

基于多轮分簇的无线传感器网络路由协议

曹建玲 陈永超 任 智 李晴阳

(重庆邮电大学移动通信技术重庆市重点实验室 重庆 400065)

摘 要 提出了一种基于多轮分簇的无线传感器网络路由协议 MCBMC(multi-round cluster based Multi-hop clustering routing protocol),它对 RBMC (ring based multi-hop clustering routing algorithm)进行了改进,在簇头选举中引入剩余能量参数,同时改单轮成簇为多轮成簇,减少了频繁分簇和重复建立多跳路由的次数。仿真结果表明,与 RBMC 相比,MCBMC 能够降低节点平均能耗,提高网络的寿命。

关键词 无线传感器网络,路由协议,多轮成簇

中图分类号 TP393.04 **文献标识码** A

Multi-round Cluster Based Multi-hop Clustering Routing Protocol for Wireless Sensor Networks

CAO Jian-ling CHEN Yong-chao REN Zhi LI Qing-yang

(Chongqing Key Lab of Mobile Communications Technology, Chongqing University of Post and Communications(CQUPT), Chongqing 400065, China)

Abstract A multi-round cluster based multi-hop clustering routing protocol (MCBMC) for wireless sensor networks (WSN) was proposed. It improves the RBMC protocol as follows: it adds a parameter of energy for the head node's election arithmetic, uses multi-round clustering instead of every round clustering, reduces frequent clustering and repetition to establish multi-hop routing. Finally, it is simulated on OPNET14.5, and the results are compared with LEACH and RBMC. The results show that MCBMC can reduce node energy consumption and improve the network lifetime.

Keywords Wireless sensor networks, Routing protocol, Multi-rounds clustering

随着微机电系统(Micro-Electro-Mechanism System, MEMS)、片上系统(System on Chip, SOC)、无线通信和低功耗嵌入式等技术的进一步发展,无线传感器网络(Wireless Sensor Networks, WSN)引起了人们的广泛关注。无线传感器网络是由部署在检测区内大量廉价的微型传感器节点组成的通过无线通信方式形成的一个多跳的自组织的网络系统,网络内的节点包括数据汇聚节点和传感器节点^[1]。传感器节点通常由电池供电,能量有限,且难以补充能量,因此传感器网络协议的首要设计目标就是要均衡地使用能量,延长网络的生存时间。

从网络拓扑结构的角度出发,传感器网络协议分为两类:平面路由协议和分簇路由协议。基于分簇的层次型无线传感器网络可以对资源进行平衡分配,具有拓扑管理方便、能量利用高效、数据融合简单等优点^[2],是近年来的研究中比较热门的路由协议。在分簇路由协议中,网络通常被划分为簇,网络中的节点被划分成为簇头节点和簇成员节点两类。簇头用于管理和协调整个簇内的成员节点之间的工作,负责簇内信息的收集和数据的融合处理以及向汇聚节点转发数据。由于簇头到汇聚点的距离一般较远,在簇头与汇聚点之间采用多跳通信方式,更有利于节约能量^[3]。然而这种方法带来了能量消耗不均衡的问题,簇头和汇聚点之间构成了“多对一”的数

据发送接收关系,靠近汇聚点的簇头由于需要转发其他簇头的数据而造成负载过重,能量过早耗尽,降低网络生存时间,此现象被称为“热区”问题^[4]。

1 相关工作

近年来,研究人员在分簇路由算法方面进行了大量的研究,提出了多种分簇协议和改进算法。Heinzelman 等人提出了 LEACH 协议^[5],LEACH 的操作是分轮进行的,每一轮又被分为两个阶段:创建阶段和稳定阶段。在簇建立阶段,一部分节点随机循环地成为簇头;在稳定数据传输阶段,传感器节点采集数据并传给簇头,簇头将数据融合后以单跳的通信方式发往汇聚点。Manjeshwar 等人提出的 TEEN 协议^[6]的基本原理是在 LEACH 协议中设置了软硬两个阈值,用以减少发送数据的次数。

