# 自组网下基于多信道和组播的 MAC 协议（MCMAC）[1]

**赵耀、向勇、徐雷鸣、史美林**

**（北京清华大学计算机科学与技术系** 100084）

zyao@csnet4.cs.tsinghua.edu.cn

**摘要**:多信道技术是利用多个信道在同一区域并行传输从而提高无线网络传输能力的 MAC 层技术，目前主要针对单播通信。在无线网中，组播数据的发送一般采用广播的方式，这使得它无法利用多信道带来的吞吐量提高的好处。本文提出一种基于多信道针对组播的 MAC 层算法 MCMAC，能与绝大部分已有的组播路由算法既协同工作而又互相独立，并且提高了组播通信的吞吐量和传输效率。同时，为了在 MAC 层提供一定的可靠性保证，在 MCMAC 的基础上又扩展出了 RMCMAC 协议。我们以 ODMRP 协议为上层组播协议示例，通过模拟仿真实验比较，验证了 MCMAC 协议和 RMCMAC 协议在组播通信的吞吐量和可靠性方面相比传统单信道 MAC 协议的优势。

**关 键 词：**MAC; **组播**; **路由**; **自组网**; **多信道**

## 1. 简介

无线自组网是最近涌现出的无线网络，其特点就是没有固定的基站，其中所有的节点都能任意地移动，并且可以采用任意的方式进行动态的连接，除了无线网络天生的广播特性外最显著的特点就是网络拓扑结构变化频繁和不可预测。此外，有限的电源储备、相对较低的带宽、高出错率也是自组网中重要的限制条件，因此有线网络的那一套协议体系不能够只做点细枝末节的修改就能适应自组网的要求，而必须做大的修改，从而在自组网的研究中引发了许多新的概念和新的思想。

随着网络技术的发展和各种新应用的产生，组播已经成为 Internet 中一个重要的应用，例如视频会议、数据分发等应用都要求下层组播路由的支持。在无线自组网中，组播同样有着许多重要的应用，如灾难恢复、搜索和救援以及自动化战争应用等。常见的组播协议有 MAODV、ADMRP、AMRIS、 AMRoute、ODMRP（On-Demand Multicast Routing Protocol）[2]、FGMP、CAMP 等。其中 ODMRP 协议是上述自组网组播协议中基于网格（Mesh-based），比较简单而且性能也比较好的一个协议。

多信道技术是利用多个频段或扩频、跳频等技术使得一个终端可以使用多个不相交的信道。基于多信道的 MAC 算法在某个特定的信道采用 CSMA 或者 TDMA 等技术，但是可以在多个不同的信道进行发送或者接收数据。虽然发送或接收的速率并没有提高，但是减少了无线传输中的冲突，同一空间内可以在不同信道上同时进行传输，相当于提高了网络实际传输能力。这里，我们在改进 IEEE 802.11[6]的基础上，提出了 MCMAC(Multi-Channel Media Access Control for Multicast)协议，使其能够利用多信道技术，并提供适当的接口给组播协议，使得组播通信能享用多信道技术带来的好处。同时为了提供比较可靠的组播传输，在 MCMAC 的基础上扩展出 RMCMAC (Reliable Multi-Channel Media Access Control for Multicast)协议，通过重传机制来增强组播传输可靠性。此外，MCMAC 和 RMCMAC 略加修改就可以成为能同时支持单播的多信道 MAC 协议。

本文安排如下，第 2 部分详细描述了 MCMAC 协议和 RMCMAC 协议行为，第 3 部分描述模拟测试的模型和结果分析，最后在第 4 部分给出简单的小结。

## 2. MCMAC 协议

MCMAC 协议是基于 IEEE 802.11 DCF 扩展而来的，这是因为 IEEE 802.11 是一个广泛使用的无线 MAC 标准。MCMAC 保持了 IEEE802.11 的基本算法（如 CSMA/CA 算法、RTS/CTS/ACK 握手方式），针对组播特点与上层

[1] 本文受国家自然科学基金项目(批准号：60273010)和 863 项目(编号：2002AA123022)资助。

组播协议密切配合，利用多信道技术有效地提高组播通信的性能。

### 2.1 多信道利用方式

在[8]中提出了多种多信道采用方式，这里我们采用的是发送者多信道方式（common-transmitter-based mechanism），即：首先有一个公共信道，广播包和 MAC 层控制消息（RTS/CTS）都在这个信道发送和接收；每个节点选择一个发送信道，发送单播或组播数据时就切换到这个信道来发送，而其他节点要接收它的数据也要切换到这个发送信道来。发送和接收结束后，所有节点都切换回公共信道继续进行监听。

