文章编号：1001-0920(2009)11-1652-05

一种检测无线网络违规行为的改进退避算法

刘志新，张 伟，华长春，关新平
（燕山大学 a.电气工程学院，b.工业计算机控制工程河北省重点实验室，河北 秦皇岛 066004）

摘 要：无线媒体访问控制(MAC)协议通常使用分布式竞争机制来共享无线信道，但在动态和开放的网络环境中，部分违规节点会有意识地抢占信道以获取更多的信道资源.为此，通过对 IEEE 802.11 协议的 DCF 机制进行修改，提出一种改进的退避算法，可实现对网络中违规行为节点的有效检测，并通过惩罚机制加以纠正.仿真结果表明，该方法能够更有效地检测出无线网络中的违规行为，提高整个网络的吞吐量.

关键词：无线网络；IEEE 802.11 协议；MAC 协议；违规行为；分布式协调功能模式
中图分类号：TN925 **文献标识码**：A

Improved back-off algorithm for detecting misbehavior in wireless networks

LIU Zhi-xin, *ZHANG Wei*, *HUA Chang-chun*, *GUAN Xin-ping*
(a. Institute of Electrical Engineering, b. Key Laboratory of Industrial Computer Control Engineering of Hebei Province, Yanshan University, Qinhuangdao 066004, China. Correspondent: LIU Zhi-xin, E-mail: lzxauto@ysu.edu.cn)

Abstract: Wireless medium access control (MAC) usually uses distributed contention resolution mechanisms for sharing the wireless channel. However, in an open and dynamic wireless network, to obtain more bandwidth resources, some nodes may preempt channel resource. Modifications to the distributed coordination function (DCF) mechanism of IEEE 802.11 protocol are presented, and an improved algorithm to implement the detection of misbehavior is proposed. The penalty measures are taken further to correct the misbehavior. Simulation results show that the ratio of correctly detecting the misbehavior is improved and the throughput of the whole networks is increased by using the proposed mechanism.

Key words: Wireless network; IEEE 802.11 protocol; MAC protocol; Misbehavior; Distributed coordination function

1 引 言

近年来，无线网络得到了快速发展，无线设备在军事、灾难救助以及工业等领域得到了普遍应用.IEEE 802.11 协议广泛应用于无线移动自组网中[1]，节点通常依靠无线媒体访问控制(MAC)机制共享无线信道[2].该机制依靠分布式协调功能(DCF)，即在发送前从指数增长的竞争窗口中随机选择一个退避时间进行等待，通过 RTS-CTS 握手机制竞争无线信道.但是，在动态和开放的无线环境中，一些具有自私性行为的节点可能为获得大的信道资源而违反 IEEE 802.11 的 MAC 协议[3].如何有效、及时地检测出违规行为，已成为当前研究的热点和难点之一[4].

针对这些违规行为，文献[5]提出通过修改 IEEE 802.11 协议的方案来解决自私性节点的违规行为.但是，该方案存在的问题是 CW(竞争窗口)值的变化仍然是 IEEE 802.11 协议标准的 CW 值，网络的不公平性依然得不到改善[6].文献[7,8]不同于文献[5]以退避值的不同来判断 MAC 层的违规行为，而是对 DCF 机制中定义的两个固定时间 SIFS(短帧间间隔)和 DIFS(长帧间间隔)进行分析，通过判断它们的大小来检测节点是否发生违规行为.

本文对文献[5]中存在的问题加以改进.改进算法能更好地检测出这种自私性违规行为，并加以纠

收稿日期：2008-11-04；**修回日期**：2009-03-20.
基金项目：国家杰出青年基金项目(60525303)；国家自然科学基金项目(60604004,60804030,60604012)；河北省科技支撑配套项目(072435155D)；河北省教育厅基金项目(2008147).
作者简介：刘志新(1976—)，男，河北唐山人，副教授，博士，从事网络控制、跨层优化等研究；关新平(1963—)，男，黑龙江齐齐哈尔人，教授，博士生导师，从事网络控制系统、鲁棒控制等研究.

正.这样不但可以提高整个网络的吞吐量,而且能解决隐藏节点的问题[3].

