一种应用干扰消除进行冲突消解的分布式无线MAC协议

沈 虎 吕绍和 王晓东 周兴铭
(国防科技大学计算机学院并行与分布式处理国家级重点实验室 长沙 410073)

摘 要 媒介接入控制(MAC)用以协调无线节点对公共信道的共享,对无线网络性能有至关重要的影响。传统的MAC协议只能抑制冲突,不能根除及处理冲突。提出了一种基于已知干扰消除技术的新型消解冲突方法,并以此为基础设计了一个全新的MAC协议——CR-MAC。在CR-MAC协议中,无线接入点(AP)通过将部分报文传输与已知干扰消除相结合来解码冲突所包含的所有报文。因此发生冲突的报文传输过程能够被充分利用,且所需的报文重传减少了。实验结果表明,在网络吞吐率及预期报文时延指标上,CR-MAC协议较普遍采用的IEEE 802.11 DCF协议均有明显优势。

关键词 干扰消除,媒介接入控制,冲突消解,报文重传
中图法分类号 TP311 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.12.014

Distributed Collision-resolvable MAC Protocol for Wireless LANs with Interference Cancellation Support

SHEN Hu LV Shao-he WANG Xiao-dong ZHOU Xing-ming
(National Key Lab of Parallel and Distributed Processing, College of Computer, National University of Defense Technology, Changsha 410073, China)

Abstract Medium access control is critical to wireless network performance. We introduced a novel collision resolution method based on known interference cancellation, and proposed a new MAC protocol named as CR-MAC. Basically, AP tries to decode all the data packets in a collision by combining partial retransmissions and known interference cancellation. Hence, the collided transmission can be fully utilized, and less retransmission is required. The simulation results show that CR-MAC performs much better than IEEE 802.11 DCF in terms of both the aggregation throughput and the expected packet delay under various network settings.

Keywords Interference cancellation, Medium access control, Collision resolving, Packet retransmission

1 引言

由于无线局域网可用的信道带宽资源非常稀缺,多个无线节点只能共享同一个信道。为避免冲突并提升网络传输性能,需要设计实用且高效的媒介接入控制协议。工业界普遍采用的MAC协议标准簇——IEEE 802.11 a/b/g/n,均按照时间维度将公共信道资源划分为多个时间片,并将这些时间片分别指派给节点使用。当两个以上的节点同时使用一个时间片进行报文传输时,会导致一个报文冲突的发生,并且在这个冲突中所有传输的报文都将无法被正常接收。不幸的是,报文冲突在无线局域网中并不只是偶然出现:有实测结果表明在无线局域网中有超过10%的通信链路会由于报文冲突而产生严重的丢包现象[1];当网络中存在隐藏终端时丢包问题更加严重,进而导致网络性能急剧下降或单个节点独占信道,其他节点无法正常接入[2]。

为消除无线局域网的报文冲突,IEEE 802.11协议簇主要采用了两种机制:基于指数退避的载波侦听机制以及RTS/CTS握手机制。利用载波侦听机制,发送节点侦听信道状态:当信道忙碌时,节点退后其报文传输;当该节点与其他节点发生报文冲突时,冲突节点倍增其竞争窗口大小。令人遗憾的是,载波侦听机制无法处理隐藏终端产生的问题。因此,IEEE 802.11协议还另外提出了RTS/CTS握手机制——每个发送节点先对信道使用权进行预约,预约成功后方允许其进行报文传输。但这些机制都有非常高的控制开销,并且这种开销在短数据帧、高物理层数据率或长距离网络中显得尤为突出[3-5]。

IEEE 802.11协议簇在处理报文冲突方面的低效根源在于IEEE 802.11采用的是冲突避免思路:一方面,简单地丢弃发生冲突的报文意味着在整个冲突传输过程中没有任何有用的数据得以传递;另一方面,非常高比例的时间槽被用于规避冲突而不是进行报文传输。

为提升IEEE 802.11 DCF的通信效率,Cali等提出了一

到稿日期:2014-01-01 返修日期:2014-03-22 本文受国家自然科学基金项目(61070203,61202484),国家教育部高等学校博士学科点专项科研基金项目(20124307120033),国防科技大学优秀研究生创新基金项目(B120608)资助。

沈 虎(1986-),男,博士生,主要研究方向为无线网络传输协议及调度算法,E-mail:shenhu@nudt.edu.cn;吕绍和(1982-),男,博士,主要研究方向为无线自组织网络及机器学习;王晓东(1973-),男,教授,主要研究方向为无线网络及社交网络;周兴铭(1938-),男,教授,院士,主要研究方向为高性能计算及无线网络。

种最佳优化竞争窗口大小的方案[6]；Y. He 等引入了一种能够为每个节点设置一个目标退避时间的半随机退避机制[7]；Z. Zeng 等将多个节点形成一个竞争组，以此减少单个竞争域内竞争实体的数量[8]。此外，一些最新的研究提出以一种新型的频域竞争方法来取代时域内的指数退避的方法[9-11]。上述工作都有效地减少了节点平均退避时间，但没有从根本上解决报文冲突问题。

近年来，对无线网络进行干扰管理乃至解码冲突报文成为了无线网络 MAC 协议研究的新趋势。其中，S. Verdu 首先提出了采用相继干扰消除(SIC)技术解码冲突[12]，并由 D. Halperin 通过构建 SIC 实验原型系统验证了该想法的可行性[13]。但是，相继干扰消除需要满足极其严格的信干噪比(SINR)约束，因此该技术所带来的性能增益在许多场景中并不容易实现[14]。MIT 的 Gollakota 等人开发了一种新的干扰消除技术 ZigZag 用以解码多个报文的冲突[15]，但是由于 ZigZag 解码报文中的符号(symbol)是有依赖关系的，以此解码错误会不断累积。此外，Li 等人探讨了随机线性解码[5]，但其需要在网络中进行信道状态信息(CSI)的广播，这对于无线网络是一个沉重的负担。