Lindsey 等人提出的 PEGASIS 协议^[7]是将网络中的节点组织成链状,数据在链上经融合后,最后传输至汇聚点。Younis 等人提出的 HEED 协议^[8]是一种混合式分簇算法,该算法首先根据节点剩余能量来概率性地选取候选簇头,然后以簇内部通信代价的高低来竞争簇头。上述协议均是周期性地重新分簇,节点轮流担任簇头,达到了均衡簇成员节点能量消耗的目的,但是没有考虑簇头间的能量均衡问题。针对此

到稿日期:2012-09-27 返修日期:2013-01-29 本文受国家自然科学基金(60972068),教育部留学回国人员科研启动基金(2010-1561),重庆市教委科研项目(KJ120510),应急通信重庆市重点实验室开放课题(201201)资助。

曹建玲(1974-),女,博士生,讲师,主要研究方向为无线传感器网络路由协议,E-mail:caojl@cqupt.edu.cn。

问题,叶懋等人提出了 EECS 算法^[9];簇头与汇聚点之间仍采用单跳通信的方式,节点在选择簇头时考虑了簇头到汇聚点的距离远近,构造出了大小非均匀的簇,以均衡簇头的负担。

Soro 等人首次提出利用非均匀分簇的思想来解决多跳路由中的“热区”问题。李成法等人提出的非均匀分簇算法 EEUC^[10]是一种基于簇头竞争的分布式算法。候选簇头利用非均匀的竞争范围来构建大小不等的簇,靠近汇聚点的簇规模较小,可以节省部分簇内通信消耗的能量用于簇间的数据传送。EEUC 算法的簇头数比 LEACH 算法更稳定,能量消耗更均匀,网络的生命周期更长。EEUC 算法中用到了 4 个参数,文中没有给出参数的选取策略,需要进行人工选取,实际操作起来比较困难,算法性能难以达到最优。

刘志等提出的 RBMC 是一种分环多跳的路由协议^[11]。RBMC 算法通过在不同环中构建大小不同的簇来解决“热区”问题。不同的环使用不同的簇头选举概率 P ,从而使网络的分簇非均匀化,靠近汇聚节点的簇的规模较小,远离汇聚节点的簇的规模较大。外环的簇头收集数据后,通过内环的簇头转发数据,使多跳路由的生成协议变得简单、清晰。但 RBMC 簇头选举协议过于简单,和 LEACH 协议相同,并未考虑其他因素,极易造成簇头分布不均衡,使分环的效果降低。

2 MCBMC 分簇路由协议

2.1 网络模型

考虑一个由 K 个随机部署的传感器节点形成的大、中型网络,其应用场景为周期性的小规模数据收集(如温度、湿度等)。用 n_i 表示网络中的第 i 个节点,网络中所对应的无线传感器节点集合为 $N = \{n_1, n_2, \dots, n_k\}$, $|N| = K$ 。我们做如下假设:

(1) 汇聚节点位于圆形监测区域的正中央,采用 RBMC 分环的方式将网络分割成若干个同心圆环,圆环的中心为 sink,圆环的间距相同并设其为 σ ,单位为米(m)。

从汇聚节点向外将环区域分别编号为第 1 环,第 2 环, ..., 第 n 环。其中第 1 环中的传感器节点是可以直接与汇聚节点进行通信的。传感器节点在监测区域中的部署是随机的,传感器节点和汇聚节点在部署完成后均不再发生位置移动。