如图 1，当 MAC 层准备发送组播数据包时，先在公共信道广播 RTS 控制消息。RTS 消息中除了包括原 IEEE 802.11 MAC 协议中的 RTS 消息部分（例如发送者地址，数据包长度，目的地址等）外，还包括发送者的发送信道号。发送者并不等待 CTS 就直接切换到自己的发送信道，等待一段特定时间后就发送组播数据。数据发送完毕后，直接切换回公共信道。

如有线网里组播一样，参与转发或接收特定组播组数据的节点会将组播地址映射成特定的 MAC 层地址。所以当某节点收到 RTS 后发现其中的目的地址是自己的某个组播 MAC 地址，就知道是发送给自己所在组的组播数据。如果它要接收该数据，则根据 RTS 里给出的发送者的信道号切换到特定信道进行数据接收。数据接收完毕后，节点切换回公共信道继续监听。

图 2 给出了 MCMAC 的时序图。上述过程非常简单，与单信道 MAC 协议的主要区别就在于接收组播数据时切换到发送者指定的信道去，使得公共信道只用来发送协议控制包（RTS/CTS）和广播数据，大大减少了公共信道的数据量，从而减少了控制包之间的冲突。组播数据也分散到不同的信道进行发送，同一区域数据传输有了并行性，从而吞吐量能大幅提高。

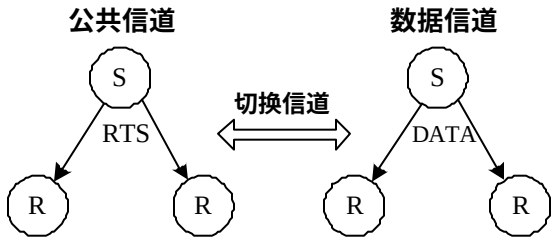


图 1 多信道的利用

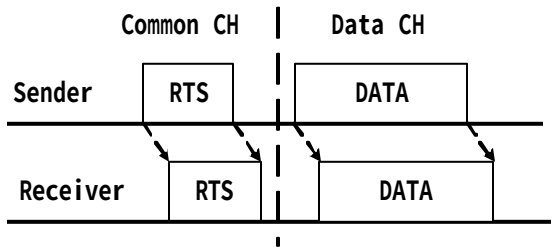


图 2 RMCMAC 的时序图

### 2.2 重复包检测

在无线网组播协议中，一般不再依靠 RPF(Reverse Path Forwarding)来避免传输重复包，而采用包的序列号(SEQ_ID)来检测重复数据包。大部分组播协议通过记录组播发送源的地址以及收到的数据包的序列号(最大序列号或者最近收到包的序列号集合)，来判断新收到的数据包是否重复包。

在 MCMAC 中，一个节点如果切换到某发送节点的发送信道去接收一个重复包，则该节点这段时间无法继

续在公共信道监听，当然也更不可能去接其他节点的数据了。这无疑是一种浪费，因此我们把重复包检测这一步下移到 MCMAC 中进行。

MCMAC 中对每个组播组，缓存一定数量(MAC_SEQ_COUNT)的过时组播数据包序号，并采用简单的替换最旧包序号的方式进行更新。这种检测重复包的序号由组播协议来定义，例如可以简单采用组播源的地址和组播源发出该数据包的序列号合成所得的序号。

组播路由层在把组播包送到 MCMAC 时，同时把这个序号也传送给 MCMAC。在 MCMAC 发出的 RTS 包中，除了添加了前面提到的发送者信道号外，还包括了该序号。这样，本组成员接收到 RTS 后可以检测该包是否重复数据包。如果是重复包，则不切换信道，而是继续留在公共信道监听。这样可以避免重复包的接收，提高了信道的利用率。

然而这种做法在一定程度上增大了 MAC 层对路由层的依赖，而且也重复完成了组播路由层检测重复包的功能，但是只依靠很小的代价能取得 MAC 层性能的很大提高，特别是在上层组播路由是基于网格（Mesh）方式的情况。同时 MAC 层和组播路由间的接口非常简单，具有很大的通用性（适合绝大部分组播路由协议）。

