

一种基于节点位置信息的无线传感器网络并行传输 MAC 协议

杨国燕^{1,2} 张国印¹

(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)¹

(黑龙江大学信息科学与技术学院 哈尔滨 150080)²

摘要 针对无线传感器网络多跳通信方式产生的暴露终端问题,提出了一种基于地理位置信息的高效并行传输 LACT-MAC 协议。该协议突破了传统基于 CSMA 协议对并行传输的限制,利用节点地理位置信息实现了暴露终端的并行传输,有效地提高了宝贵无线信道资源的复用效率。分析了根据节点的位置坐标并行传输暴露终端节点的可行性,并通过并行传输检测完成了传输过程。仿真结果证明,与标准的 IEEE 802.11 DCF 协议比较,LACT-MAC 协议能显著提高网络的平均吞吐量,降低数据传输延迟,有效提高无线传感器网络效率和性能。

关键词 无线传感器网络,暴露终端,并行传输,MAC 协议

中图分类号 TP393 **文献标识码** A

Concurrent Transmission MAC Protocol for Wireless Sensor Network Based on Nodes' Geographical Location Information

YANG Guo-yan^{1,2} ZHANG Guo-yin¹

(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)¹

(College of Information Science and Technology, Heilongjiang University, Harbin 150080, China)²

Abstract Aiming at the exposed terminal problems in multi-hop wireless sensor networks, this paper proposed the efficient concurrent transmission LACT-MAC protocol based on geographical location information. The protocol breaks through the limit of concurrent transmission based on traditional CSMA MAC protocols, for this protocol exploits nodes' geographical location information to achieve the concurrent transmission of exposed terminal, so as to enhance the reuse efficiency of the valuable wireless channel resources. According to the location coordinates of the nodes, this paper explored the feasibility analysis of concurrent transmission of exposed terminal node, and completed the concurrency check. Simulation results show that, compared to IEEE 802.11 DCF protocol, LACT-MAC protocol can significantly improve the average throughput of the network, reduce data transmission delay, and effectively improve the efficiency and performance in wireless sensor networks.

Keywords Wireless sensor networks, Exposed terminal, Concurrent transmission, MAC protocol

无线传感器网络是一种特殊的无线自组织网络,综合了传感器技术、嵌入式计算技术、分布式信息处理技术和通信技术,是由部署在监测区域内大量的微型传感器节点组成、通过无线方式进行通讯的多跳网络,其目的是采集、处理和传递所覆盖区域内的信息^[1]。无线传感器网络的共享方式是多跳共享广播方式。由于传感器节点的通信范围受限,在发送节点传输范围以外的节点感知不到任何通信的存在,因此在发送节点以外的节点不受发送节点的影响,可以同时发送报文,这种共享的方式提高了无线信道的空间复用度。无线传感器网络多跳共享无线信道方式产生的影响是数据传输冲突与节点的地理位置相关。由于发送节点和接收节点所感知的信道状况不同,因此带来了隐藏终端和暴露终端等问题^[2]。

无线传感器网络中 MAC (Medium Access Control) 协议

决定了无线信道的使用方式以及无线传感器网络节点之间的通信资源分配。目前典型采用载波监听多路访问 (CSMA) 的 MAC 协议,如 IEEE 802.11 DCF 实现在单信道条件下在数据发送前附加 RTS/CTS 握手的方式,很好地解决了隐藏终端问题,但可暴露终端的问题一直存在。暴露终端对信道利用不充分,限制了网络吞吐量的提高,尤其在节点密集、数据量较大的无线传感器网络中,这个问题更为突出。解决暴露终端问题,提高网络吞吐量,减少数据传输延迟,实现有效传输的关键是设计高效 MAC 协议。

本文主要的贡献是提出了一种新型高效的 MAC 协议 (LACT-MAC),该协议利用无线传感器网络中节点的地理位置信息,实现多个节点的有效并行传输,解决了传统 MAC 协议中的暴露终端问题,显著提高了宝贵信道资源的空间复用

到稿日期:2011-03-15 返修日期:2011-05-31 本文受国家自然科学基金(61073042),哈尔滨市科技创新人才研究专项资金项目(2011 RFDXG005)资助。