在本文中，我们探讨了采用一种新的信号处理手段即已知干扰消除(KIC)[16]来处理无线网络中的报文冲突，并且通过主动重传而非被动监听来增强其解码可能性。此外，我们基于已知干扰消除消解冲突的能力设计了一个全分布式的 MAC 协议。据我们所知，我们所提出的 CR-MAC 是第一个利用已知干扰消除和部分重传来提升信道共享效率的方案。

本文的主要贡献包括：(1)我们将信道共享的研究转向一个新的方向，即由传统的冲突避免到全新的冲突消解，并据此设计了一个新的冲突可消解 MAC 协议(CR-MAC)。在 CR-MAC 协议中，无线接入点将缓存最新的冲突报文，然后通过利用部分冲突报文重传及已知干扰消除等手段逐步对冲突报文进行消解。(2)我们所设计的 CR-MAC 协议能以完全分布式的方式进行工作，并且并不需要提供额外的控制开销。(3)我们进行了大量的模拟试验，结果表明 CR-MAC 协议较 IEEE 802.11 有明显的性能优势。

本文首先对相关研究工作进行了总结；第 2 节介绍了干扰消除等信号处理的相关背景知识；第 3 节描述了 CR-MAC 协议的框架及设计细节；第 4 节给出了一个理论模型用于分析及评估新协议的网络性能；第 5 节提供了模拟试验结果；最后总结全文。

2 干扰消除技术

2.1 未知干扰消除与已知干扰消除

在传统理念中，若在一个接收节点处有两个及以上相互干扰的报文传输，则产生了一个报文冲突。在此情形下，目标信号只能通过捕获效应进行解码，并且目标信号需要远强于其他干扰信号且满足一定的 SINR 阈值，才能解码正确。

最近不断发展的信号处理技术表明通过重建干扰信号并将其从混合信号中进行消除，有可能使得目的信号被正确解码[13]。通过这种干扰消除技术，即使目标信号不满足直接解码所需的 SINR 阈值，接收节点依然可以成功解码该目标信号，而由此带来的性能增益取决于接收节点刻画干扰的能力。

若一个接收节点没有干扰信号的先验知识，称该干扰为未知干扰。消除未知干扰需要未知干扰与目标信号满足严格的串行 SINR 约束条件及解码要求，因此多个节点的报文传输必须被细致地调度及指派，这在分布式网络中显然是不切实际的。与未知干扰相对应的已知干扰(KI)指的是在消除流程接收节点已知的干扰信号，因此无论已知干扰与目标信号之间的大小关系如何，已知干扰都可以被重建并从原始的冲突信号中移除：若已知干扰强于目标信号，移除已知干扰可以提供解码目标信号的可能；另外，当已知干扰比目标信号弱时，移除已知干扰可以提升目标信号的 SINR 值，从而增加目标信号可取的数据传输率。总而言之，未知干扰消除，如相继干扰消除，不需要任何附加的先验知识，但其性能增益有限并且不容易实现。反之，已知干扰消除可以提供更多的性能增益但需要获知干扰信号。

2.2 已知干扰消除流程

一个具备已知干扰消除能力的接收节点首先尝试对接收信号进行直接解码。如果 CRC 校验失败，接收节点可以通过能量检测的方法检查是否发生了报文成功(当多个信号混合叠加时，混合信号的能量较单个信号会处于一个明显更高的水平)。当报文冲突发生并且其中部分冲突报文能够通过报头识别时，这个冲突可以被归为潜在的可消解冲突，然后接收节点扫描其缓存空间并进行报头信息对比，以判断缓存中是否存在包含在上述冲突中的报文。如果冲突报文与缓存报文能匹配上，则通过已知干扰消除操作可以将该已知报文从冲突中移除，然后再对残余冲突信号进行解码，有可能可以获取一个新的未知报文。

已知干扰消除的关键步骤在于对冲突中包含的已知干扰信号进行重建。其中，需要利用前导码及能被正确接收的部分数据来辅助对无线信道进行建模，在此我们采用了文献[13]所使用的信道建模方法，该方法整体考虑所有的信道参数包括衰落、频率偏移及符号间干扰等，并以单个信道函数 $R(t)$ 进行表征。为响应无线信道的时变性，每隔 3 个连续报文符号就对信道函数 $R(t)$ 进行一次更新。然后冲突中相对应的已知干扰信号可以通过应用信道函数 $R(t)$ 于已知报文符号而得到，接着从冲突信号中移除这些已知干扰信号，并将新的残余冲突信号传递到下一个解码过程。

3 CR-MAC 协议

3.1 主体框架

我们考虑一个单跳无线局域网上行链路的情形，其中有一个位于网络中央的无线接入点 AP 及其它的 n 个客户端节点，每个客户端节点能够直接与 AP 相连。我们所提出的 CR-MAC 协议基于 IEEE 802.11 DCF 协议[18]而设计，CR-MAC 的主要设计思路是当一个报文冲突发生时，AP 将检测其是否可消解，若为可消解冲突，则冲突信号中包含的部分冲突报文会被马上安排在后继的时间槽内进行重传，最后借助于已知干扰消除操作，所有的冲突报文将被顺利接收。换言之，部分冲突报文可以从冲突信号及重传的其他冲突报文中推断而来，则其相对应的重传可得以精简，故 CR-MAC 凭此可以大为提升网络性能。例如，若发生一个包含两个冲突报文的可消解冲突，CR-MAC 仅仅只需要安排其中的一个冲突