图 3 描绘了 MCMAC 的有限状态机。由于没有利用 CTS/ACK 等控制消息，MCMAC 的状态非常简单，只有三个状态：IDLE（空闲状态），WF_DATA（等待数据状态）和 TR_DATA（发送数据）。

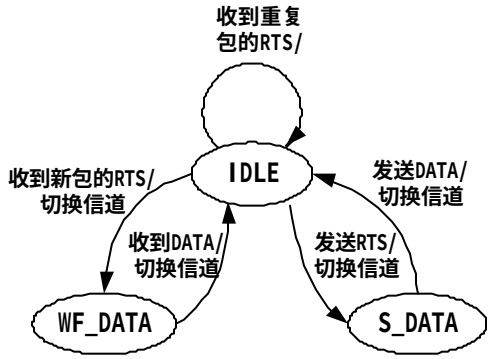


图 3 MCMAC 的有限状态机

### 2.3 有限信道下均衡利用

在理想情况下，可假设信道数多于节点数，每个节点都可以有自己的独占的发送信道，那么发送组播数据时不会发生冲突，数据的转发成功率由信道本身的可靠性决定。在这种理想情况下，原来无线网中的隐藏终端问题、暴露终端问题以及侵入终端问题对于通过数据信道传送的组播数据的传送都不存在了。当然，在公共信道上发送广播数据还是有可能由于冲突而丢失。

然而实际上信道资源十分有限，不可能每个节点独占一个信道，而是共享有限个信道，从而需要考虑如何尽量充分利用这些信道，减少因抢占相同信道而带来的冲突。

在 MCMAC 中，维护一个信道占用表。当某节点 N 收到其他节点的 RTS 后，则按照 RTS 里内容，把信道占用表里指定的信道置占用标志，并根据要发送的数据的长度计算出信道将被占用的时间。

当节点 N 要发送组播数据时，它查询信道占用表，从所有没有被占用的信道中随机选择一个信道作为自己的发送信道，并且在随后发出的 RTS 中包含选定的信道号。如果所有的信道都被占用，则送回发送队列队头，重新进行退避。

这样的算法可以在很大程度上避免多个临近节点在同一个信道同时发送数据而引起的冲突，但是由于每个节点并不能正确收到所有邻居节点发出的 RTS（例如公共信道的冲突或当时节点不在公共信道），所以发送节点同样可能选择一个已经被占用了的信道进行数据发送，无法完全避免冲突的发生，然而冲突的概率却因为多个信道的选择而大大下降。

## 2.4 可靠的多信道 MAC 协议 RMCMAC

在多信道情况下，如果不是每个节点独占一个数据发送信道，隐藏终端问题、暴露终端问题和侵入终端问题同样存在。暴露终端问题并不会带来很大的问题，只有在所有信道都被占用（某些占用是因为暴露终端问题带来的）的情况下才会使得 MAC 层重新退避。对隐藏终端问题，只依靠 RTS 这个控制信息无法解决，可以引入 CTS 和 ACK 控制信息来进一步解决。此外，无线信道传输本身具有不可靠性，受环境的影响比较大。这里我们提出 Reliable Multi-Channel MAC for Multicast (RMCMAC) 协议，该协议采用类似 IEEE802.11 MAC 协议的 RTS/CTS/DATA/ACK 策略，通过 CTS 和 ACK 控制信息来提高 MAC 层协议的可靠性。

### 2.4.1. 通过重传提高可靠性

不同于单播，组播协议中一个节点发出的一个组播数据可能被多个邻居组播转发者或组播成员接收，因此需要多个 CTS 的应答。但是多个节点应答 CTS，如果没有设定好顺序，这些节点间应答 CTS 就可能导致冲突而失败，所以必须设定好一个顺序，RMCMAC 在 RTS 中指定这个顺序。RMCMAC 需要上层组播路由协议把组播树在该点的下游情况告诉它，即应该接收该点发出的组播数据的下游节点集合。对于采用组播树（共享树或最短路径树）的组播协议，只需要把该点的树结构的下游告诉 RMCMAC 协议即可；而对于采用网格（Mesh）结构的组播协议（例如 ODMRP），同样有着一个组播树核心骨干，只是依靠扩展而得的网格获得更高的可靠性，这里只需要提高组播核心树的传送成功率，即把核心组播树的下游告诉 RMCMAC 协议。