(2) 网络中的所有传感器节点都是同构的,并且同时具备数据融合的功能。每个传感器节点都拥有一个属于自己的唯一的标识(ID)。

(3) 每个节点事先知道自己的位置,发送节点可通过与接收节点之间的距离来调整发送功率,以便节能和降低干扰。

我们采用文献^[12]提出的传感器无线通信的能耗模型。如图 1 所示,发送端由发射电路和发送功率放大器两部分组成。

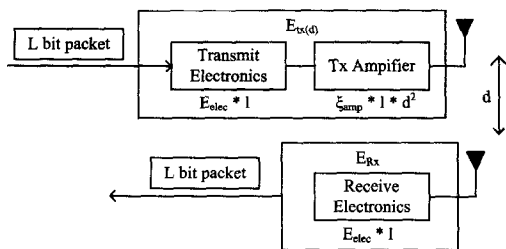


图 1 传感器无线电模型

发送端的能耗公式为:

$$E_{Tx}(l, d) = E_{Tx_elec}(l) + E_{Tx_amp}(l, d) \quad (1)$$

式中, l 为发送包的比特数, d 为发送机到接收机之间的距离。由于在无线信道中,电磁波的功率会随着接收机和发射机距离的增加而减弱,本文中我们采用自由空间和多路径衰减两种能耗模型。将两种模型代入式(1)得到:

$$E_{Tx}(l, d) = \begin{cases} lE_{dec} + l\epsilon_{fa}d^2, & d < d_0 \\ lE_{dec} + l\epsilon_{ma}d^4, & d \geq d_0 \end{cases} \quad (2)$$

式中, E_{dec} 表示发射机的电路损耗能量, d_0 表示选择两种模型的阈值,如果发射机和接收机之间的距离小于 d_0 ,功率放大器损耗采用自由空间模型;如果距离大于 d_0 ,则采用多路径衰减模型。 ϵ_{fa} 、 ϵ_{ma} 分别是两种能耗模型中功率放大器的能量因子。接收端没有功率放大器,接收机的电路损耗能量与发射机相同。

2.2 MCBMC 协议的执行过程

MCBMC 协议的执行步骤如下:

1) 当节点部署完成后,汇聚节点 sink 计算得到各环的最优初始簇头选举概率 $T = \{T_k | k \in 1, 2, \dots, n\}$,将每个环区域的簇头选举概率 T 、 δ 和汇聚节点 sink 的位置放入 SINK_NOTIFY 包中,并以一个固定的发送功率广播出去(此发送功率必需覆盖整个监测区域内的所有传感器节点)。

2) 区域中的任意一传感器节点 j 收到 SINK_NOTIFY 包后,计算自己与汇聚节点 sink 的位置 $d(POS_j, POS_{sink})$ ($d(\cdot)$ 为距离运算,取欧氏距离),再通过 δ 确定自己所在的环,最后从集合 T 中确定自己的簇头选举概率 T_k 。

3) 簇头自选:每个节点以均匀分布生成一个随机数,将其与所在环的簇头选举概率进行比较判决,确定是否在本轮中担任簇头。

4) 当选的簇头将随机向外发送 CH_NOTIFY 消息,其中包含该节点的 ID、簇头的位置和随机选择的一个扩频码,此时广播范围尽可能大(如 2δ),以使所有的非簇头节点及 $k+1$ 环的簇头节点都能收到一个或几个簇头信息。

5) 非簇头节点收到 CH_NOTIFY 消息后,通过计算获取簇头节点和自己之间的距离,放入 CH_DIST 列表中,经过 RCVD_CH_INFO_TIME 时间后,非簇头节点将 CH_DIST 列表中的簇头信息进行比较,选择当前环中距离自己最近的簇头节点,将自己的扩频码设置成属于该簇的扩频码的值以减少簇间干扰,然后在 JOIN_CLUSTER_TIME 时间内随机发送 CH_JOIN 消息给自己的簇头;而第 $k+1$ 环的簇头节点则从接收到的所有第 k 环簇头节点的 CH_NOTIFY 消息中选择距离自己最近的簇头节点作为下一跳,并向其发送 ROUTE_REQ 消息,从而形成了相对应的簇间多跳路由,如果没有收到 k 环节点的信息,表明自己周围出现了空洞,没有合适的簇头节点可以为自己传递数据到汇聚节点,此时则把本环内距离自己最近的簇头节点作为自己的下一跳,让这个簇头节点为自己转发聚合后的监测数据。