报文在下一个传输时间槽内进行重传，那么另外一个冲突报文就可以通过冲突信号与后继的重传信号之间的已知干扰消除操作来获得。因此发生冲突的传输时间槽被有效利用，并且报文重传只需要一个额外的时间槽。而在其他传统的MAC协议中，传输两个相冲突的报文，至少需要安排两个传输时间槽。

如图1所示，CR-MAC协议将整个传输周期分为两个部分：随机接入部分和数据传输部分。CR-MAC协议的随机接入使所有客户端节点能够以相同的概率访问共同信道，此外它还可以减少发生冲突时所涉及的冲突节点数目，这是非常有必要的，因为过多的节点同时传输数据将导致所发生的冲突很有可能是不可消解的，即所发生的冲突传输过程是无效的、不可被利用的。而CR-MAC协议的数据传输部分包括一个数据传输阶段及若干个可能的数据重传阶段，且每个数据传输或重传阶段均包括一个数据传输及其对应的确认报文传输。

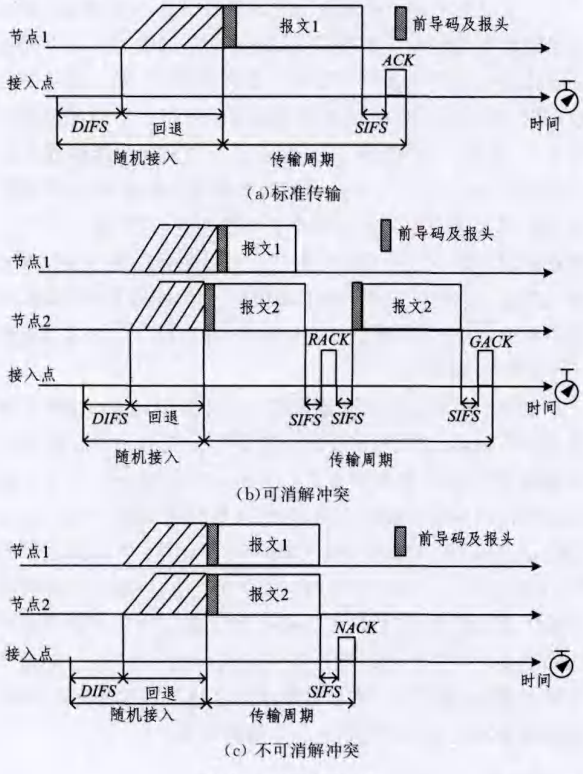


图1 协议流程样例

CR-MAC协议的随机接入机制与IEEE 802.11 DCF的指数退避机制相似，两者的区别在于在CR-MAC协议中，客户端节点只有在遭遇不可消解冲突时才增加其竞争计数器；而在IEEE 802.11 DCF中，只要冲突(包括可消解冲突和不可消解冲突)发生，冲突的客户端节点就倍增其竞争计数器。

CR-MAC协议的数据传输机制则较为复杂，在随机接入之后根据并发接入信道的节点数目可以分为3种情形。

(1)标准传输：在这种情形中，只有一个客户端节点接入信道并传输数据，如图1(a)所示。而AP在正确接收完数据后等待一段SIFS空闲时间，再发送一个标准ACK报文进行确认。

(2)可消解冲突：在这种情形中，有多个客户端节点同时接入信道并传输数据，这里我们假设并发接入节点数目为K，则产生了一个包含K个数据报文的冲突。若这些冲突报文的前导码及报头相互是非重叠的，如图1(b)所示，那么所发生的冲突信号是可消解的。经过$K-1$步串行重传及对应的已知干扰消除操作，所发生的冲突信号包含的K个冲突报文能够全部被AP正确解码。需要特别指出的是，每个数据重传阶段是由上一个数据传输或重传阶段的RACK报文所发起的，而最后一个数据重传阶段是由GACK报文来对所有未确认的报文进行确认。

(3)不可消解冲突：在这种情形中，有一些冲突报文的前导码及报头相互是部分或者完全重叠的，如图1(c)所示，因此已知干扰消除操作无法进行。AP会广播一个NACK报文表明其收到一个不可消解冲突，则所涉及到的冲突节点会倍增其竞争计数器。

3.2 协议设计细节

3.2.1 前导码及报头

在一个报文中增加前导码的目的是通知接收节点一个信号的到来并同步接收节点的解调器。报文前导码由12个训练符号构成，其中的10个短训练符号用于调整AGC(自动增益控制)、参差选择及对载波信号进行初步的频偏估计，此外接收节点使用其它的2个长训练符号进行信道建模及细粒度的频偏估计。而报文头部(报头)由4个速率比特、1个预留比特、12个长度比特、1个检验比特、6个尾比特及16个服务比特构成，此外我们还在报头增加了一个报文源地址字段用以标识发送报文的节点。整个报文前导码及报文使用BPSK调制并以6Mbps速率进行传输。PPDU报文格式如图2所示。

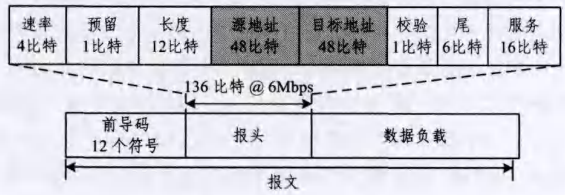


图2 PPDU报文格式

如前所述，一个冲突信号是否可消解取决于所含冲突报文的前导码及报头是否可区分(重叠与否)。但是，由于在无线局域网中AP会周期性地发送beacon报文来同步所有客户端节点的时钟，因此冲突报文的前导码及报头很有可能是会完全或部分重叠的，如图3(b)所示。为了增加冲突信号的可消解性，我们采用文献[19]所使用的方法，即在每个数据报文尾部增加后导码及报尾，其中的后导码与前导码具有同样内容，报尾与报头具有同样内容，但后导码及报尾的所有比特是反向的。当冲突报文一端对齐时，由于具有不同的报文长度及数据传输速率，这些冲突报文的另一端就能够区分开来。若冲突信号中有未被侵腐的报文后导码及报尾(或前导码及报头)，如图3(c)或图3(a)所示，则AP可以在不解码整个报文的情况下通过利用后导码(或前导码)中的训练序列解码报尾(或报头)，这样AP就能够知道冲突信号含有的冲突报文信息(主要是其源节点地址)，然后再安排在下一个传输时间槽内对冲突报文进行重传。