RMCMAC 协议的 RTS 比 MCMAC 作了进一步的扩展，把当前需要保证接收的下游节点的地址按照任意的顺序添加到 RTS 消息中增加的接收者列表中。这样当这些接收者收到 RTS 消息后，就依照 RTS 中给定的顺序和 CTS 的长度（长度固定）以及应答间隙，确定自己的应答 CTS 时间，按顺序进行 CTS 应答。此外，其他具有该组 MAC 地址的结点（不在 RTS 指定列表中的）同样可以在判断不重复后切换到发送者的发送信道去接收组播数据，只是省掉了应对 CTS 以及接收后应答 ACK 的过程。这样，基于网格的组播协议不会因为 MAC 层而带来效率降低。

接收者应答的 CTS 中也包括了发送者的信道号，可被其他节点用来更新信道占用表情况，有助于进一步避免隐藏终端问题。此外，CTS 中添加了一个标志位 RECVED_FLAG，当某个下游检测到该数据已经接收过了（通过 RTS 的内容），它应答的 CTS 中 RECVED_FLAG 标志位就置 1，这样发送者就知道它已经正确接收过了，而该接收者并不切换信道去接收重复数据。当发送者和接收者都切换到发送者信道并且数据发送完毕后，接收者按照给定的顺序依次应答 ACK。

发送者根据收到的 RECVED_FLAG 置 1 的 CTS 和 ACK 消息可以确定哪些接收者正确接收了数据。如果不是所有的接收者都正确接收了，则记录没有收到数据的接收者信息，并把这个数据包送入重传队列进行重传（重传次数有限，例如 RMCMAC 中设为 3 次）。然而如果发送者一开始发送了 RTS 而没有收到 CTS，则直接把数据包送回重传队列。

图 4 描绘了 RMCMAC 的时序图。通过 RTS/CTS/DATA/ACK 这套机制，RMCMAC 可以进一步解决隐藏终端问题，并且通过重传减少因冲突带来的丢包，获得较高的接收率和可靠性。

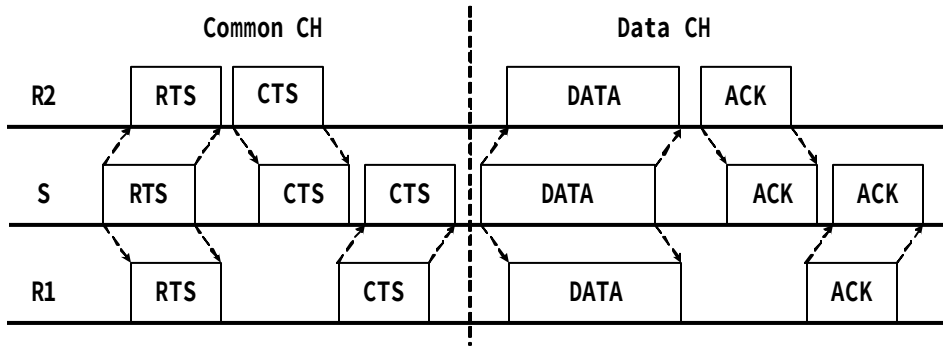

图 4 RMCMAC 的时序图

2.4.2. 链路断开检测

RMCMAC 中利用了组播路由协议提供的组播（核心）树的下游情况。然而在自组网这种拓扑频繁变化的网络环境中，组播路由协议维护的组播（核心）树在拓扑变化时需要一定的时间间隔才能完成调整，在这个过渡期间，RMCMAC 获得的组播（核心）树下游集合是不准确的。如果该集合中包含了某个已经断开了的下游（超出无线传送范围），那么必然导致 RMCMAC 无法收到所有下游应答的 CTS 或 ACK，从而导致 RMCMAC 进行多次没有必要的重传，反而影响效果。所以，RMCMAC 进行链路断开检测，减少这种无效的重传，避免自己受到上层路由协议效率的影响。

RMCMAC 中设定一个无效链路表，里面保存了自己无法直接通信的节点地址和通信失败程度（BREAK_DEGREE）。当 RMCMAC 重传几次失败准备丢弃某个组播数据包时，它把没有接收该数据包的下游节点添加到无效链路表中去，设定 BREAK_DEGREE 为 1（如果节点已经存在无效链路表中，则把 BREAK_DEGREE 加 1）。当某个节点的 BREAK_DEGREE 超过一定的阈值（MAX_BKDEGREE）时，认为该链路断开。

