一种新的无线传感器网络层次型拓扑生成算法

李 捷[1] 吴志斌[1] 王汝传[2]

(河南大学计算机与信息工程学院 开封 475004)[1] (南京邮电大学计算机学院 南京 210003)

摘 要 拓扑控制是无线传感器网络(WSN)中最重要的技术之一。在对现有拓扑控制方法分析的基础上提出了一种基于能量预测与代理簇头的分簇方法,通过区分热区的分簇方式减轻了漏斗效应;提出了代理簇头的概念,实现了簇结构的局部更新维护并降低了簇头选举算法的复杂性;仿真结果表明基于能量预测的簇头轮换更好地提高了网络负载的均衡度。

关键词 非均匀分簇,能量预测,热区

Novell Hierarchy Topology Generation Algorithm of WSN

LI Jie[1] WU Zhi-bin[1] WANG Ru-chuan[2]

(College of Computer&Information Engineering, Henan University, Kaifeng 475004, China)[1]

(College of Computer, Nanjing University of Post and Telecommunication, Najing 210003, China)[2]

Abstract Topology control of wireless sensor networks is the focus study of wireless sensor networks application. Based on the analysis of existing topology control algorithm a dynamic clustering algorithm was proposed, which is based on energy forecast and agent-cluster-head. The clustering method characterized by distinguishing hot zones reduces the funnel effect in WSN; the introducing of agent-cluster-head not only makes the topology can be updated in partial area but also reduces the complexity of the cluster-head voting algorithm; the alternation of the cluster-head based on energy forecast balances the energy consumption of all sensor nodes.

Keywords Uneven clustering, Energy forecast, Hot zones

1 引言

由于无线传感器网络中节点的计算能力和通信能力十分有限,要求充分考虑网络资源的有限性、变化性,从而设计出优化的网络拓扑控制机制。目前基于分簇的层次型拓扑结构生成算法主要包括 LEACH [1],GAF[2],TopDisc[3]等。文献[1]证明了基于簇的层次型拓扑结构是能量更为有效的一种方式,同时文献[1]通过动态选举的簇头来平衡节点的能耗,但频繁的簇头选举引发的通信量耗费了能量且簇头的选举没有考虑节点的剩余能量。文献[2,3]在簇头选举时考虑了能量因素但算法实现复杂且需严格的时间同步[4]。由于 WSN 自身的特点使得靠近汇聚节点(sink)点区域内节点的通信负荷大,该区域称为热区[5],本文借鉴了 GAF 算法采用虚拟单元格分簇的思想,提出了热区与非热区不同单元格大小的非均匀分簇思想以解决热区问题,以此增加热区内簇的数量来平衡能量消耗,延长网络生命时间;为了实现在簇头选举中既考虑能量因素又不依赖严格的时间同步,本文引入了代理簇头的概念,通过随机选取的代理簇头来管理基于能量的簇头选举过程,从而可选出能量优先的簇头而不必有严格的时间同步;本文使 ARMA[6]模型对节点电量的预测结果参与到簇头轮换的决策过程中,使得簇头的轮换不在基于定时器策略,避免了频繁的簇头选举引发的通信量所带来的能量消耗。综上本文提出了 UCEF(Uneven Clustering and Energy Forecast)算法。

第 2 节介绍本文相关的约定与定义,第 3 节介绍电量预测使用的 ARMA 基本理论及其仿真效果分析,第 4 节是 UCEF 算法的设计,第 5 节是实验仿真,最后总结全文。

2 预备知识

定义 1 无线传感器网络可以表示成一个无向图 $G(V, E)$,V 为网络中的结点集,E 为各个结点间可能的边集。设 Sink 结点为 O,各个节点的通信半径相同且设为 R,图 G 是连通的。

定义 2 簇 S 定义为这样一个三元组 (t,m,n),且称 $H(t,m,n)$ 为簇 S 的簇名,对于任意的结点 $P \in V$,P 相对于 sink 结点的相对坐标为 (x,y),若存在 $P \in S$,也就是 $P \in (t,$

到稿日期:2008-08-16 返修日期:2009-04-10 本文受国家自然科学基金(60573141,60773041),国家高科技 863 项目(2007AA01Z404,2007AA01Z478),河南省重点攻关项目(082102210006),河南省高等学校青年骨干教师资助计划资助。