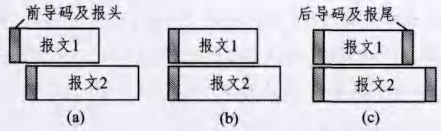


图3 报文重叠的3种情形

3.2.2 ACK 帧的修改

如图 4 所示，AP 将传递 4 种类型的确认报文。第一种确认报文是与 IEEE 802.11 相同的标准 ACK 报文，用以确认未遭受干扰能被 AP 成功接收的数据报文。第二种确认报文是 RACK(重传 ACK)，它不是对报文进行确认，而是要求某个冲突节点重传其最近传输的数据报文。RACK 中有一个附加的 ACK 控制字段，它是用来表示 ACK 帧的类型，该字段在 RACK 中取值为 0000。第三种确认报文是 GACK(组 ACK)，用以在重传及已知干扰消除结束后对冲突信号所含的所有 K 个冲突报文进行一次性确认，因此 GACK 帧的接收地址字段被扩充为 K 个地址字段。最后一种确认报文是 NACK(否定 ACK)，用以广播 AP 遭遇到一个不可消解冲突。NACK 帧没有接收地址字段，其附加的 ACK 控制字段取值为 1111。

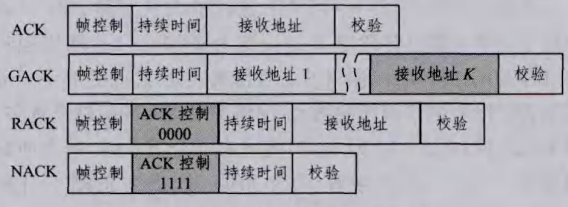


图 4 不同确认报文的帧格式

3.2.3 兼容性问题

在 CR-MAC 协议中，对传统 IEEE 802.11 MAC 的修改主要是在软件层面进行的。对于客户端节点而言，它们仅仅需要辨别 4 种不同类型的 ACK 帧，然后根据不同情形决定是重传还是等待下一次传输周期的到来。AP 端的修改则较为复杂，不仅需要更改 ACK 帧格式，还要改变其解码流程。

遗留节点(运行传统 IEEE 802.11 MAC 协议的节点)是可以在 CR-MAC 协议中共存的。当一个遗留节点加入到运行 CR-MAC 协议的网络，获得信道使用权并开始传输数据时，网络中的 AP 及其它客户端节点会保持沉默，因为它们会探测到此时信道处于忙碌状态。两种结果可能发生：1)若遗留节点收到一个给它的标准 ACK 确认报文，则该遗留节点进入到下一个报文的流程；2)否则，遗留节点在等待 ACK 确认报文最大回应时间 $T_{timeout}$ 后进入报文重传流程。而遗留节点也不会干扰或中断其它客户端节点正在进行的数据传输或重传，理由是在其它节点进行数据传输及后续重传过程中信道始终处于锁定状态。遗留节点进行数据传输对 CR-MAC 协议的唯一影响在于若一个可消解冲突包含来自遗留节点的报文，由于遗留节点无法响应 RACK 及 GACK，则 AP 对该冲突的处理会失败。总之，尽管遗留节点的存在会影响网络性能，但其依然可以与我们所提出的 CR-MAC 协议相兼容。

4 性能分析

假设报文负载 L 满足几何分布，其取值区间为 $[L_{\min}, L_{\max}]$。此外，为使问题简单化，假定所有客户端节点保持恒定的数据传输率 R_{data}，已知干扰消除操作只用于两个报文的冲突，这意味着可消解冲突所涉及的并发传输节点数 K 限制为 2。

如果一个冲突信号包含两个报文，其报文长度分别为 L_1 和 L_2，则标记该冲突可消解的概率为 $p_r(L_1, L_2)$。我们假设冲突信号所包含的两个报文在报头端是严格对齐的，那么 $p_r(L_1, L_2)$ 可计算如下：

$$\begin{aligned} p_r(L_1,L_2) &= p(L_1>L_2+L_{ph}\,|\,L_1>L_2)+p(L_2>L_1+L_{ph}\,|\,L_2>L_1) \\ &= 2p(L_1>L_2+L_{ph}\,|\,L_1>L_2) \end{aligned} \tag{1}$$

式中，L_{ph} 表示报文中前导码及报头的有效长度。$p_r(L_1, L_2)$ 的期望值为：

$$\begin{aligned} p_r &= E[p_r(L_1,L_2)] \\ &= 2E[p(L_1>L_2+L_{ph}, L_1>L_2)\cdot p(L_1>L_2)] \\ &= E[p(L_1>L_2+L_{ph}, L_1>L_2)] \\ &= E\left[\frac{L_{\max}-(L_2+L_{ph})}{L_{\max}-L}\right] \\ &= 1-\frac{L_{ph}}{L_{\max}-E[L_2]} = 1-\frac{2L_{ph}}{L_{\max}-L_{\min}} \end{aligned} \tag{2}$$