杨国燕(1976-),女,博士生,副教授,主要研究方向为无线传感器网络,E-mail: hdyanguoyan@gmail.com;张国印(1962-),男,教授,博士生导师,主要研究方向为网络与信息安全、无线网络、嵌入式系统。

效率。本文假设节点通过 GPS 接收机或节点定位算法^[3,4], 可以获知自己的地理位置信息。

1 问题描述和相关工作

暴露终端的存在其实质是由于采用载波侦听技术而带来的问题。IEEE 802.11 DCF 是目前基于 CSMA 的 MAC 协议在无线网络中应用最广泛的协议。在 DCF 中采用了虚拟载波监听技术, 节点在发送大的数据包之前, 采用 RTS/CTS 控制帧判断信道的忙闲状态, 以减少冲突造成的信道资源浪费。发送节点 A 要竞争信道, 首先广播 RTS 帧, 表明节点 A 要向节点 B 发送数据。节点 B 收到 RTS 后, 向所有节点发出 CTS 帧, 表明已准备就绪, 节点 A 可以发送数据, 而其他要向节点 B 发送数据的节点暂停发送。双方在成功交换 RTS/CTS 帧后, 节点 A 才开始真正地向节点 B 发送 DATA 帧, 节点 B 正确接收数据帧后向节点 A 发送 ACK 帧。暴露终端是指在发送节点的通信范围内而在接收节点的通信范围之外的节点^[5]。在图中 1, 当节点 A 为了给节点 B 发送数据向所有节点广播 RTS 帧时, C1 和 C2 就为暴露终端。而节点 B 给节点 A 应答 RTS 帧时, D1 和 D2 也为暴露终端。此时节点 A 和节点 B 的数据通信使暴露终端节点无法同时向其他节点发送信号, 导致信道利用不充分, 浪费了宝贵的无线信道资源, 限制了网络吞吐量的提高并增加了数据传输延迟。

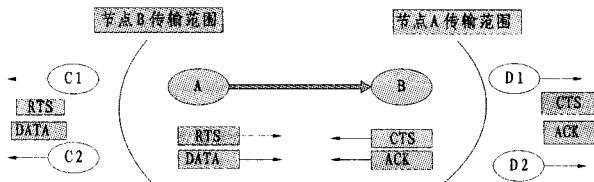


图1 IEEE 802.11 DCF 中暴露终端问题

但实际上, 由于暴露终端在接收节点传输范围之外, 每个暴露终端节点可以与发送节点 A 并行发送数据。目前, 国内外许多学者已经在传统的 MAC 协议基础上提出了几种允许暴露终端的并行传输, 从而提高空间复用率的改进机制^[6-9]。文献[10]指出载波侦听范围是信道空间复用率的重要参数, 并利用最优的载波侦听范围减少暴露终端节点的数量。文献[11]中研究人员利用有效的功率控制算法来提高信道空间复用效率。文献[12]中提出一种并行传输机制, 即在 RTS/CTS 和 DATA/ACK 报文之间添加附加控制时隙, 完成邻近节点数据传输的并发调度, 但这种附加控制时隙的协议, 只考虑了相邻节点同为发送或者接收节点的情况, 而未能充分挖掘网络中的并发潜力。

在上述的研究工作中, 虽然对暴露终端并行传输提出了一些解决方法, 但都没有充分利用节点的地理位置信息准确地分析暴露终端并行传输的可行性及对并行传输进行检测。在本文设计的 LACT-MAC 协议中, 利用节点地理位置坐标来判断暴露终端节点的身份, 并分析了暴露终端并行传输的可行性, 通过并行传输检测使暴露终端的并行传输不会干扰当前正在进行的传输, 而且不会被正在进行的传输破坏, 从而有效地提高了无线传感器网络的吞吐量。

2 暴露终端并行传输可行性分析

为了确保暴露终端进行的并行传输不干扰当前正在进行

的主传输, 首先分析并行传输中接收节点的干扰范围。根据无线信号传播模型采用双线地面反射模型^[13]可以计算接收节点的接收功率 P_r :

$$P_r = \frac{P_t G_t G_r (h_t h_r)^2}{d^4} \quad (1)$$

式中, P_t 是节点的发送功率, G_t 和 G_r 各为发送节点和接收节点的天线增益, h_t 和 h_r 各为发送节点和接收节点的天线高度, d 是发送节点和接收节点之间的距离。