6) JOIN_CLUSTER_TIME 时间过后,簇头节点广播 CH_SCHED 消息给该簇成员节点,CH_SCHED 消息包含每个簇成员节点的时隙安排,簇成员节点在自己的时隙内发送数据包,其他时隙处于休眠状态以节省能量。

7) 各环在每轮结束后,将各簇头节点的能量和当前环平

均能量进行比较,如果本环所有簇头的能量大于当前环平均能量,保持当前所有簇头节点和多跳路径不变。否则,循环从3)到7)的步骤。

2.3 簇头选举概率

RBMC 节点采用类似于 LEACH 的簇头选举策略,但和 LEACH 略有不同,每个环采用不同的簇头选举概率 T_k ,各环节点簇头选举门限为:

$$T_k(n) = \begin{cases} \frac{m_k}{N_k - m_k * \lceil r_k \bmod (N_k/m_k) \rceil}, & \text{if } n \in G_k \\ 0, & \text{其它} \end{cases} \quad (3)$$

式中,下标 k 表示区域中的第 k 环, r_k 为第 k 环节点进行簇头选举的当前总轮数。 N_k 为第 k 环的节点总数, m_k 为第 k 环中期望的簇头个数。 G_k 表示在该簇头周期的前面所有轮中还没有充当过簇头的节点的集合。在文献[11]中,作者已经估算了 N_k 和 m_k ,其分别为:

$$N_k = \frac{2k-1}{S^2} N \quad (4)$$

$$m_{kopt} = \sqrt{\frac{N_1}{2}} \frac{\delta}{\sqrt{E[d_{a1}^2]}} \quad (5)$$

能量均衡要求满足 $E_{chk} = E_{ch(k-1)} = E_{ch(k-2)} = \dots = E_{ch1}$ 。

这种改进后的簇头选择策略在 LEACH 协议的基础上能够使网络的生命周期有效地提高 20%~30%。但是 RBMC 协议的簇头选举策略并没有考虑能量因素,因此无论节点的剩余能量是多少,在节点能量耗尽之前,依然会选择自己作为簇头节点,使剩余能量少的节点能量快速耗尽。

MCBMC 改进的簇头选举门限:

$$T_k(n) = \begin{cases} \frac{m_k}{N_k - m_k * \lceil r_k \bmod (N_k/m_k) \rceil} \\ \left[\frac{E_{current}}{E_{max}} + (r_k \div \frac{N_k}{2m_k}) (1 - \frac{E_{current}}{E_{max}}) \right], & \text{if } n \in G \\ 0, & \text{其它} \end{cases} \quad (6)$$

式中, $p_k = m_k/N_k$ 是簇头节点所有节点的百分比, k 表示当前所在的扇环数,不同环中的 p_k 是不同的,用以实现不均匀的分簇方式,距离汇聚节点越近, p_k 的值就越大; r 是当前网络运行中进行的轮数; G 是最近 N_k/m_k 轮中还没有当选过簇头的传感器节点; $E_{current}$ 是传感器节点当前的剩余能量; E_{max} 是传感器节点初始的能量; r_k 是传感器节点在上一次担任过簇头节点后,连续未当选过簇头的轮数(一旦传感器节点当选为簇头节点,此节点的 r_k 将被重置为 0)。 $\div$ 是整除操作,通过此操作,式(6)的第一部分公式分为两种情况:

1)如果当前传感器节点没有当选簇头的轮数小于 $N_k/2m_k$ 轮,整除操作部分为零。此时,能量较大的节点将会有更多的机会成为簇头;

2)如果当前传感器节点没有当选簇头的轮数等于或大于 $N_k/2m_k$ 轮,那么无论传感器节点剩余能量是多少,节点都会像 LEACH 协议一样来推选自己作为簇头。