2　问题描述

由于无线局域网采用开放式机制接入无线媒体,一些具有违规意图的节点可通过以下两种行为影响正常的网络性能:

1)节点不按照 DCF 定义的区间选择退避值,而是有意缩短退避时间;从平均退避值较小的分布中选择退避值(如从区间[0,$CW_{min}/4$],而不是[0,CW_{min}]中选择退避值),甚至所选择的退避值仅仅为一个时间间隔.

2) 采用不同的重传策略,当冲突发生时 CW 保持不变.即使节点不实施违规行为,信道也总是给予发送成功的节点以最小的竞争窗口 CW_{min},同时加倍竞争失败节点的 CW.发送成功的节点由于 CW 为最小值 CW_{min},在下次传输时更容易占用信道,从而加剧网络的不公平性.此外,节点在一次发送成功后,CW 即减少到最小值 CW_{min},从而不能正确反映信道的占用情况,容易导致新的冲突.

3　改进算法描述

3.1　算法说明

首先给出如下假设:

1) 接收节点(R)都是可信的,同时 R 兼有发送器和监测器的功能,且能够监测 S 退避值以及实时更新分配给发送节点(S)的退避值;

2) R 内设有一个比较器,可完成 S 实际的退避值与 R 分配给它的退避值的大小比较.

算法分为 3 个过程:检测、惩罚、诊断.算法流程如图 1 所示.

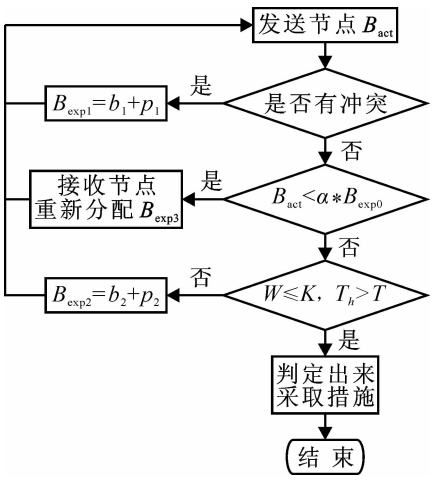

图 1　算法流程图

图中:B_{act} 为 S 实际退避的时间;B_{exp0} 为 R 最新更新的 S 应遵循的退避值;B_{exp1} 为发生冲突后,S 应等待的总的退避值;B_{exp2} 为实际退避值与规定退避值有偏离时,S 应遵循的退避值;B_{exp3} 为正常节点成功发送后,R 分配给 S 的退避值;b_1 为本次冲突发生之前 S 应该退避的时间;b_2 为实际退避值与规定的退避值有偏离时,R 分配给 S 的退避值;p_1 为发生冲突后,S 需要重新等待的退避值;p_2 为实际退避值与规定的退避值有偏离时,R 给 S 施加的惩罚;α,T,K,W 和 T_h 的含义将在惩罚策略和诊断策略中给出.

3.2　算法具体实施过程

首先在 IEEE802.11DCF 机制的基础上,进行如下修改:当节点第 1 次发送数据时,仍然按照 IEEE 802.11 协议的标准,在[0,CW_{min}] 中随机选择一个退避值进行传输,但在第 2 次传输时,所需要的退避时间为包含在 ACK 包内的 R 给 S 分配的退避值.

因为 R 分配的退避值也在[0,CW_{min}] 中选择,所以可利用竞争窗口 CW 值的改进方法,即 EIED 方法来改善网络的公平性[9].该方法的过程如下:

发送成功

$$CW \leftarrow \max(((CW+1)/n-1), CW_{min}),$$

为方便计算,选择 $CW_{min}=31$;

发送失败

$$CW \leftarrow \min(((CW+1)*m-1), CW_{max}),$$

为方便计算,选择 $CW_{max}=1023$.