设 P_r 为距发送节点距离为 d , 时接收节点的接收功率, P_i 为接收干扰功率的和, 接收节点成功接收数据时信干比的阈值为 SIR_T , 则接收节点能够成功接收数据的信干比必须大于阈值即为:

$$SIR = \frac{P_r}{P_i} \geq SIR_T > 1 \quad (2)$$

根据双线地面反射模型和式(2), 可以得出在距接收节点 d_r 范围内进行的传输可以干扰到当前正在进行的主传输。由此可以得到接收节点的干扰范围为:

$$R_i = d_r \sqrt[4]{SIR_T} \quad (3)$$

为了不失一般性, 在坐标轴上表示当前正在进行的主传输的节点和暴露终端进行的并行传输节点的位置, 主传输中发送节点为 $A(d_0, 0)$, 接收节点为 $B(d_0 + m, 0)$, 节点 C 为暴露节点并行传输的发送节点, 节点 $D(x, y)$ 为并行传输的接收节点, 如图 2 所示。

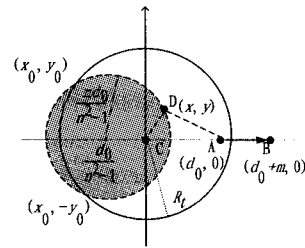


图2 暴露终端和主传输进行并行传输范围

现在考虑能够进行成功并行传输节点 D 的范围。由式(3)可得, 若实现不被当前主传输干扰的并行传输时节点 C 与节点 D 的距离为:

$$n \sqrt{x^2 + y^2} \leq \sqrt{(x - d_0)^2 + y^2} \quad (4)$$

此处 $n = \sqrt[4]{SIR_T} > 1$ 。把式(4)进一步整理为:

$$\left(\frac{nd}{n^2 - 1}\right)^2 \leq \left(x + \frac{d_0}{n^2 - 1}\right)^2 + y^2 \quad (5)$$

由式(5)可以得出, 进行并行传输时接收节点 D 的可行范围是以 $(-d_0/n^2 - 1, 0)$ 为圆心、以 $nd/(n^2 - 1)$ 为半径的圆形区域, 见图 2 中的阴影圆部分。另外, 考虑接收节点 D 要在发送节点 C 的传输范围之内才能进行成功传输, 在图 2 中, R_c 表示节点 C 的传输范围, 即实线大圆是节点 C 的传输范围, 可以得到:

$$R_c^2 \geq x^2 + y^2 \quad (6)$$

则接收节点 D 的可行范围是阴影圆和实线大圆的交叉部分, 这两点的坐标分别为 (x_0, y_0) 和 $(x_0, -y_0)$ 。由式(5)和式(6)可以得出:

$$x_0 = \frac{n^2 d_0}{2(n^2 - 1)} - \frac{n^2 - 1}{2d_0} R_c^2 - \frac{d_0}{2(n^2 - 1)}$$

$$y_0 = \sqrt{\frac{(n^2 + 1)R_c^2}{2} - \frac{(n^2 - 1)^2 R_c^4}{4d_0^2} - \frac{d_0^2}{4}}$$

由 x_0 和 y_0 的值可以得出,暴露终端进行并行传输的可能性随其传输范围的减小而增大,同时随进行并行传输时接收节点距离的增加而增大。

3 LACT-MAC 协议描述

LACT-MAC 协议实现的主要目的是解决传统的基于 CSMA 方式的 MAC 协议中存在的暴露终端问题,所以本文的研究是在 IEEE 802.11 DCF 协议机制基础上进行的。LACT-MAC 协议主要由 4 部分组成:(1)节点地理位置信息的获取和转发;(2)暴露终端节点的确认;(3)并行传输的检测和执行;(4)多个并行传输冲突避免机制。

3.1 节点地理位置信息的获取

目前国内外许多学者正致力于无线传感器网络节点定位技术的研究并取得了高速进展。可以直接获取节点位置信息的方法是为每个节点配备全球定位系统(GPS)。本文假设节点可以通过 GPS 系统或节点定位算法^[3,4] 获得位置坐标信息。