式(6)的引入,既可以使能量多的节点集中在前几轮,以减少因为单一节点能量不足而使当前环重新成簇,又可以保证网内簇首节点的数量,减少某一轮没有簇头节点产生的概率,因此增加了网络的可靠性,进一步降低了“热点”问题出现的可能性,本文使用式(6)的簇头推举公式来选举每一个环

中的簇头。

2.4 MCBMC 多轮分簇机制

RBMC 协议采用 LEACH 协议的每轮重新成簇的机制,每轮重新成簇虽然可以更加公平地使整个网络的每个节点均衡耗能,但每次分簇所产生的开销也是巨大的,尤其是 TM-DA 的时隙分配信息在分簇过程中占能耗的很大一部分,MCBMC 采用了多轮分簇的机制来解决这一问题。

下面分析 RBMC 协议中第 k 环所有节点 M 轮总的能耗。

设第 k 环中一个簇消耗的能量包含 2 部分:簇头消耗能量 E_{chk} 和非簇头消耗能量 E_{nonchk} 。

数据传输阶段:

$$E_{chk_tr} = lE_{RX} \left(\frac{N_k}{m_k} - 1 \right) + lE_{DA} \frac{N_k}{m_k} + l \sum_{i=k+1}^S \frac{m_i}{m_k} (E_{RX} + E_{TX} + E_{fs} E[d_{chk,k-1}^2]) + l(E_{TX} + E_{fs} E[d_{chk,k-1}^2]) \quad (7)$$

$$E_{nonchk_tr} = l(E_{TX} + E_{fs} E[d_{tochk}^2]) \quad (8)$$

成簇阶段:

$$E_{chkoh} = l_{can} (E_{TX} + E_{fs} R^2) + l_{join} E_{RX} \left(\frac{N_k}{m_k} - 1 \right) + l_{idma} (E_{TX} + E_{fs} R^2) \quad (9)$$

$$E_{nonchkoh} = l_{can} E_{RX} + l_{join} (E_{TX} + E_{fs} E[d_{tochk}^2]) \quad (10)$$

一个簇每轮的总能耗为:

$$E = E_{chk_tr} + E_{chkoh} + \left(\frac{N_k}{m_k} - 1 \right) (E_{nonchk_tr} + E_{nonchkoh}) \quad (11)$$

故而第 k 环中所有节点 M 轮消耗的总能耗为:

$$E_{totalk} = Mm_k [E_{chk_tr} + E_{chkoh} + \left(\frac{N_k}{m_k} - 1 \right) (E_{nonchk_tr} + E_{nonchkoh})] + M(N_k - m_k) (E_{nonchk_tr} + E_{nonchkoh}) \quad (12)$$

MCBMC 采用多轮分簇,第 k 环 M 轮簇头保持不变,所有节点总能耗为:

$$E_{mul_totalk} = Mm_k (E_{chk} + E_{chkoh}) + m_k \left(\frac{N_k}{m_k} - 1 \right) (E_{nonchk} + E_{nonchkoh}) + Mm_k (E_{chk} + E_{chkoh}) + (N_k - m_k) (E_{nonchk} + E_{nonchkoh}) \quad (13)$$

因为 $M \geq 1$, 所以

$$E_{totalk} \geq E_{mul_totalk} \quad (14)$$

多轮成簇和单轮成簇相比,会有环平均能量收集,我们引入估计方法对环平均能量进行相应的估计^[12],其消耗的能量小。综上所述,采用多轮分簇能减少能量开销。

下面详细描述 MCBMC 协议的多轮分簇机制。

当一轮结束后,MCBMC 并不让剩下的节点重新选举簇头。而是将自己的剩余能量 `node_energy_remain` 与当前环的平均剩余能量 `ring_ave_energy_remain` 进行比较,此时,有一个很短的公共的时间段,用于收集环平均能量和发送重新成簇信息,所有节点将扩频码设置成公用的,以接受汇聚节点的数据。