李 捷(1975—),男,博士,副教授,主要研究方向为网络管理、分布式计算、无线传感器网络,E-mail:jsjt9@henu.edu.cn;吴志斌(1983—),男,硕士研究生,主要研究方向为无线传感器网络;王汝传(1943—),男,教授,博士生导师,主要研究方向为计算机软件、计算机网络和网格、对等计算、信息安全、无线传感器网络等。

$m,n)$，当且仅当：

$$\begin{bmatrix} t \\ m \\ n \end{bmatrix}=\begin{cases} \begin{bmatrix} 1 \\ T(2x) \\ T(2y) \end{bmatrix} & |T(x)|+|T(y)|\leqslant GN \\ \begin{bmatrix} 0 \\ T(x) \\ T(y) \end{bmatrix} & |T(x)|+|T(y)|>GN \end{cases}$$

其中，$T(z)$为 z 的函数，$T(z)=\left\lceil \frac{z}{r} \right\rceil$ $\frac{\sqrt{2}}{4}R<r\leqslant\frac{R}{\sqrt{5}}$ $GN>0$

其中，r 为一个簇密度因子，决定簇密度的大小；GN 为热区规模因子，决定热区的大小。这里我们以 $t=1$ 表示该簇处于热区内，以 $t=0$ 表示该簇处于热区外。这种区分热区的分簇方法使在热区内的簇头数量增多一倍，提高了热区内网络的负载均衡度，从而缓解了热区问题。

定义 3 簇头集 HC 定义为无线传感器网 G 中所有簇头节点的全体。相邻簇头集定义为：若簇 S 的簇头节点为 A $(A\in HC)$，A 相对 sink 点的坐标为 (a,b) 则 $\forall B\in HC-\{A\}$ B 相对 sink 点的坐标为 (x,y) 这样一个集合 Q。

$$Q=\{B|\sqrt{(x-a)^2+(x-b)^2}<R\}$$

称为 A 的相邻簇头集，其中 R 为节点的通信半径。

定义 4 节点中包含的数据域如表 1 所列。

表 1 节点中包含的数据域

数据域	意义
簇名域	标识该节点所属的簇
节点状态域	节点当前处于的状态，状态值也代表了处于当前状态的节点在网络中所扮演的角色
代理簇头域	标识当前节点所属簇内代理簇头节点的信息(ID、能量水平、位置坐标)
簇头域	标识当前节点所属簇内簇头节点的信息(ID、能量水平、位置坐标)
邻居信息列表域	标识各个邻居所属簇的簇名，该簇簇头的坐标，该簇簇头节点的 ID，该簇簇头节点的能量水平，该簇代理簇头的坐标，该簇代理簇头节点的 ID，该簇代理簇头节点的能量水平。

定义 5 节点的状态分为 $\alpha,\beta,\gamma,\omega,\mu$，其意义如表 2 所列。

表 2 节点的状态和意义

状态	意义
α	处于该状态的节点说明是处于代理簇头的寻找期
β	处于该状态的节点已获知所属簇的代理簇头信息正进入簇头选举期
γ	处于该状态的节点已获知所属簇的代理簇头和簇头信息
ω	处于该状态的节点是所属簇的代理簇头
μ	处于该状态的节点是所属簇的簇头

3 基于 ARMA 的传感器节点电量预测

3.1 预测模型

假设某传感器节点历史能量序列为 $X_0',X_1',\cdots,X_i',\cdots,X_n'$，采用平稳化序列方法对 $X_0',X_1',\cdots,X_i',\cdots,X_n'$ 进行取对数后得到 $X_0,X_1,\cdots,X_i,\cdots,X_n$。

我们采用 ARMA(2,1)模型作为电量的预测模型

$$X_t-\varphi_1X_{t-1}-\varphi_2X_{t-2}=a_t-\theta_1a_{t-1}$$

我们利用逆函数法进行一步预测，记最小二乘法对模型参数 φ_1,φ_2 和 θ_1 的估计值为 $\hat{\varphi}_1,\hat{\varphi}_2$ 和 $\hat{\theta}_1$，ARMA 的逆函数记为 $I_1,I_2,\cdots,I_j$，有

$$I_j=\begin{cases} \hat{\varphi}_1-\hat{\theta}_1 & j=1 \\ \hat{\varphi}_2-I_1\hat{\theta}_1 & j=2 \\ I_{j-1}\hat{\theta}_1 & j\geqslant 3 \end{cases}$$