发送者发送 RTS 时，同样包含断开下游的地址。但是当发送者发送完组播数据后，检查应答情况时首先把已经断开的节点排除掉，即不会为这些已经断开的节点进行重传。如果一条链路在断开后又恢复连接了（而上层组播路由可能没有意识到先断开再连接这个变化），那么下游节点会应答 CTS 或 ACK，这时 RMCMAC 将它从无效链路表中去掉。此外，经过一定时间（较长）后 RMCMAC 将无效链路表中很久都没有刷新的无效链路删掉。这样 RMCMAC 只是利用组播路由协议的信息来提高可靠性，而避免了受组播协议的影响。

图 5 给出了 RMCMAC 的状态自动机，比 MCMAC 复杂了许多，包括七个状态：IDLE（空闲状态）、W_CTS（等待 CTS）、S_CTS（发送 CTS）、W_DATA（等待数据状态）、S_DATA（发送数据）、W_ACK（等待 ACK）和 S_ACK（发送 ACK）。一般出错处理都是重新回到公共信道处于 IDLE 状态，图中就没有一一画出。

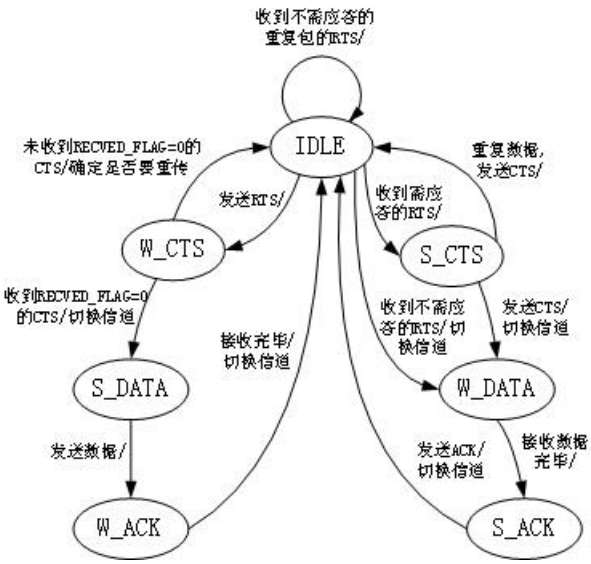


图 5 RMCMAC 的状态自动机

2.5 与组播路由协议的接口

MCMAC 协议和 RMCMAC 协议为了与上层组播路由协议协作，需要获得组播层的一些信息，所以提供了几个接口供组播协议调用。这里我们以 ODMRP[2]协议为例，描述如何使用这些接口。

1) **映射组播地址到** MAC **层地址：**

**在** ODMRP **协议中，当节点加入某个组** G **或者组** G **的转发组（**Forwarding Group**）时，**ODMRP **协议调用** MCMAC **提供的添加组地址接口，把组** G **的地址传个** MCMAC**，由它来获得映射后的** MAC **地址。同样，当节点改变状态成为既不是组** G **的成员也不属于** G **的转发组时，它调用删除组地址接口，从而** MAC **层以后不会再去接收组** G **的数据。**

2) **组播数据序号接口**

**在** MCMAC **中提供了重复包检测，在** RTS **中包含了可以区分数据包的序列号，这需要上层协议在送下数据包的同时调用** MCMAC **的组播数据信息接口包含该序号。**ODMRP **协议可采用组播源的地址和组播源发出该数据包的序列号合成所得的序号来避免重复包接收。**

3) **组播下游信息接口（**RMCMAC **特有）**

**在** RMCMAC **中，需要获得组播树的下游信息来进行可靠性保证。**ODMRP **协议利用网格（**Mesh**），但是转发组的建立同样是通过** JOIN_REPLY **消息的应答建立最短树（**SPT**）的核心。在** ODMRP **协议中增加了对下游的记录，并且在发送组播数据时通过** RMCMAC **提供的接口将这些下游信息传给** RMCMAC**。**

**我们把这样扩展后的** ODMRP **协议叫做** ODMRP-MCT **（**On-Demand Multicast Routing Protocol with Multi-Channel Technique**）。由上面提出的接口，可见结合** MCMAC**（或** RMCMAC**）协议和组播路由协议并不需要组播协议做多少改动，只是需要组播协议将一些常用的组播信息传递给下层** MAC **协议，而不会影响上层组播协议行为，具有通用性。**