这里假设一个权值 K (K 的取值在 0~1 之间),当所有节点的 `node_energy_remain` 都大于 `ring_ave_energy_remain * K`,保持当前所有簇头节点和多跳路径不变。

如果有一个簇头节点的 `node_energy_remain` 小于 `ring_ave_energy_remain`

ave_energy_remain * K, 此簇头节点将向汇聚节点以多跳的形式发送 CLUSTER_RESET_REQ 消息, 汇聚节点收该消息后, 向 k 环的所有节点发送 CLUSTER_RESET 消息, $k-1$ 环的簇头节点也需要接收此消息。所有节点收到 CLUSTER_RESET 消息后, k 环所有节点的轮数加 1, 然后用式(6)来自举, 并以上一节的方式分簇, 此时, $k+1$ 环和 k 环建立路由。分簇完成后, 由 $k-1$ 环和 k 环的簇头节点进行路由建立的广播, 完成多跳路由的建立。然后继续进入数据传输阶段, 直到本轮结束。

当每环到达每个周期的最后一轮时, 最近 N_k/m_k 中所有没有担任过簇头的节点以 1 为概率全部担任簇头节点, 本轮的所有节点负责收集本轮的剩余能量。在本轮开始时, 簇成员节点将剩余能量放入 CH_JOIN_E 包中发给自己的簇头节点, 簇头节点收到所有的 CH_JOIN_E 包后, 统计自己簇的剩余能量, 在下一个簇间专用的时间段内把本簇的剩余能量放入 CH_ENERGY 包中发送给汇聚节点, 汇聚节点通过 N_k/m_k-1 轮的能量来预测 N_k/m_k 轮的能量, 并在收到环重置 CLUSTER_RESET_REQ 消息时, 向该环发送 CLUSTER_RESET_E 消息, 使该环的每个传感器节点都可以得到当前环的剩余能量。

3 协议仿真及结果分析

3.1 仿真环境

本文采用 OPNET14.5 作为网络仿真工具, 并对节点总数 $N=300$ 、区域半径从 120m 到 300m 的场景进行了仿真。

在仿真中, 我们采用 LEACH 来设置轮的时间, 将每轮的时间设为 30s。网络仿真的参数设置如表 1 所列。

表 1 OPNET 网络仿真参数表	
参数	值
环半径	60m
汇聚节点坐标	网络的中心
节点数	300
节点初始能量	10J
E_{elec}	50nJ/bit
ϵ_{fa}	10pJ/bit/m ²
ϵ_{tra}	0.0013pJ/bit/m ⁴
d_0	86.2
数据包大小	500 bytes
信道带宽	1 Mbps

3.2 仿真结果分析

本文的 MCBMC 对 RBMC 进行了多处改进, 并设计出了完整的仿真代码, 将 MCBMC 与 RBMC 协议和 LEACH 协议进行了比较。

图 2 表明, 使用 300 个节点分别对 4 个场景进行仿真, 随着网络仿真场景的增大, LEACH 协议的网络生存时间逐渐变小, RBMC 协议和 MCBMC 协议的网络生存时间逐渐变大。这是由于随着网络仿真场景的增大和环数的增加, 节点并没有增加, 分环较多的场景因每个簇的规模较小且多跳需要转发的数据也小反而使能量消耗得较慢。在相同的环数下, MCBMC 协议与 RBMC 协议相比, 平均能耗更低, 所以生命周期更长。