则一步预测模型为

$$\hat{X}_t(1)=\sum_{j=1}^{m}I_jX_{t+1-j}$$

其中 m 为 X_t 之前 m 次观测值，可根据预测精度的要求取值。

其多步预测模型为

$$\hat{X}_t(l)=\hat{\varphi}_1\hat{X}_t(l-1)+\hat{\varphi}_2\hat{X}_t(l-2)$$

3.2 仿真验证

对于一个 WSN 节点的实时电量消耗情况如图 1 所示，利用最小二乘法对其进行估计得模型估计值为 $\hat{\varphi}_1=0.7337$，$\hat{\varphi}_2=0.0234$，$\hat{\theta}_1=0.3761$，我们取 $m=3$ 得其一步预测模型为：

$$\hat{X}_t(1)=0.3576X_t-1.1109e{-}1X_{t-1}-4.178e{-}3X_{t-2}$$

多步预测模型：

$$\hat{X}_t(l)=0.7337\hat{X}_t(l-1)+0.0234\hat{X}_t(l-2)$$

其一步预测效果如图 2 所示。实验证明利用 ARMA 模型可以有效地对节点的能量消耗作实时的预测，我们考虑节点的未来能耗因素决定是否进行簇头的轮换，从而避免了定时器策略所带来的通信消耗，进一步地节省了节点能量，延长了网络的生存时间。

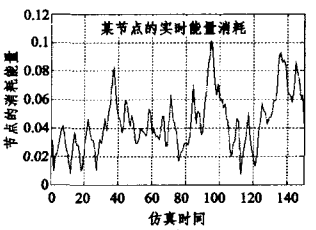

图 1 节点实时能量消耗

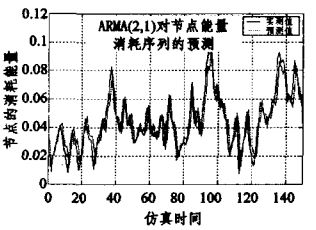

图 2 ARMA 对能耗的预测

4 UCEF 算法

4.1 簇组织结构生成

(1)初始化

对于网络 $G(V,E)$ 中的任意节点 $P\in V$，按照定义 2 分别计算自己所属的簇 (t,m,n)，并将自身状态置为“α”状态。

(2)代理簇头选举

在簇 (t,m,n) 中随机找出一个节点 A 来做代理簇头节点，A 将自身状态“α”改为“μ”，并且同时向本簇内发出数据包 $\mathrm{VgClusterH}_A(CName_A,E_A,ID_A)$，$\mathrm{CName}_x$ 为节点 X 所属簇的簇名，其中 E_x 表示节点 X 的能量水平，ID_x 是节点 X 的编号。节点在 α 状态下收到 $\mathrm{VgClusterH}_A$ 数据包即将自身状态改为“β”，同时以 $\mathrm{VgClusterH}_A$ 包中的信息替代自身代理簇头域信息。

(3)簇头选举

设 p 为 (t,m,n) 簇内任一成员在进入 β 状态后，连续向代理簇头 A 发送竞选簇头的数据包 $M_P(\mathrm{CName}_P,E_P,\mathrm{ID}_P)$，$A$ 在 μ 状态下若收到 M_P 信息即与自身簇头域信息中能量水平比较，若 M_P 中较大则以 M_P 中的信息来替换簇头域信息，

否则丢弃 M_P。A 向全簇广播竞选结果 ClusterH$_A$($CName_B$, E_B, ID_B),簇内成员在 β 状态下若收到 ClusterH$_A$ 数据包,则将其中的 ID_B 与自身 ID 比较,若一致则改自己状态为"ω",否则以 ClusterH$_A$ 信息替换簇头域信息,并改状态为"γ"。