网络中所有节点定时广播自己的位置信息,因而各节点可以获得所有邻居节点的位置信息。在节点邻居节点状态列表增加位置信息字段,用来保存邻居节点的地理位置信息坐标。在节点广播位置信息时,保存一跳范围内邻居节点的位置。当节点的位置信息发生变化时,节点可以及时地更新邻居列表中的邻居节点的位置信息值,这样每个节点都会保存两跳范围内的邻居节点的位置。

3.2 暴露终端节点的确认

传感器网络中的节点收到其他节点发出的 RTS 帧之后,通过 RTS 帧中的信息可获得通信的源节点和目的节点。该节点通过两跳局部拓扑比较自己与目的节点的位置关系,判断自己是否为暴露终端。当源节点和目的节点建立起链接关系后,节点判断接收了邻居节点 RTS 帧,没有 CTS 帧,则该节点利用物理载波监听判断信道是否空闲。若信道空闲,则可判断自己是暴露终端。同时根据节点的位置信息可以计算出节点与主传输中接收节点的距离大于接收节点传输范围,即 $d_x > R_t$,并且发送节点是当前节点的邻居节点,由暴露终端的定义可知,该节点为暴露终端节点,如图 3 中 C1、C2 和 C3 均为暴露终端。

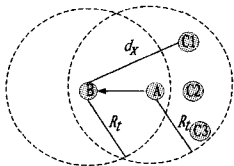


图 3 暴露终端节点确认

3.3 并行传输的检测和执行

LACT-MAC 协议允许暴露终端进行并行传输,但并不是所有的暴露终端都可以进行并行传输,由第 3 节可知,只有当暴露终端进行的并行传输不会干扰当前正在进行的主传输才可以,所以暴露终端在进行并行传输之前要进行检测,符合条件才被允许执行。例如在图 3 中确认的其中一个暴露终端 C 要并行传输数据给节点 D,如图 4 所示。根据节点地理位置坐标,可以计算节点 A 和节点 D 的距离为 d_{AD} ,节点 B 和节点 C 的距离为 d_{BC} ,节点 B 和节点 D 的干扰范围即为 R_B 和 R_D ,可由式(3)计算得出,则满足条件 $d_{AD} > R_B, d_{BC} > R_D$

同时成立,暴露终端节点 C 和节点 D 的并行传输被允许执行。在 LACT-MAC 协议中,要求暴露终端进行的并行数据传输必须在当前主传输数据传输期间完成,以保证数据传输的过程和接收 ACK 帧不受干扰。

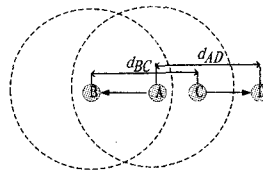


图 4 暴露终端进行的并行传输

3.4 多个并行传输冲突避免机制

由于在发起当前主传输的节点 A 周围可能存在多个暴露终端,每个暴露终端通过并行传输检测机制都可以进行并行传输,同时竞争信道会引起多个暴露终端的并行传输发生冲突,因此在 LACT-MAC 协议中设计了并行传输冲突避免机制。本文采用类似传统 MAC 中的随机退避机制,设置了一个随机退避时间来限制潜在的多个并行传输开始的时间。随机退避时间 t_b 以如下方式计算:

$$t_b = INT[CW \times rand()] \times aSlotTime$$

式中, CW 是 CW_{min} 和 CW_{max} 之间的一个整数值, $rand()$ 是 0~1 之间的随机数, $aSlotTime$ 是时隙值。

当暴露终端侦听当前主传输开始发送数据帧时,开始按 t_b 时间进行退避计数,在此期间仍然侦听是否有其他的并行传输开始进行。如果侦听到有其他的并行传输开始,则取消计数器,否则当计数器为零时,该暴露终端开始并行传输数据。

4 性能仿真及分析

为了评估 LACT-MAC 协议的性能,本文采用了实验仿真的方法,在 OPNET 网络仿真环境中比较 LACT-MAC 协议和 IEEE 802.11DCF 协议的性能。由于暴露终端主要对网络的吞吐量和延迟影响比较大,本文在仿真中主要考虑平均端到端网络吞吐量和端到端数据传输延迟 2 个性能指标。网络中设定每个节点始终有数据帧待发,即系统处于饱和状态。