## 3. 模拟实验及分析

**在模拟实验中，**MAC **层协议分别采用** IEEE802.11 DCF **和改进后的** MCMAC **协议、**RMCMAC **协议，以** ODMRP-MCT **为上层组播协议，体现了支持多信道的** MAC **层协议的优势。**

### 3.1 模拟模型和方法

**对各** MAC **层协议和** ODMRP-MCT **协议的模拟实现都采用的是** ns2.1b9[12]**。实验场景由** ns2 **的** setdest **工具生成，在** 1200m×1200m **的方形区域中，**50 **个节点随机分布其中运动。网络中可能暂时性的分裂，节点的平均邻居数为** 7.62**。每次运行** 400 **秒，多次结果取平均数。**

**传播模型采用的是** Two Ray Ground **模型。每个节点广播范围是** 250 **米，载波监听范围是** 550 **米。 每个信道的无线传输速率都为** 2mbps**，一个节点同一时刻只能在一个信道进行监听、接收或发送，在不同信道间进行切换需要一定的切换时间。**MAC **层分别采用** IEEE 802.11 MAC **协议的** DCF**（**Distributed Coordination Function**）方式，**MCMAC **和** RMCMAC**。**

**组播组大小固定为** 20**，**5 **个组播源从** 50 **个节点中随机选择，其中绝大部分发送者同时作为接收者。组播接收者在模拟开始时就加入组播组，在整个模拟阶段都不会退出组。由** ns2 **的** CBR Agent **产生带抖动的速率固定的组播数据流，数据包的大小都为** 512 **字节。**

**这里采用组播传输成功率**(Packet Delivery Ratio)**作为度量来反映** MAC **层协议与组播路由协议结合后的整体效果，传输成功率即在应用层接收节点实际收到的数据量与接收节点应该接收到的数据量之比，成功率越高反映了协议的性能越高越可靠。**

### 3.2 模拟结果和分析

#### 3.2.1. MCMAC 的性能

**本实验测试了** MCMAC **在网络传输能力上相对单信道** IEEE 802.11 **的提升。实验场景中节点平均运动速度为** 1m/s**，最大运动速度为** 2m/s**，这种低速运动并不会对传输成功率带来大的影响。**

图 6 反映了 MCMAC 协议随着负载量的增加的性能表现。图中，MCMAC-k 中的 k 表示 MCMAC 协议只利用 k 个数据信道，而 MCMAC 表示信道无限的理想情况。从图中可以看出，利用多信道可以大大提高无线传输的能力，从而组播协议的传输成功率也大幅增加。只使用单信道的 IEEE 802.11MAC 层随着负载加重，性能首先下降很快，符合基于竞争机制的 MAC 层的规律。但当负载超过一定量后下降趋于平缓，类似双曲线的形状。这也是因为负载过大，MAC 层已经达到实际能发送的数据的限度，再增加的负载也只能在缓冲队列中丢掉。理想的 MCMAC 避免了数据传输的冲突，几乎不受隐藏终端、侵入终端问题的影响，所以传输能力有显著的提高，即使在重负载下（100pkt/s）仍然可以获得超过 90%的传输成功率。图中同样可以看出，MCMAC-k 利用的数据信道越多，则性能越好。但是，当利用的信道数达到一定数量后，性能提高有限，例如 MCMAC-8 的性能相比 MCMAC-6 提高很少，这里无限信道的 MCMAC 实际上等价于用了 50 个（节点数）信道。所以，选择合适的信道数量，可以获得较好的性能，而又不浪费信道。