(4)相邻簇头集确认

$\forall p \in V$ 若 p 在 ω 或者 μ 状态下且收到 ClusterH$_A$($CName_B$, E_B, ID_B)信息包,则根据定义 3 判断节点 B 即 $CName_B$ 是否在 p 的相邻簇头集 Q 内,若 $B \in Q$ 则将 ClusterH$_A$($CName_B$, E_B, ID_B)中的信息记录进 p 的邻居信息列表域中。

上述过程的状态转换图如图 3 所示。

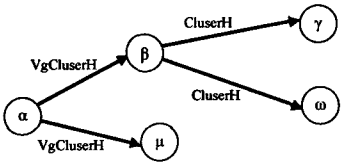

图 3 状态转换图

至此每个簇内都选出了一个簇头和一个代理簇头,且每个节点根据自身的状态信息就可以知道自己在网络中所扮演的角色:簇头节点的状态是 ω,代理簇头的状态是 μ,其余普通簇内成员的状态是 γ,且簇内的每个节点都已知道当前簇内的簇头和代理簇头的相关信息。在簇头的选举中由于有代理簇头的参与从而使得簇头的选举有了一个集中式的控制,由于代理簇头是随机选取的,使其成为分布式算法与集中式算法的揉合,从而不但避免了某些纯分布式的簇头选举算法需要严格的时间同步的问题,而且兼有分布式与集中式算法的优点。

4.2 簇组织结构维护

处在 ω 状态的簇头节点 A 将运行第 3 节介绍的 ARMA 预测算法,以时间 T_k 为时间间隔的历史能耗序列 X_t 为输入预测下一 T_{k+1} 时间能耗为 $\hat{X}_t(k+1)$。如果节点的剩余能量 $W-\hat{X}_t(k+1)<0$,则向簇内发送 RESET 数据包,簇成员收到 RESET 后即将自身状态改为 α,重新进行生成簇组织结构的步骤(3)和步骤(4)。

5 实验与仿真

本文采用 JSIM 仿真器在一个 1000×1000 区域内随机放置 400 个节点进行 UCEF 算法的仿真和实验。分别为 200 和 300 个节点网络的各节点分布、簇划分及网络连通性情况如图 4、图 5 所示。

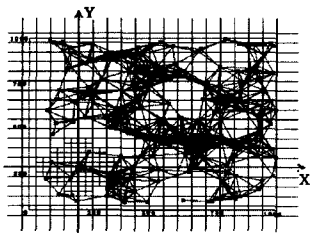

图 4 200 个节点的簇划分和连通性

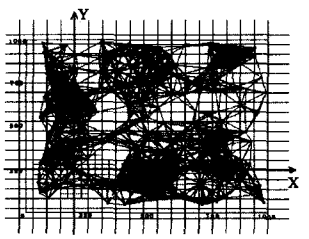

图 5 300 个节点的簇划分和连通性

这里,我们假定每个节点最初都具有 20 J 的初始能量,每个节点接收或发送数据需要消耗 0.001J / bit,且每个数据包的大小固定为 200 bit,所有节点一旦放置就不能再移动,节点死亡只发生在能量为零时,在簇头集上路由时使用 flooding 路由。我们使用两个 target 类型(可移动类型)的节点作为数据源,target 节点在仿真区域内随机移动触发数据转输事件。

图 6 给出了依文献[7]实现的 TEEN,LEACH 算法与本文提出的 UCEF 算法模型在上述设置下生存节点数随仿真时间的变化图,实验结果取自 20 次实验的平均值。结果表明 TEEN 比 LEACH 有更长的生存时间,主要是因为 TEEN 通过软硬门限减少了数据传输量,也较 LEACH 有更好的负载平衡性。UCEF 由于采用基于能量预测的机制,减少了由于簇重组带来的通信消耗而获得了更久的生存时间。

若定义网络的稠密度 DENS 为:$DENS=\frac{N}{A\times B}$,其中 N 表示在长为 A 宽为 B 的矩形仿真区域内布置的节点数,由图 7 给出的 UCEF 在不同网络规模下的生存时间结果可知 UCEF 在 DENS 越大的网络下其生存时间越长,因此 UCEF 更适合大型稠密型网络。