本实验主要是通过改变网络负载来仿真网络吞吐量、数据包传输延迟性能。网络拓扑结构采用节点随机分布方式,在 1000m×1000m 的矩形区域中,布置 5 种不同节点数目的仿真情景。节点在全向天线方式下的传输范围为 250m,物理载波检测范围为 550m,接收信号干扰比的阈值为 10dB。OPNET 无线建模中可获取节点位置坐标,用于模仿 GPS 设备。其他仿真参数设置如表 1 所列。

表 1 仿真参数设置

参数说明	值	参数说明	值
数据帧长度	1024 bytes	信道速率	1MB/s
MAC 头长度	224bits	SIFS 帧间隔	10us
ACK 帧长度	304bits	DIFS 帧间隔	50us
RTS 帧长度	352bits	CW _{min}	31
CTS 帧长度	304bits	CW _{max}	1023
PHY 头长度	192bits	时隙长度	20us

由图 5 的仿真结果可以看出,在 LACT-MAC 协议中,随着网络中节点数目的增多,暴露终端并行传输的机会越大,网络的吞吐量也会不断增加。当网络中节点数目为 150 个时,网络吞吐量为 18.2Mbit/s,而 IEEE 802.11 MAC 协议是采

用虚拟载波侦听方式,某一时刻只允许一对收发节点进行数据传输,吞吐量一直保持在 10.1Mbit/s 左右不变。仿真过程中,设定系统为饱和状态,实验结果表明,采用 LACT-MAC 协议较 DCF 协议网络端到端吞吐量有显著的提高。

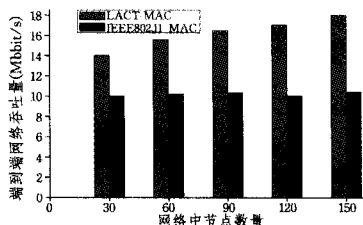


图 5 不同节点数目的 5 种仿真情景时端到端吞吐量分析

图 6 给出了 5 种不同节点数目仿真场景下平均端到端数据包传输延迟的曲线。从图 6 可以看出,802.11DCF 协议随着网络中节点数目的增加,节点间冲突会增多,导致数据重传率升高,从而使平均数据包传输延迟逐步增加。而采用 LACT-MAC 协议时,多个暴露终端可以同时进行数据传输,从而大大降低了平均数据包传输延迟。由实验结果可知 5 种仿真情况下,LACT-MAC 协议与 DCF 协议平均端到端的延迟的比值分别为 64.28%,60.60%,70%,80%和 78.57%。仿真实验证明,LACT-MAC 协议传输数据包的平均延迟远小于 802.11DCF 协议。

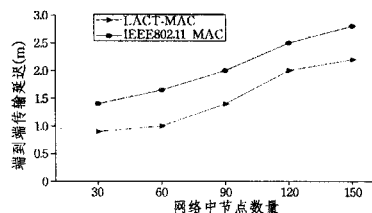


图 6 不同节点数目的 5 种仿真情景时端到端延迟分析

结束语 本文主要解决了无线传感器网络中暴露终端导致无线信道利用率低的问题。首先利用节点地理位置信息分析了暴露终端并行传输的可行性,在此基础上提出了一个高效无线传感器并行传输 LACT-MAC 协议。在 LACT-MAC 协议中,节点首先通过 GPS 或其他定位算法获取当前的地理位置信息,然后根据此位置信息识别自己暴露终端身份,只有通过并行传输检测的暴露终端才能进行并行传输调度。为了避免多个并行传输之间发生冲突,协议中增加了随机退避机制,从而减少了数据发送冲突产生的能量消耗。仿真结果表明,相比于 IEEE 802.11 DCF 协议,LACT-MAC 协议显著提高了网络的平均吞吐量,降低了数据传输延迟,并有效提高了