这里标识竞争节点数目为 n，最小竞争窗口大小为 W，最大退避次数为 m，节点传输概率为 τ。此外每个节点的条件冲突概率 p 被假定为常值，即与节点所经历的重传次数无关，这个假设已经在 Bianchi 的文献[20]中得以验证。这里，根据实际情况拓展 Bianchi 的求解模型如下：

$$p = 1-(1-\tau)^{n-1}-p_r\cdot C_{n-1}^{1}\tau(1-\tau)^{n-2} \tag{3}$$

$$\tau = \frac{2(1-2p)}{(1-2p)(W+1)+p\cdot W(1-(2p)^m)} \tag{4}$$

式(3)反映了只有一个节点接入信道或者有两个节点接入信道，但所产生的冲突可消解时，AP 均可以顺利对数据传输进行解码。否则，视 AP 遭遇到一个不可消解冲突。

由节点传输概率 τ，可以分别计算 p_{tr}，p_s^1，p_c^2，p_c 如下：

$$p_{tr} = 1-(1-\tau)^n \tag{5}$$

$$p_s^1 = n\cdot\tau\cdot(1-\tau)^{n-1}/p_{tr} \tag{6}$$

$$p_c^2 = C_n^2\tau^2(1-\tau)^{n-2}/p_{tr} \tag{7}$$

$$p_c = 1-p_s^1-p_r\cdot p_c^2 \tag{8}$$

其中，p_{tr} 表示在指定传输时间槽内至少有一个节点传输数据的概率，p_s^1 表示正好只有一个节点在公共信道传输数据的概率，p_c^2 表示有两个节点在公共信道传输数据的概率，p_c 表示由于遭遇一个不可消解冲突导致数据传输失败的概率。

由图 1 可知，在标准传输及可消解冲突情形下，AP 是能够正确解码数据报文，而在不可消解冲突情形下，数据解码会失败。此外，所考虑的传输时间槽有可能处于空闲状态，即没有任何节点进行数据传输。在此，分别计算各种传输情形所占用的时间如下：

$$\begin{aligned} T_s^1 &= DIFS+\delta+T_H+E[L/R_{data}]+SIFS+\delta+T_{ACK} \\ &= DIFS+2\delta+T_H+\frac{L_{\max}+L_{\min}}{2R_{data}}+SIFS+T_{ACK} \end{aligned} \tag{9}$$

$$\begin{aligned} T_s^2 &= DIFS+\delta+2T_H+E\left[\frac{L}{R_{data}}\,|\,L_1>L_2+L_{ph}\right]+3SIFS \\ &\quad +3\delta+T_{RACK}+T_{GACK} \\ &= DIFS+\frac{L_{\max}+L_{\min}+2L_{ph}}{R_{data}}+3SIFS+4\delta+2T_H+ \\ &\quad T_{RACK}+T_{GACK} \end{aligned} \tag{10}$$

$$\begin{aligned} T_c &= DIFS+\delta+T_H+E\left[\frac{\max\{L_1,\cdots,L_K\}}{R_{data}}\right]+SIFS+ \\ &\quad \delta+T_{NACK} \\ &\triangleq DIFS+SIFS+\delta+T_H+T_{NACK}+\frac{L_{\max}}{R_{data}} \end{aligned} \tag{11}$$

其中，T_s^1 表示在标准传输情形下进行一次成功传输所占用信道的平均时间，T_s^2 表示在可消解冲突情形下完成一次成功传输所占用信道的平均时间，T_c 表示在不可消解冲突情形下进

行一次失败传输所占用信道的平均时间，σ 表示一个空闲传输时间槽所持续的时间。此外，式(9)－式(11)中 T_{ACK}，T_{PACK}，T_{GACK}，T_{NACK} 分别表示用以传输 ACK，PACK，GACK，NACK 报文所需的时间，δ 表示传播时延。$H=PHY_{hdr}+MAC_{hdr}+L_{ph}$ 是物理层、MAC 层等报文开销，T_H 是传输报文开销所需时间。

需要指出的是，Bianchi 的分析针对的是饱和状态场景，即所有节点始终有数据报文等待传输。针对非饱和状态场景，Malone 等给出了另外一个理论分析模型[21]，他们指出两者的差别在于节点传输概率 τ 的计算。在非饱和状态场景，可计算节点传输概率 τ 如下：

$$\tau=b_{(0,0)e}\cdot\frac{q^2}{1-q}\cdot\left(\frac{W}{(1-p)(1-(1-q)^W)}-(1-p)\right) \tag{12}$$

$$\begin{aligned}b_{(0,0)e}=&(1-q)+\frac{q^2\cdot W\cdot(W+1)}{2(1-(1-q)^W)}+\frac{q\cdot(W+1)}{2(1-q)}\cdot\\&\left(\frac{q^2\cdot W}{2(1-(1-q)^W)}+p\cdot(1-q)-q\cdot(1-p)^2+\right.\\&\frac{p\cdot q^2}{2(1-p)(1-q)}\cdot\left(\frac{W}{1-(1-q)^W}-(1-p)^2\right)\cdot\\&\left.\left(2W\cdot\frac{1-p-p(2p)^{m-1}}{1-2p}+1\right)\right.\end{aligned} \tag{13}$$

其中，q 表示数据报文在一个节点的生成概率。当 q 取值为 1 时，非饱和状态转变为饱和状态。

5 性能评测

本节将根据上一节建立的理论分析模型对 CR-MAC 协议进行数值模拟实验，并将其与标准的 IEEE 802.11 DCF 协议的实验结果进行对比。

在实验中，考虑一个单跳全连通的无线局域网，设置网络范围为 $500\times500m^2$，其中有一个位于网络中心的 AP 以及随机散布在 AP 周围的若干客户端节点。我们的实验主要考虑了两个网络性能指标：