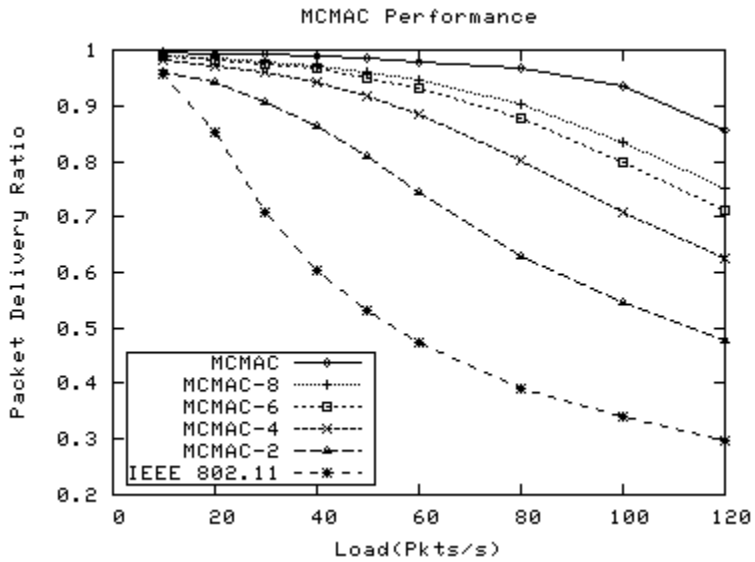


图 6 随着发送者数量变化包传输率的变化

3.2.2. RMCMAC 的可靠性

这里我们测试了不同的信道的传输成功率下 RMCMAC 协议和 MCMAC 协议的性能。在维持较高的短包（RTS/CTS/ACK 等）传输成功率情况下，改变长包（组播数据）的传输成功率，比较不同 MAC 层协议的可靠性。为了验证通过链路断开检测，RMCMAC 协议并不受上层路由协议的影响，我们采用了比较高速的运动场景，节点平均移动速度为 5m/s，最大运动速度为 10m/s。实验中负载量较轻（30packets/s），信道的长包传输出错率变分别为 0、0.1、0.2、0.3、0.4。如图 7，随着信道传输出错率的增加，MCMAC 协议的性能下降越来越快。然而由于 ODMRP 协议基于网格，本身就通过一定的冗余传输来提高传输性能，所以应用层的成功率反而高于信道的成功率。而 RMCMAC 协议由于重传机制增强了可靠性，性能下降非常平缓，适合恶劣环境下的要求。实际上如果不考虑冲突等其他影响传输失败的因素，粗略估计 RMCMAC 通过 3 次重传可以把原本为 x 的信道出错率降为 $x^3$，即使在出错率为 0.4 的信道情况下也只有 0.064 的出错率。

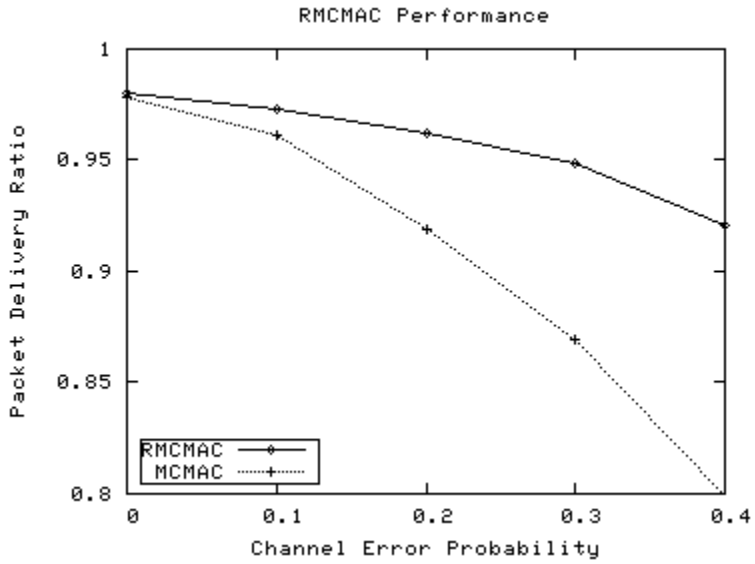


**图 7 随着传输出错率变化 RMCMAC 和 MCMAC 的性能**

RMCMAC 协议实际上是依靠重传来提高组播数据传送的可靠性的，同时它额外的 CTS/ACK 应答机制更增加了协议开销，这使得它在重负载下的传输性能比 MCMAC 要差，这也是提高可靠性带来的副作用。对组播数据而言，大部分是音频或视频流，对可靠性的要求并不是那么严格，而是需要大的传输量作保证。只有少数如文件分发等应用需要较高的可靠性，往往也不会带来很大的负载量。所以，我们设想的情况是 MCMAC 和 RMCMAC 相互协作（RMCMAC 本来也是在 MCMAC 上扩展而来，只要上层路由协议不调用组播下游信息接口就可演变为 MCMAC），由上层协议根据应用的需要或当前环境（信道）的恶劣情况来选择 MAC 层提供不同的服务。