无线传感器网络的效率和性能。

参考文献

- [1] Akyildiz F, Su W, Sankarasubramaniam Y, et al. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8):102-114
- [2] Jiang L B, Liew S C. Improving throughput and fairness by reducing exposed and hidden nodes in 802.11 networks[J]. IEEE Transactions on Mobile Computing, 2008, 7(1):34-49
- [3] 姜志鹏,高随祥.无线传感器网络节点定位的同心圆改进算法[J]. 计算机科学, 2009, 36(10):46-49
- [4] Shi Q, He C, Chen H, et al. Distributed wireless sensor network localization via sequential greedy optimization algorithm [J]. IEEE Transactions on Signal Processing, 2010, 58(6):3328-3340
- [5] Wu X, Mukherjee B, Chan S H G. MACA-an efficient channel allocation scheme in cellular networks[C]//IEEE Global Telecommunications Conference. San Francisco, CA, USA, 2000; 1385-1389
- [6] Bencini L, Fantacci R, Maccari L. Analytical model for performance analysis of IEEE 802.11 DCF mechanism in multi-radio wireless networks[C]//Proc. of ICC. Cape Town, South Africa, 2010;1-5
- [7] Son I K, Mao S, Hur S M. Medium Access Control for Opportunistic Concurrent Transmissions Under Shadowing Channels [J]. Sensors, 2009, 9(6):4824-4844
- [8] Fu L, Liew S C, Huang J. Effective Carrier Sensing in CSMA Networks Under Cumulative Interference[C]//Proceedings of INFOCOM. San Diego, USA, 2010;1-9
- [9] Jiang L, Walrand J. A Distributed CSMA Algorithm for Throughput and Utility Maximization in Wireless Networks [J]. IEEE/ACM Trans on Networking, 2010, 18(3):960-972
- [10] Zhai H, Fang Y. Physical carrier sensing and spatial reuse in multirate and multihop wireless ad hoc networks[C]// Proc. IEEE INFOCOM. Barcelona, Spain, Apr. 2006; 1-12
- [11] Alawieh B, Zhang Y, Assi C, et al. Improving Spatial Reuse in Multihop Wireless Networks-A Survey[J]. IEEE Commun, Surveys Tutorials, 2009, 11(3):71-91
- [12] Heuvel-Romaszko S V D, Blondia C. Enhancements of the IEEE 802.11, a MAC protocol for ad hoc network with history of power adjustment[C]//Proc IEEE Conf Wireless Netw. 2005; 48-54
- [13] Zhou Y H, Nettles S M. Balancing the hidden and exposed node problems with power control in CSMA/CA-based wireless networks[A]// IEEE Wireless Communications and Networking Conference[C]. New Orleans, LA, USA, 2005; 683-688

(上接第 94 页)

前 4 轮轮密钥,结合密钥扩展即可获取 ARIA 主密钥。下一步的工作将在实际的物理加密平台上采集加密算法运行过程泄露的旁路信息,并对其进行多种功耗分析方法的研究。

参考文献

- [1] Kocher P C, Jaffe J, Jun B. Differential Power Analysis[A]// Proc. of the CRYPTO 1999[C]. LNCS 1109. Berlin: Springer-Verlag, 1999;388-397
- [2] Brier E, Clavier C, Olivier F. Correlation Power Analysis with a Leakage Model[A]//Joye M, Quisquater J J, eds. Cryptographic Hardware Embedded System-CHES 2004[C]. Springer-Verlag,

LNCS 3156, 2004;16-29

- [3] Kwon D, Kim J, Park S. New block cipher: ARIA[A]//Proc. of the Information Security and Cryptology-ICISC'03[C]. Berlin: Springer-Verlag, LNCS 2971, 2003;432-445
- [4] Thomas M. Using Second-order Power Analysis to Attack DPA Resistant Software[A]//Proc. of the CHES 2000[C]. Berlin: Springer-Verlag, LNCS 1965, 2000;238-251
- [5] Mangard S, Elisabeth O, Thoms P. Power Analysis Attacks [M]. Berlin: Springer-Verlag, 2007;119-165
- [6] Moradi A, Mischke O, Eisenbarth T. Correlation-enhanced Power Analysis Collision Attack[A]//Mangard S, Standaert F X, eds. CHES 2010[C]. LNCS 6225, 2010;125-139