(1)网络吞吐量 S (Mbps，兆比特每秒)，定义为在给定网络负载下单位时间内网络成功传输有效报文负载的比特数量。网络吞吐量 S 可计算如下：

$$S=\frac{E[\text{一个传输周期内传递的报文负载比特数}]}{E[\text{一个传输周期的时间长度}]} \tag{14}$$

$$\begin{aligned}S=&[E[L]\cdot p_s^1+(E[L_1]+E[L_2])\cdot p_r\cdot p_c^2]/[(1-p_{tr})\cdot\\&\sigma+p_{tr}\cdot p_s^1\cdot T_s^1+p_{tr}\cdot p_c^2\cdot T_s^2+p_{tr}\cdot(1-p_s^1-p_r\cdot\\&p_c^2)\cdot T_c]\end{aligned} \tag{15}$$

特别地，将随网络负载增大而能达到的网络吞吐量极限称为饱和吞吐量。要达到饱和吞吐量，网络中所有节点都要工作在饱和条件[20]下，即每个节点待传输的数据队列永远不为空队列。

(2)报文预期时延 $E[D]$ (second，秒)，定义为传输一个报文所需要的时间，这段时间从报文成为节点报文队列头部开始，到节点收到对该报文的确保 ACK 结束。$E[D]$可表述如下[22]：

$$E[D]=E[X]E[l] \tag{16}$$

其中，X 表示计数器递减的次数，即节点退避初始值；l 表示退避计数器两次连续递减的间隔时间。

$$\begin{aligned}E[l]=&(1-p_{tr})\cdot\sigma+p_{tr}\cdot p_s^1\cdot T_s^1+p_{tr}\cdot p_r\cdot p_c^2\cdot T_s^2+\\&p_{tr}\cdot(1-p_s^1-p_r\cdot p_c^2)\cdot T_c\end{aligned} \tag{17}$$

$$\begin{aligned}E[X]=&\sum_{i=0}^{m-1}\left(p^i+\frac{W_i+1}{2}\right)+\frac{p^m}{1-p}\cdot\frac{W_m+1}{2}\\=&(1-2p)\cdot(W+1)+\frac{p\cdot W(1-(2p)^m)}{2(1-2p)(1-p)}\end{aligned} \tag{18}$$

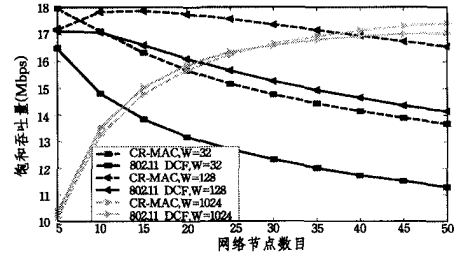
其它重要的网络参数配置如表 1 所列。

表 1 网络参数设置

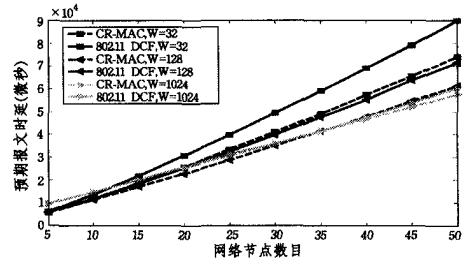
参数	值	参数	值
m	7	L_{ph}	48us
δ	1us	L_{min}	1000bits
σ	9us	L_{max}	40000bits
SIFS	16us	ACK	120bits+PHY_{hdr}
DIFS	34us	RACK	124bits+PHY_{hdr}
PHY_{hdr}	40us	GACK(K=2)	168bits+PHY_{hdr}
MAC_{hdr}	288bits	NACK	72bits+PHY_{hdr}
R_{data}	6Mbps		

5.1 饱和状态

首先在饱和状态网络场景下进行了大量实验。图 5(a)描述了当节点数据传输率 R_{data} 固定为 24Mbps 时，网络饱和吞吐量与网络规模(以网络节点数目来表征)之间的关系。可观察得知随着网络规模的增大，网络中发生的冲突越来越多：设置竞争窗口大小 W 为 32，当网络有 5 个节点时，报文冲突概率为 9.55%；当网络有 50 个节点时，报文急剧上升到 30.65%。虽然增大竞争窗口 W 能够降低报文冲突概率进而提升网络性能，但一方面这种性能提升相当有限，另一方面竞争窗口 W 的增大会导致更多的空闲时间槽，这可能损害网络性能，例如当竞争窗口 W 自 128 增大到 1024 时，对于小规模的网络(节点数目小于 20)而言网络性能非但没有提升，反而大幅度下降。不同于通过优化网络参数来减少冲突，我们采用了干扰消除与部分重传相结合的冲突消解机制，因此一些可消解冲突的传输过程得到了充分利用，与之相对应的报文重传可以得到精简。虽然本文采取的干扰消除操作仅限于两个报文的冲突，但在绝大多数情况下，我们所设计的 CR-MAC 协议明显优于 IEEE 802.11 DCF 协议，所带来的网络吞吐量增益在 10%到 25%之间。



(a)饱和吞吐量

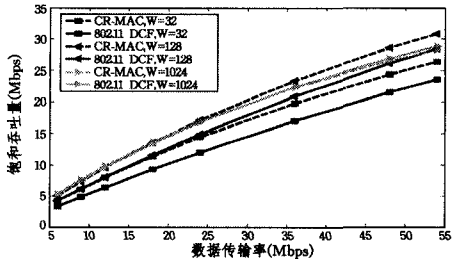


(b)报文预期时延

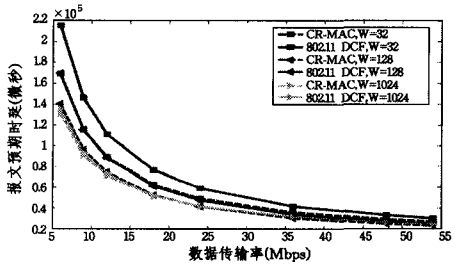
图 5 数据传输率为 24Mbps 时，饱和条件下的网络性能比较

图 5(b)向我们展示了 CR-MAC 协议不仅能够提高网络饱和吞吐量 S，而且能够降低报文预期时延 $E[D]$。当竞争窗口 W 为 32，128 及 1024 时，所带来的报文预期时延增益分别