当节点再次要求发送数据时,可分为以下两种情况加以考虑:

1) 当数据发送成功后,S若想再次发送数据,则需等待 R 分配给 S 的退避时间.此时 R 记录下上次发给 S 的 ACK(确认) 包的时间,并与本次接收到的 RTS(请求发送) 包的时间进行比较,得到的差值就是 S 的实际退避值 B_{act}.如果 B_{act} 的值小于 B_{exp0} 的某个倍数 α,即

$$B_{act} < \alpha * B_{exp0},\ 0 < \alpha \leqslant 1, \qquad (1)$$

式中 α 是一个能根据信道环境的不同而自适应调整的系数,则认为 S 可能存在违规行为,要对其实施一定的惩罚.其细节将在惩罚策略中加以说明.

2) 当数据发送失败后,如两个 S 的退避计数器同时减到零,即传输发生冲突时,需重新选择退避值,等到信道空闲时再发送.所以要定义一个函数,使 S 能根据冲突的次数在[0,CW_S] 中选择一个新的退避值进行等待.该情况下新的退避值为

$$B_{exp1} = B_1 + \sum_{2}^{attempt} f(b_1, s, i) * CW_i. \qquad (2)$$

式中:$f(b_1,s,i)=(a*X+c)\bmod(CW_S+1)$,$a=5$,$c=2*i+1$;$X=(b_1+s)\bmod(CW_S+1)$,$b_1$ 为上次成功传输后分配的退避值;f 函数是一个决定函数[10],它能根据信道冲突情况从(0,1) 之间选择一

个合适的值，从而有效地避免下次传输数据时再发生冲突；s 为冲突时发送节点的标号；attempt 为冲突次数；CW_S 为上次成功传输时S的竞争窗口；CW_i 为冲突发生后变化的竞争窗口，取值为 $\min((CW_S+1)*m^{i-1}-1, CW_{max})$.

3.3 对潜在违规行为的惩罚策略

当 B_{act} 和 B_{exp0} 满足式(1)时，认为S可能存在违规行为，则在分配退避值时对其进行适当的惩罚，惩罚值为

$$p_2 = \max(\alpha * B_{exp0} - B_{act}, 0). \tag{3}$$

从而总的退避值为

$$B_{exp2} = b_2 + p_2. \tag{4}$$

这样便给了S一个大的退避值. 如果S遵从了这次惩罚，则认为不存在违规行为，S也不会获得很高的吞吐量；否则，根据诊断策略进一步判断S是否为违规行为节点.

一次偏离不能完全反映S就是违规行为节点. 由于信道环境的不同，S可能认为信道是空闲的，而R认为信道忙(即存在隐藏节点)[2]. 此时，R的计数器应停止计数，而S不了解这个情况仍然按原来的退避值计数，这样便可能对S造成误判断. 所以应根据信道环境调整 α 值，使得对正常节点误判断的几率降低，对网络不会产生很大的影响.

α 的选择可分为以下4种情况：

1) 如果二者都监听信道空闲，则选择中等 α 值.

2) 如果S认为空闲而R认为忙时，则可能存在隐藏节点，从而造成误判断. 所以选择小的 α 值，不但可以避免误判断，而且即使判断出来，所施加的惩罚也不大.

3) 如果二者均监听信道忙，则是违规行为节点的几率比较大，此时选择大的 α 值，可以给该节点较大的惩罚，或者直接认定其是违规行为节点.

4) 如果S认为忙，而R认为空闲时，则同第3种情况，选择大的 α 值.

3.4 诊断为违规行为的策略

惩罚策略只是基于对潜在的违规行为节点的一次判断，而诊断策略是经过多次监测，通过相应的计算来确定是否为违规行为节点，并采取相应措施来处理这些行为的策略.

在该策略中需要定义两个参数 K 和 T. K 值为R接到的每个S几次发送最后一个包之和，每当接收到一个新包时，便将差值 $B_{exp0}-B_{act}$ 存到一个存储器. 若这些差值的和大于某一阈值 T，则这个S即被视为具有违规行为的节点.

当诊断出S具有违规行为时，R便会拒绝接受来自S的下一个RTS包，或者通知网络上层，采取相应的措施来处理这些具有违规行为的节点.