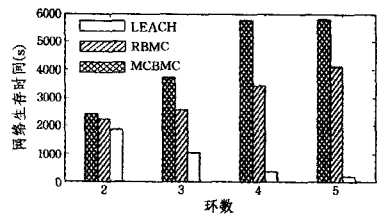


图 2 网络生存时间的比较

图 3 的仿真结果描绘了不同环数下, 采用 LEACH 算法、RBMC 和 MCBMC 算法时的节点平均能耗速率情况。图中显示出, 随着网络仿真场景的增大和环数的增加, LEACH 协议节点平均能耗速率逐渐变大, RBMC 协议节点平均能耗速率逐渐变小, MCBMC 协议由于改进了簇头选举机制和多轮分簇机制, 平均能耗比 RBMC 协议有所降低。这意味着在能源的大量节约上, MCBMC 协议与 RBMC 协议相比有较大提高。

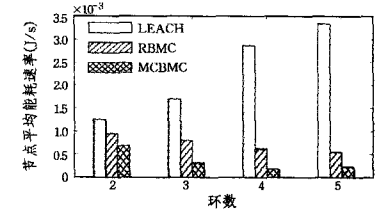


图 3 节点平均能耗速率比较

图 4 比较了不同场景下, RBMC 和 MCBMC 协议的节点成簇比特开销情况。随着网络仿真场景的增大和环数的增加, RBMC 协议的节点成簇比特开销逐渐增大。这是由于节点总数没有增加, 分环较多的场景每个簇的规模较小, 成簇个数增多, 用于成簇的比特开销相应增加。而 MCBMC 协议由于采用多轮分簇机制, 减少了成簇的次数, 和 RBMC 相比, 成簇的开销减少, 节约了能量。

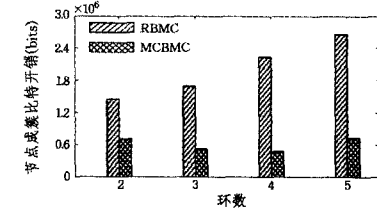


图 4 节点成簇比特开销比较

图 5 比较了不同场景下, RBMC 和 MCBMC 协议平均每轮的运行时间。随着网络仿真场景的增大和环数的增加, RBMC 协议的平均每轮的运行时间不变, 为 30s。而 MCBMC 协议由于采用多轮分簇机制, 每轮的平均运行时间变长, 减少了成簇的次数, 和 RBMC 相比, 节约了能量。

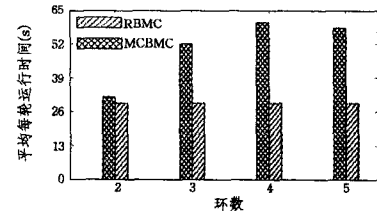


图 5 平均每轮运行时间比较

结束语 本文在分析已有分环多跳分簇路由算法 RBMC 的基础上, 提出了 MCBMC 算法, 其采用分环模式实现传

(下转第 97 页)

不能满足不可伪造性,攻击者可以根据一个合法的签名伪造其他消息的签名;并改进了 Li 基于属性签名方案^[12],提出了一个高效的支持动态门限的基于属性签名方案,降低了签名代价和签名长度,并且利用 CDH 问题的困难性,在随机预言机模型下证明了所提方案满足在适应性选择消息和断言下的不可伪造性。仿真实验结果表明,所提签名方案可以较好地应用于移动对等网数据分发,以实现消息认证。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signatures schemes [C]//Proceedings of CRYPTO 84 on Advances in Cryptology. 1985;47-53

[2] Boneh D, Franklin M. Identity based encryption from the weil Pairing[C]//Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. California, USA, August 19-23, 2001;213-229

[3] Sahai A, Waters B. Fuzzy Identity-Based Encryption[C]//Proceedings of EUROCRYPT. Aarhus, Denmark, May 2005; 457-473

[4] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proceedings of ACM Conference on Computer and Communications Security. New York, USA, 2006; 221-238

[5] Yang P, Cao Z, Dong X. Fuzzy identity based signature[R]. Report 2008/002. IACR Cryptology ePrint Archive, 2008

[6] Guo S, Zeng Y. Attribute-based signature scheme [C]// Proceedings of the 2nd International Conference on Information Security and Assurance. Busan, Korea, April 2008; 509-511