为 16.65%，12.33%及 2.04%。此外从图 5 及图 6 可以得出这样的结论：CR-MAC 协议所带来的性能增益，包括饱和吞吐量及报文预期时延两个方面，是独立于诸多具体网络参数（如竞争窗口 W、网络节点数目 n 及数据传输率 R_{data}）的设定的；并且 CR-MAC 协议可以与退避优化及速率自适应相兼容。



(a)饱和吞吐量

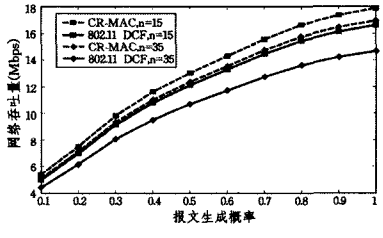


(b)报文预期实验

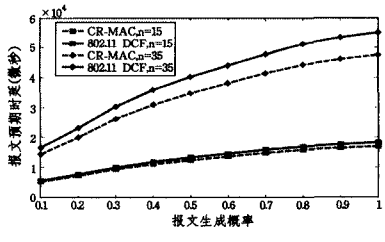
图 6　网络节点数设置为 35 时，饱和条件下的网络性能对比

5.2　不饱和条件

这一小节研究了不饱和条件下两个协议的网络性能。图 7(a)及图 7(b)比较了两个网络场景下的网络吞吐量及报文预期时延：第一个场景的网络规模为 15 个节点，第二个场景的网络规模为 35 个节点。如图 7 所示，随着网络负载不断增加，网络吞吐量及报文预期时延均有所增加。此外，较小规模的网络拥有更好的网络性能，即有较大的网络吞吐量及较小的报文预期时延，这是因为在小规模网络中参与竞争信道的网络节点较少，因而报文冲突几率随之减小。而 CR-MAC 协议在处理冲突方面有明显优势，故两种协议的网络性能差异在网络负载较重时更为显著。最后，实验结果表明无论网络负载还是网络规模发生变化，CR-MAC 协议在网络吞吐量及报文预期时延两个方面均有明显的优势。



(a)网络吞吐量



(b)报文预期时延

图 7　竞争窗口设为 128 时，不饱和条件下的网络性能比较

结束语　本文提出了一个基于已知干扰消除的新型冲突消解方法，并以此设计了一个新的 MAC 协议即 CR-MAC。在所提出的 CR-MAC 协议中，当一个可消解冲突发生时，部分冲突报文被安排在随后的传输时间槽内进行重传，通过已知干扰消除技术，AP 可以解码出冲突信号中的所有数据报文。因此，冲突信号的传输过程得以有效利用，其所需的报文重传得以精简。实验结果表明无论网络参数的设置条件，在网络吞吐率及预期报文时延指标上，CR-MAC 协议均较普遍采用的 IEEE 802.11 DCF 协议有明显优势。

参 考 文 献

[1] Cheng Y C, Bellardo J, Benk P, et al. Jigsaw: Solving the Puzzle of Enterprise 802.11 Analysis [C]// Proceedings of the ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communications (SIGCOMM). 2006: 39-50

[2] Khurana S, Kahol A, Jayasumana A P. Effect of Hidden Terminals on the Performance of IEEE 802.11 MAC Protocol [C]// Proceedings of the IEEE Conference on Local Computer Networks (LCN). 1998: 12-20

[3] Chatzimisios P, Boucouvalas A C, Vitsas V. Effectiveness of RTS/CTS Handshake in IEEE 802.11a Wireless LANs [J]. IET Electronics Letters, 2004, 40(14), 2004: 915-916

[4] Xu K, Gerla M, Bae S. Effectiveness of RTS/CTS Handshake in IEEE 802.11 Based Ad Hoc Networks [J]. Ad Hoc Network, Elsevier, 2003, 1(1): 107-123

[5] Li T, Han M K, Bhartia A, et al. CRMA: Collision-Resistant Multiple Access [C]// Proceedings of the ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communications (SIGCOMM). 2011: 61-72

[6] Cali F, Conti M, Gregori E. Dynamic Tuning of the IEEE 802.11 Protocol to Achieve a Theoretical Throughput Limit [J]. ACM Transaction on Network, 2000, 8(12): 785-799

[7] He Y, Yuan R, Sun J, et al. Semi-Random Backoff: Towards Resource Reservation for Channel Access in Wireless LANs [C]// Procee-dings of the IEEE International Conference on Network Protocols (ICNP). 2009: 21-30

[8] Zeng Z, Gao Y, Tan K, et al. Chain: Introducing Minimum Controlled Coordination into Random Access MAC [C]// Proceedings of the IEEE International Conference on Computer Communications (INFOCOM). 2011: 2669-2677

[9] Tan K, Fang J, Zhang Y, et al. Fine Grained Channel Access in Wireless LAN [C]// Proceedings of the ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communications (SIGCOMM). 2010: 147-158

[10] Sen S, Choudhury R R, Nelakuditi S. No time to countdown: Migrating backoff to the frequency domain [C]// Proceedings of the ACM Annual International Conference on Mobile Computing and Networking (MOBICOM). 2011: 241-252

[11] Feng X J, Zhang J, Zhang Q, et al. Use Your Frequency Wisely: Explore Frequency Domain for Channel Contention and ACK [C]// Proceedings of the IEEE International Conference on