4 结果与分析

应用 NS-2[11] 进行模拟仿真. 使用 shadowing 的信道模型，该模型的数学表述为

$$\left[\frac{P_r(d)}{P_r(d_0)}\right]_{dB} = -10\beta\log\left(\frac{d}{d_0}\right) + X_{dB}. \tag{5}$$

式中：β 表示路径衰减指数，$P_r(d)$ 表示接收能量，$P_r(d_0)$ 表示在规定距离 d_0 内的接收能量，X_{dB} 表示高斯随机变量. 仿真参数设置如表1所示.

表1 相关参数

路径衰减指数 β	2	数据流的速率 /Mbps	2
监听范围 /m	550	背景流传输数据的速率 /Kbps	500
传输范围 /m	250	数据包大小 /bytes	512
数据流形式	CBR	仿真时间 /s	50

假设R是可信的，用带有中心基站的网络代替无线 AD HOC 网络，在R周围均匀分布8个节点来竞争信道向R传输数据，如图2所示. 为更好地反映实际的网络环境，设定两条背景流. R可以监听到两条背景流的数据传输，了解信道情况，但它们不能向R传输，以此模拟存在隐藏节点的情况.

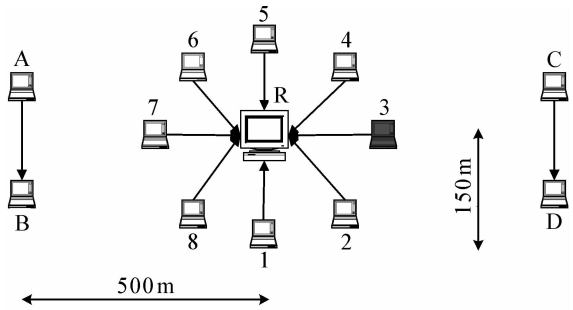

图2 仿真拓扑图

仿真时假定节点3为违规行为节点. 违规方式从两方面考虑：一是节点3一直执行违规行为，只是它所选择的退避值与规定值的偏离程度不同；二是节点3并不完全执行违规行为，它只是在某个时间内执行，本算法主要解决这种情况下的违规行为的检测.

对仿真结果的说明：正确判断率为根据诊断策略将违规节点正确判断出来的比例；逃脱判断次数为违规节点实施了违规行为，但没有被判断出来的次数；平均吞吐量为除违规节点外的其他节点吞吐量的平均值.

对于第1种违规方式，由于原算法已经给出该网络背景下的最佳网络参数($T=20, K=5, \alpha=1$)，这里只给出改进算法与原算法在该参数下的正确判断率的比较，如图3所示.

从图3可以看出，改进算法在执行违规行为比

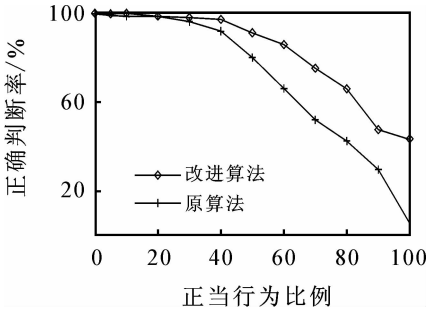

图 3　两种算法正确判断率的比较

例较高(正当行为比例小于 40%)时,比原算法效果稍好,两种算法都能很好地将违规行为正确地判断出来.但是,当节点执行违规行为的比例较小(正当行为比例大于 40%)时,改进算法比原算法正确判断出来的比例高很多,如图 3 所示.因此,改进算法在这种情况下效果更好,能更好地检测出违规行为节点.

对于第 2 种情况,当 T 和 K 值太小时,容易造成误判断;当 T 和 K 值太大时,每诊断一次节点是否为违规行为需进行多次判断,造成很大的时延,所以仿真时选择 $T=20, K=5$.

下面比较相同的 $T=20, K=5$ 时,不同 α 值情况下的正确判断率和违规节点逃脱判断的次数,如图 4 所示.