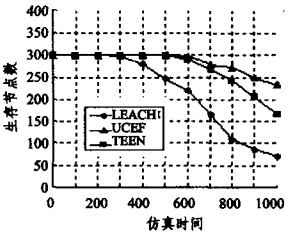

图 6 生存时间比较

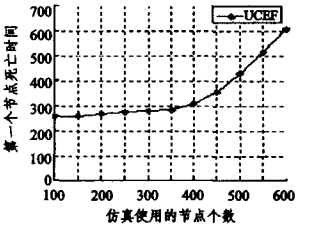

图 7 不同规模网络生存时间

结束语 综合考虑无线传感器网络中节点能量等资源的有限性和各节点能耗的不均衡性,本文提出了一种区分热区与非热区的非均匀分簇算法 UCEF。通过增加热区内的簇头数量的方法来提高热区内网络的负载均衡度从而缓解了热区问题;同时还提出了一种基于能量预测的簇头轮换机制,进一步提高了全网能量的负载均衡;每个簇通过增加一个代理簇头来监督簇头节点的工作状态和簇头轮换过程,实现了拓扑结构的局部更新和维护,节省了大量控制报文的开销。无线传感器网络拓扑控制算法还有很多工作值得去做,比如与拓扑结合的路由、功率控制等,这些也是我们正在深入研究的课题。

参 考 文 献

[1] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-Efficient communication protocol for wireless microsensor networks [C]// Proc. of the 33rd Annual Hawaii Int'l Conf. on System Sciences. Maui: IEEE Computer Society, 2000: 3005-3014

[2] Xu Y, Heidemann J, Estrin D. Geography-informed energy conservation for ad hoc routing[C]// Proc. 7th Annual Int'l Conf. on Mobile Computing and Networding. Rome, Italy, July 2001: 70-80

[3] Handy M J, Haase M, Timmermann D. Low energy adaptive clustering hierarchy with deterministic cluster-head selection[C]// Proc. of the 4th IEEE Conf. on Mobile and Wireless Communications Networks. Stockholm: IEEE Communications Society, 2002. 368-372. http://citeseer.ist.psu.edu/handy02low.html

(下转第 92 页)

ic-CBE。首先，由于使用了计算性能更好的 MAC 来代替 SOTS 方案作为组件，因此加/解密效率要优于方案 Generic-CBE；其次，密文长度也大大短于方案 Generic-CBE 的密文长度。方案 Generic-CBE'的密文由消息的密文和密文的消息认证码组成，而方案 Generic-CBE 的密文则由密文、密文的签名及签名的验证密钥组成。在具体实现中，方案 Generic-CBE'使用 CBC-MAC 来产生密文的消息认证码可以短至 128bit；而方案 Generic-CBE 在使用 BLS 短签名[13]的前提下，密文的签名也有 170bit 左右。但方案 Generic-CBE'的不足之处是无法在完全解密前对密文的有效性进行验证，即使密文是无效的。

最后，方案 Generic-CBE'的安全性有如下的结论：

定理 2 若方案 IBE 是 IND-ID-CCA 安全的、方案 PKE 是 IND-CCA2 安全的并且方案 MAC 是一个强一次性信息认证码，则方案 Generic-CBE'是 IND-CBE-CCA 安全的。

定理 2 的证明方法与定理 1 几乎相同。不同之处是需要将事件 Forge 定义为 IND-CBE-CCA 敌手 A 对$\langle \tau, id, upk, usk, C=\langle c, tag\rangle\rangle$ 作过解密查询，其中 $C=\langle c, tag\rangle$是有效的密文，$\langle c, tag\rangle \neq \langle c_{ch}, tag_{ch}\rangle$，并且 c 和 c_{ch} 解密后获得的 MAC 标记的验证密钥相同，即 $mk=mk_{ch}$。由 MAC 的抗一次性选择消息攻击安全性，Pr[Forge]显然是可忽略的。

结束语 由于基于一般密码学原型而非具体的代数假设，能够最大程度地保留其组件的优点，公钥密码体制的通用构造近年来得到了广泛的关注。本文以 IND-CCA2 安全的公钥加密方案、IND-ID-CCA 安全的基于身份的加密方案以及强一次性签名方案等密码学原型为组件提出了两个 CBE 方案的通用构造，并在标准模型下证明了其安全性。