Computer Communications (INFOCOM). 2012:549-557

[12] Verdu S. Multiuser Detection [M]. Cambridge University Press,1998

[13] Halperin D, Anderson T E, Wetherall D. Taking the Sting Out of Carrier Sense: Interference Cancellation for Wireless LANs [C]// Proceedings of the ACM Annual International Conference on Mobile Computing and Networking (MOBICOM). 2008:339-350

[14] Sen S, Santhapuri N, Choudhury R R, et al. Successive Interference Cancellation: A Back-of-the-Envelope Perspective [C]// Proceedings of the ACM SIGCOMM Workshop on Hot Topics in Networks (HOTNETS). 2010:1-6

[15] Gollakota S, Katabi D. ZigZag Decoding: Combating Hidden Terminals in Wireless Networks [C]//Proceedings of the ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communications (SIGCOMM). 2008: 159-170

[16] Qin C, Santhapuri N, Sen S, et al. Known Interference Cancellation: Resolving Collisions due to Repeated Transmissions [C]// Proceedings of the IEEE Workshops on Wireless Mesh Network (WIMESH). 2010

[17] Jiang C, Shi Y, Hou Y T, et al. Squeezing the Most Out of Interference: An Optimization Framework for Joint Interference Exploitation and Avoidance [C]// Proceedings of the IEEE International Conference on Computer Communications (INFOCOM). 2012:424-432

[18] IEEE Std. 802. 11, IEEE Standard for Wireless LAN medium access control (MAC) and physical layer (PHY) specifications [S]. IEEE Computer Society,1999

[19] Jamieson K, Balakrishnan H. PPR: Partial Packet Recovery for Wireless Networks [C]// Proceedings of the ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communications (SIGCOMM). 2007:409-420

[20] Bianchi G. Performance analysis of the IEEE 802. 11 distributed coordination function [J]. IEEE Journal on Selected Areas in Communications (JSAC),2000,18(3):535-547

[21] Malone D, Duffy K, Leith D. Modeling the 802. 11 Distributed Coordination Function in Nonsaturated Heterogeneous Conditions [J]. IEEE/ACM Transactions on Networking, 2007, 15 (1):159-172

[22] Chatzimisios P, Vitsas V, Boucouvalas A C. Throughput and Delay Analysis of IEEE 802. 11 protocol [C]// Proceedings of the IEEE International Workshop on Network Applicances (IWNA). 2002:168-174

(上接第 42 页)

预防合谋欺骗和不实反馈等恶意推荐行为。

结束语 在复杂开放的云计算环境中,信任是服务交互活动的前提和关键,其直接影响云服务的质量和云计算技术的发展与推广。因此本文针对云计算环境中服务实体间信任关系的不确定性,在云模型理论基础上借鉴现有评估方法的思想,提出基于加权多属性云的服务信任评估方法,该方法以多属性信任云细化信任评估的粒度,通过引入时间衰减因子来反应信任的时效性,考虑了推荐可靠性对信任评估的影响,能够更加客观真实地反应云计算环境中服务实体间的信任特征。实验结果表明,该方法明显地提高了服务交互成功率,并能够有效抑制不法分子的合谋欺骗和恶意推荐,更加真实地反映云计算环境中服务信任情况,为用户的服务选择提供可靠的安全决策。

参 考 文 献

[1] Buyya R, Yeo C S, Venugopal S, et al. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility[J]. Future Generation Computer Systems,2009,25(6):599-616

[2] Armbrust M, Fox A, Griffith R, et al. A view of cloud computing [J]. Communications of the ACM,2010,53(4):50-58

[3] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报,2011,22 (1):71-82

[4] Vivekananth P. Reputation Based Trust Model for Grid with Enhanced Reliabilty[C]// Junior E R H, et al., eds. INTECH 2011, CCIS. Berlin Heidelberg: Springer-Verlag,2011

[5] Josang A, Presti S. Analyzing the relationship between risk and trust[C]// iTrust04: Proceedings of the Second International Conference on Trust Management. Berlin: Springer-Verlag,2004

[6] Ehab M, ElSalamouny. Probabilistic trust models in network security[D]. University of Southampton,2011

[7] Song Shan-shan, Hwang K, Macwan M. Fuzzy Trust Integration for Security Enforcement in Grid Computing[C]// International Symposium on Network and Parallel Computing (NPC2004). Heidelberg: Spring Verlag,2004:9-21

[8] 王文婧,杜惠英,吕廷杰. 基于第三方认证的云服务信任模型[J]. 系统工程理论与实践,2012,32(12):2774-2780

[9] 黄德才,陈姜倩. 基于集对分析的信任评估模型及其在服务选择中的应用[J]. 计算机科学,2012,39(1):210-214

[10] 唐文,胡建斌,陈钟. 基于模糊逻辑的主观信任模型研究[J]. 计算机研究与发展,2005,42(10):1654-1659

[11] 黄海生,王汝传. 基隶属云理论的主观信任评估模型研究[J]. 通信学报,2008,29(4):13-19

[12] 王守信,张莉,李鹤松. 一种基于云模型的主观信任评价方法[J]. 软件学报,2010,21(6):1341-1352

[13] 谢立军,朱智强,孙磊,等. 基于隶属度理论的云服务行为信任评估模型研究[J]. 计算机应用研究,2013,30(4):1051-1054

[14] 李德毅,杜鹢. 不确定性人工智能[M]. 北京:国防工业出版社,2005

[15] 李德毅,刘常昱. 论正态云模型的普适性[J]. 计算机工程科学,2004,6(8):431-440

[16] Ran S. A model for Web services discovery with QoS[J]. ACM SIGEcom Exchanges,2003,4(1):1-10

[17] 孟祥怡,张光卫,刘常昱,等. 基于云模型的主观信任管理模型研究[J]. 系统仿真学报,2007,19(14):3310-3317