延低于 GSEN（GSEN 的时延取决于最大组成员的数目 $G(\tau)$），它的平均时延是 46 轮，而 GSEN 是 68 轮，在时延性能上比 GSEN 平均提高了 32%，优势主要是其更适应节点随机分布的情况，而 GSEN 更适合于节点均匀分布

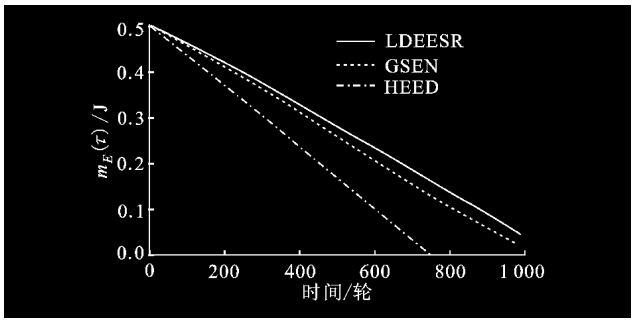

图 2　3 种协议的能量均值随时间的变化

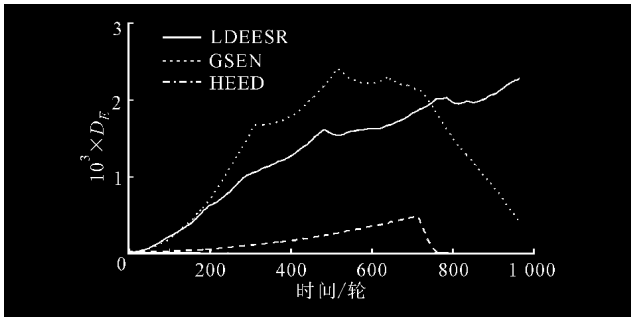

图 3　3 种协议的网络能量方差随时间的变化

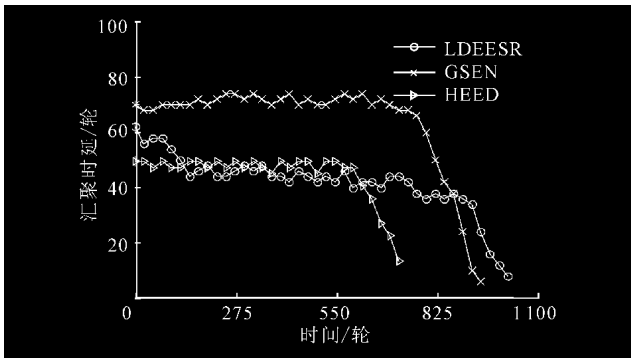

图 4　3 种协议的数据汇聚时延随时间的变化

的情况. HEED[5] 的时延主要由建簇时延和数据传输时延组成,取决于最大簇内的节点数目. 在仿真中,由于簇半径比较小, 所以图 4 中 HEED 的时延比较小,其平均时延为 48 轮, 但可以看出 LDEESR 仍有一定的优势.

6　结　论

本文提出了一种基于时变树拓扑的多跳动态安全路由机制,以用于低时延且能量均衡的情况. 本文提出的协议主要贡献有:①给出了能量均衡的定义,验证了基于树拓扑的优越性;②不需要节点的位置信息,也是一种易于实现的分布式算法;③所提时变动态树拓扑易于维护,能很好地延长网络的生命期;④针对路由算法特点有相应的安全保障机制.

由于协议实现简单, 所以 LDEESR 适用于快速建立网络拓扑和快速数据汇集. 下一步的工作是, 在考虑 MAC 层影响的情况下,评估协议的安全性能以及由安全机制带来的能耗问题.

参考文献:

[1] ESTRIN D, CULLER D, PISTER K, et al. Connecting the physical world with pervasive networks [J]. IEEE Pervasive Computing, 2002, 1(1):59 -69.

[2] ROMER K, MATTERN F. The design space of wireless sensor networks [J]. IEEE Wireless Communications, 2004,11(6):54-61.

[3] AKYILDIZ I F. A survey on sensor net-works [J]. IEEE Communications Magazine, 2002, 40(8):102-114.

[4] HEINZELMAN W, CHANDRAKASAN A, BALAKRISHNAN H. An application-specific protocol architecture for wireless microsensor networks [J]. IEEE Transactions on Wireless Communications, 2002,1(4):660 -670.

[5] YOUNIS O, FAHMY S. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks [J]. IEEE Transactions on Mobile Computing, 2004,3(4):660-669.

[6] LINDSEY S, RAGHAVENDRA C. PEGASIS: power-efficient gathering in sensor information systems [C] // Proceedings of IEEE Aerospace Conference. Piscataway, USA: IEEE,2002:1125-1130.

[7] TABASSUM N, URANO Y, HAQUE A. GSEN: an efficient energy consumption routing scheme for wireless sensor network [C]// International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies. Piscataway, USA: IEEE, 2006:117-122.

[8] TAN H O, KORPEOGLU I. Power efficient data gathering and aggregation in wireless sensor networks [J]. SIGMOD Record, 2003, 32(4):66-71.

[9] HALL D L, LINES J. An introduction to multisensor data fusion [J]. Proceedings of IEEE, 1997, 85(1):6-23.

[10] DU Wenliang, DENG Jing, HAN Y S, et al. A pairwise key pre-distribution scheme for wireless sensor networks [C]// Proceedings of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003:42-51.

(编辑　苗凌)