下一步的工作主要是对本文的通用构造做一步改进，探讨是否存在对组件的安全性要求更低的通用构造，以期提出更高效的构造方案。此外，目前还未见有标准模型下安全可证的基于证书的签名方案的通用构造，因此这方面的研究也将是下一步的工作重点。

参 考 文 献

[1] Gentry C. Certificate-based Encryption and the Certificate Revocation Problem[C]// Proceedings, Advances in Cryptology-EUROCRYPT 2003. Warsaw, Poland, 2003

[2] Yum D H, Lee P J. Identity-based Cryptography in Public Key Management[C]// Proceedings, EuroPKI 2004. Samos Island, Greece, 2004

[3] Yum D H, Lee P J. Generic Construction of Certificateless Encryption[C]// Proceedings, EuroPKI2004 International Conference on Computational Science and Its Applications-ICCSA 2004. Assisi, Italy, 2004

[4] Al-Riyami S, Paterson K G. CBE from CL-PKE: A Generic Construction and Efficient Schemes[C]// Proceedings, Public Key Cryptography-PKC 2005. Les Diablerets, Switzerland, 2005

[5] Galindo D, Morillo P, Ràfols C. Breaking Yum and Lee Generic Constructions of Certificateless and Certificate-based Encryption Schemes[C]// Proceedings, EuroPKI 2006. Turin, Italy, 2006

[6] Kang B G, Park J H. Is It Possible to Have CBE from CL-PKE? Cryptology ePrint Archive[R]. 2005/431. http://eprint.iacr.org/, 2005

[7] Fujisaki E, Okamoto T. How to Enhance the Security of Public Key Encryption at Minimum Cost[C]// Proceedings, Public Key Cryptography-PKC'99. Kamakura, Japan, 1999

[8] Fujisaki E, Okamoto T. Secure Integration of Asymmetric and Symmetric Encryption Schemes[C]// Proceedings, Advances in Cryptology-CRYPTO'99. California, USA, 1999

[9] Bellare M, Rogaway P. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols[C]// Proceedings, ACM CCS 1993. Virginia, USA, 1993

[10] Bellare M, Desai A, Pointcheval D, et al. Relations Among Notions of Security for Public Key Encryption Schemes[C]// Proceedings, Advances in Cryptology-CRYPTO'98. California, USA, 1998

[11] Boneh D, Franklin M. Identity-based Encryption from the Weil Pairing[C]// Proceedings, Advances in Cryptology -CRYPTO 2001. California, USA, 2001

[12] Canetti R, Halevi S, Katz J. Chosen-ciphertext Security from Identity-based Encryption[C]// Proceedings, Advances in Cryptology-Eurocrypt 2004. Interlaken, Switzerland, 2004

[13] Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing[C]// Proceedings, Asiacrypt 2001. Gold Coast, Australia, 2001

[14] Boneh D, Katz J. Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity Based Encryption[C]// Proceedings, RSA — Cryptographers' Track 2005. California, USA, 2005

[15] Lu Yang, Li Jiguo, Xiao Junmo. Applying the Fujisaki-Okamoto Conversion to Certificate-based Encryption[C]// Proceedings, 2008 International Symposium on Electronic Commerce and Security-ISECS 2008. Guangdong, China, 2008

[16] Lu Yang, Li Jiguo, Xiao Junmo. Generic Construction of Certificate-based Encryption[C]// Proceedings, 9th International Conference for Young Computer Scientists-ICYCS 2008. Zhangjajie, China, 2008

(上接第 74 页)

[4] 张学，陆桑璐，等. 无线传感器网络的拓扑控制[J]. 软件学报，2007(4)：943-954

[5] 张重庆，李明禄，等. 数据收集传感器网络的负载平衡网络构建方法[J]. 软件学报，2007(5)：1110-1121

[6] 李捷，刘先省，韩志杰. 基于 ARMA 的无线传感器网络流量预测模型的研究[J]. 电子与信息学报，2007(5)：1224-1227

[7] Manjeshwar A, Agrawal D P. TEEN: A protocol for enhanced efficiency in wireless sensor networks[C]// Int'l Proc. of the 15th Parallel and Distributed Processing Symp. San Francisco: IEEE Computer Society, 2001: 2009-2015