[7] Khader D. Attribute based group signatures[R]. Report 2007/159. IACR Cryptology ePrint Archive, 2007

[8] Maji H K, Prabhakaran M, Rosulek M. Attribute-based signatures: achieving attribute-privacy and collusion-resistance[R]. Report 2008/328. IACR Cryptology ePrint Archive, 2008

[9] Maji H K, Prabhakaran M, Rosulek M. Attribute-based signatures[R]. Report 2010/595. Cryptology ePrint Archive, 2010

[10] Li J, Kim K. Attribute-based ring signatures[R]. Report 2008/394. IACR Cryptology ePrint Archive, 2008

[11] Shahandashti S F, Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems [C]//Proceedings of the 2nd International Conference on Cryptology in Africa. Gammarrh, Tunisia, June 2009; 198-216

[12] Li J, LMan H A. Attribute-based signature and its applications [C]//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing, China, Apr. 2010; 60-69

[13] 陈少真, 王文强, 彭书娟. 高效的基于属性环签名方案[J]. 计算机研究与发展, 2010, 47(12): 2075-2082

[14] Herranz J, Laguillaumie F, Libert B, et al. Short attribute-based signatures for threshold predicates[C]//Proceedings of the 12th International conference on Topics in Cryptology. San Francisco, CA, USA, 2012, LNCS 7178; 51-67

(上接第 70 页)

传感器网络中的多跳路由。RBMC 协议簇头选举协议过于简单,和 LEACH 协议相同,并未考虑其他因素,极易造成簇头分布不均衡,使分环的效果降低。MCBMC 路由协议对 RBMC 作了多处改进,包括簇头自举的方法,以及根据预测环剩余能量使每环多轮成簇等。通过对协议 MCBMC 进行仿真并分析仿真结果,验证了 MCBMC 协议网络生存时间比 RBMC 协议更长,节点的平均能耗速率更小,节点成簇开销更少,能量消耗更少,提高了网络能效。

参 考 文 献

[1] 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;3-4

[2] Ahmed A, Mohamed Y. A survey on clustering algorithms for wireless sensor networks[J]. Comput Communication, 2007, 30(14/15): 2826-2841

[3] Mhatre V, Rosenberg C. Design guidelines for wireless sensor networks: communication, clustering and aggregation[J]. Ad Hoc networks, 2004, 2(1): 45-63

[4] 侯西梅, 万润泽. 无线传感器网络的多跳分簇路由协议建模与实现[J]. 江西师范大学学报, 2008, 32(2): 215-218

[5] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor net-

works[C]//Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. Hawaii, 2000; 10-15

[6] 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

[7] Lindsey S, Raghavendra C S. PEGASIS: Power-efficient gathering in sensor information systems[C]//Proc. of the IEEE Aerospace Conf. Montana; IEEE Aerospace and Electronic Systems Society, 2002; 1125-1130

[8] Younis O, Fahmy S. HEED: A hybrid, energy-efficient, distributed clustering approach for Ad hoc sensor networks[J]. IEEE n8ns, on Mobile Computing, 2004, 3(4): 366-379

[9] Ye Mao, Li Cheng-fa, Chen Gui-hai, et al. EECS: an energy efficient clustering scheme in wireless sensor network[C]//Performance, Computing, and Communications IPCCC. 2005 24th IEEE International Conference. April 2005; 535-540

[10] Li Cheng-fa, Chen Gui-hai. An Uneven Cluster-Based Routing Protocol for Wireless Sensor Networks[C]//Chinese Journal of Computers, 2007; 27-35

[11] 刘志, 裴正定. 基于分环多跳的无线传感网分簇路由协议[J]. 通信学报, 2008, 29(3): 104-113

[12] 卿利, 朱清新, 王明文. 异构传感器网络的分布式能量有效成簇算法[J]. 软件学报, 2006, 17(3): 481-489