## 4. 结论

普通的单信道下分布式的 MAC 层协议把主要的重点放在发送者与接收者之间的握手过程中，以此来减少隐藏终端带来的冲突和暴露终端带来的带宽浪费。

我们提出的 MCMAC 和 RMCMAC 协议利用多信道技术，针对上层组播应用，通过把流量合理分配到不同信道，减少了无线传播中的冲突，获得比单信道下普通 MAC 协议更高的吞吐量。这里对 MCMAC 和 RMCMAC 的改进不影响 MAC 层对单播和广播分组的处理过程，而且只要稍加改动适应单播目的地址即可以成为单播下的多信道 MAC 协议。同时，MCMAC 和 RMCMAC 使用通用的接口与上层组播联系，上下层间能做到互相促进而又互相独立。

然而利用多信道的 MAC 协议存在着由于离开公共信道而带来的暂时消失现象（其他邻居节点无法与它联系），这也同时会带来公平性方面的问题。如何解决暂时消失问题，提供公平性保证将作为我们以后的研究内容。

**References:**

[1] S. Corson and J. Macker, “ Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, RFC 2501, January 1999

[2] S.-J. Lee, W. Su, and M. Gerla , “ On-demand multicast routing protocol in Multihop Wireless Mo-bile Networks” , *ACM/Kluwer Mobile Networks and Applications, 2000.*

[3] Sung-Ju Lee, William Su, and Mario Gerla. "On-demand multicast routing protocol (ODMRP) for ad hoc networks", Internet Draft, draft-ietf-manet-odmrp-02.txt, January 2000.

[4] S.J. Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia. A performance comparison study of ad hoc wireless multicast protocols. Proceedings of the IEEE Infocom 2000, March 2000

[5] Thomas Kunz and Ed Cheng, "Multicasting in ad-hoc networks: Comparing MAODV and ODMRP", *Proceedings of the Workshop on Ad hoc Communications*, Bonn, Germany, September 2001
[6] B. P. Crow, I. Widjaja, J. G. Kim and P. Sakai, Investigation of the IEEE 802.11 Medium Access Control (MAC), in: *IEEE INFOCOM '97*, 1997.
[7] Z. J. Haas and J. Deng, "Dual Busy Tone Multiple Access (DBTMA) - A Multiple Access Control Scheme for Ad Hoc Networks," IEEE Transactions on Communications, vol. 50, no. 6, pp. 975-985, June 2002
[8] Mario Joa-Ng, I-Tai Lu, Spread Spectrum Medium Access Protocol with Collision Avoidance in Mobile Ad-hoc Wireless Networks, INFOCOM 1999, 776-783
[9] Jiandong Li, Zygmunt J. Haas, and Min Sheng, Capacity Evaluation of Multi-Channel Multi-Hop Ad Hoc Networks,ICPWC 2002, New Delhi, India, Dec 2002
[10] J. Li, Z.J. Haas, M. Sheng, and Y. Chen, Performance Evaluation of Modified IEEE 802.11 MAC for Multi-Channel Multi-hop Ad Hoc Network, Advanced Information Networking and Applications (AINA) conference, Xidian University, Xian, China, March 27-29, 2003
[11] J. Macker and S.C.(chairs). Mobile Ad-hoc Networks(manet), http://www.ietf.org/html.charters/manet-charter.html
[12] The Network Simulator - ns-2, Available from http://www.isi.edu/nsnam/ns/

# A Multi-Channel Medium Access Control Protocol for Multicast in Mobile Ad-hoc Network

*Abstract*—In mobile ad-hoc network, some multi-channel MAC protocols utilize multiple channels to reduce the collision of wireless transmission and thus get high throughput. These multi-channel MAC protocols aim at improving the performance of unicast communication, and multicast data are generally transmitted through broadcast. So multicast can't benefit from the multi-channel technique. This paper proposes a multi-channel media access control protocol for multicast(MCMAC) which uses multi-channel techniques to improve multicast performance. MCMAC and multicast routing protocols can cooperate well through some simple interfaces and each protocols keeps its independence. To improve the reliability of MAC layer, we also developed a reliable multi-channel MAC protocol for multicast(RMCMAC). Taking ODMRP[2] as an example of multicast routing protocols, we evaluate the performance of MCMAC and RMCMAC for ad hoc networks via detailed simulation.

Keyword: MAC; Multicast; Routing; Ad-hoc; Multi-Channel