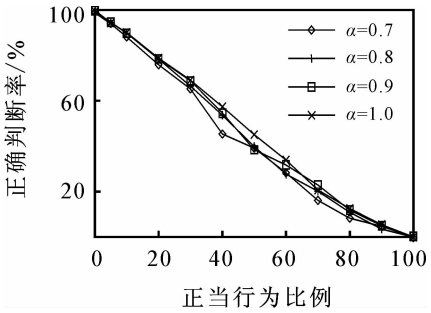

图 4　$T=20, K=5$ 时不同 α 值的正确判断率

从图 4 可以看出,在参数均为 $T=20, K=5$,而 α 值不同时,除在 $\alpha=0.7$ 时正确判断率较低外,α 值从 0.8 到 1 之间变化时正确判断率相差无几.这是因为 α 值太小时,有很多违规行为可以逃脱判断,图 5 很好地说明了这点,所以自适应调整 α 的范围选择从 0.8 到 1 之间.

以上仿真结果表明,该算法能成功地检测出违规行为节点.在此基础上进一步对该节点进行惩罚,降低违规行为给网络带来的不利影响.下面给出违规节点的吞吐量与其他节点平均吞吐量在算法改进前后的比较,以验证改进算法的优越性.

图 6 表明,违规节点的吞吐量随违规行为的比例减小而逐渐降低,而其他节点的平均吞吐量则逐渐提高,这说明在没有惩罚策略和诊断策略时,违规节点所获得的吞吐量优势是明显的.

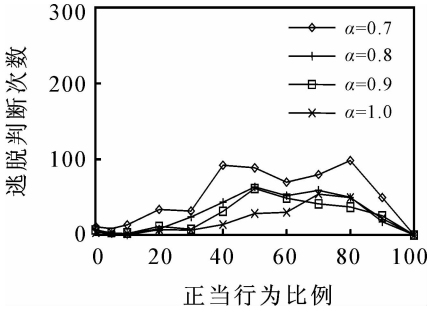

图 5　$T=20, K=5$ 时不同 α 值的逃脱判断次数

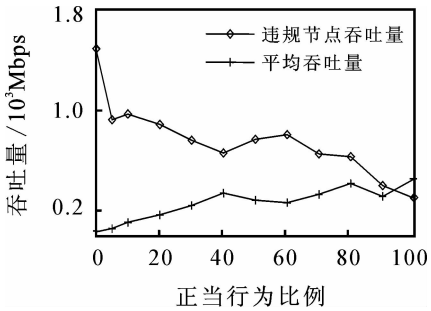

图 6　改进前违规节点吞吐量与平均吞吐量

图 7 表明,违规行为比例很大时,违规节点能获得较大的吞吐量优势,但此时很容易检测出该违规行为节点并采取相应措施.当违规行为比例不大(如正当行为比例大于 10%)时,违规节点的吞吐量下降到一个合理水平,其他节点的平均吞吐量也提高很多.这是因为虽然违规节点仍然执行违规行为,但由于惩罚策略的作用,违规节点的退避值不会一直很小,其他节点便有机会占用信道进行数据传输.这说明改进算法在正确判断出违规行为的前提下,能大幅度提高其他节点的吞吐量.

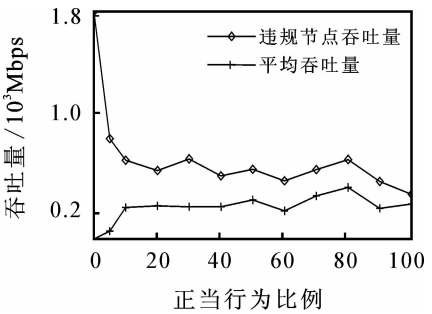

图 7　改进后违规节点吞吐量与平均吞吐量

5　结　　论

在动态和开放的无线网络环境下,部分节点为了自身的利益可能不按照标准的退避机制进行等待而占用信道,从而获得更多的网络资源.为了解决这一违规行为,本文根据标准的 IEEE802.11 协议的 DCF 机制,提出一种改进的退避算法,在惩罚策略

和诊断策略的基础上自适应调整 α 值，并采用 EIED 方法改变 CW 值，使各节点能更公平地占用信道，同时降低隐藏节点对网络的影响. 仿真结果表明，在合适的参数组合下，采用本文算法能够正确地判断出违规行为节点，并通过惩罚措施削弱其在吞吐量上的优势，使其他节点以较小的时延接入网络，实现了网络的公平性.

参考文献(References)

[1] Corson S, Macker J. Mobile Ad Hoc networking and the IETF[J]. ACM SigMobile Mobile Computing and Communications Review, 1999, 3(1): 11-13.

[2] Karn P. MACA-A new channel access method for packet radio[C]. The 9th Annual ARRL Networking Conf. London, 1990:134-140.

[3] IEEE Std. 802.11-1999, Wireless LAN-medium access control and physical layer specification[S]. 1999.

[4] Raya M, Hubaux J P, Aad I. Domino: A system to detect greedy behavior in IEEE802.11 hotspots[C]. 2nd Int Conf on Mobile Systems. Applications and Services. Boston, 2004: 84-97.

[5] Kyasanur P, Vaidya N. Detection and handling of MAC layer misbehavior in wireless networks[C]. Int Conf on Dependable Systems and Networks. San Francisco, 2003: 173-182.

[6] Zhong S, Chen J, Yang Y R. Sprite: A simple cheat-proof, credit-based system for mobile Ad Hoc networks [C]. IEEE Conf Computer Communications. San Francisco, 2003: 1987-1997.

[7] Guang L, Assi C. On the resiliency of mobile ad hoc networks to MAC layer misbehavior[C]. 2nd ACM Int Workshop on Performance Evaluation of Wireless Ad-Hoc, Sensor, and Ubiquitous Networks. Washington, 2005: 160-167.

[8] Guang L, Assi C, Ye Y H. Dream: A system for detection and reaction against MAC layer misbehavior in Ad Hoc networks [J]. Computer Communications, 2007, 30(8): 1841-1853.

[9] Song N O, Kwar B J, Song J. Enhancement of IEEE 802.11 distributed coordination function with exponential increase exponential decrease back-off algorithm [C]. Proc of IEEE VTC'2003. Orlando, 2003: 492-502.

[10] Knuth D E. The Art of computer programming[M]. 3rd ed. New York: Addison-Wesley, 2000.

[11] Fall K, Yaradhan K. NS notes and documentation[R]. San Francisco: UC Berkley, 1998.

(上接第 1651 页)

[6] Gao H, Chen T W. New results on stability of discrete-time systems with time-varying state delay[J]. IEEE Trans on Automatic Control, 2007, 52(2): 328-334.

[7] Zhang X M, Han Q L. A new finite sum inequality approach to delay-dependent H_∞ control of discrete-time systems with time-varying delay[J]. Int J of Robust and Nonlinear Control, 2008, 18(6): 630-647.

[8] Fridman E, Shaked U. Delay-dependent H_∞ control of uncertain discrete delay systems [J]. European J of Control, 2005, 11(1): 29-37.

[9] Mariton M. Jump linear systems in automatic control [M]. New York: Dekker, 1990.

[10] Boukas E K, Liu Z K. Robust H_∞ control of discrete-time Markovian jump linear systems with mode-dependent time-delays[J]. IEEE Trans on Automatic Control, 2001, 46(12): 1918-1924.

[11] Chen W H, Guan Z H, Yu P. Delay-dependent stability and H_∞ control of uncertain discrete-time Markovian jump systems with mode-dependent time delays[J]. Systems & Control Letters, 2004, 52(5): 361-376.

[12] Boukas E K, Liu H P. Delay-dependent stabilization of stochastic discrete-time systems with time-varying time-delay[C]. Proc of the American Control Conf. New York, 2007: 2448-2453.

[13] Petersen I R, Hollot C V. A Riccati equation approach to the stabilization of uncertain linear systems [J]. Automatica, 1986, 22(4): 397-411.

[14] Jiang X F, Han Q L. New stability criteria for linear systems with interval time-varying delay [J]. Automatica, 2008, 44(10): 2680-2685.

[15] Xu S Y, Lam J. On equivalence and efficiency of certain stability criteria for time-delay systems [J]. IEEE Trans on Automatic Control, 2007, 52(1): 95-101.

[16] Ghaoui L E, Oustry F, AitRami M. A cone complementarity linearization algorithm for static output feedback and related problems[J]. IEEE Trans on Automatic Control, 1997, 42(8): 1171-1176.