浙江工业大学

学 习 报 告

WLAN 中 CSMA/CA 介绍及隐蔽站点问题研究

学　　院：信息工程学院

专　　业：通信工程

学生姓名：凌智城

学　　号：201806061211

指导教师：吴哲夫

2020 年 12 月 4 日

摘　要

MAC 层的工作机制是决定局域网整体性能的关键因素。介绍了分布式协调功能（DCF）和点协调功能（PCF），并且结合 RTS/CTS 握手协议和 CSMA/MA 介质访问控制协议分析了解决方法的实现原理。

关键字：WLAN CSMA/CA RTC/CTS 静态/动态检测

Abstract

The working mechanism of MAC layer is the key factor to determine the overall performance of LAN. This paper introduces the distributed coordination function (DCF) and point coordination function (PCF), and analyzes the implementation principle of the solution based on RTS / CTS handshake protocol and CSMA / MA media access control protocol.

Keywords:WLAN CSMA/CA RTC/CTS Static detection/Dynamic monitoring

目录

第1章　引言

局域网（Local Area Network, Lan）是共享介质的广播式分组交换网络。无线局域网（Wireless Lan，WLAN）再技术上遵循了 IEEE 802 局域网体系结构，继承了局域网尤其是以太网（Ethernet）在发展过程中所取得的大量成熟技术，成为了目前倍受用户和研究者普遍关注的一个领域。其中，WLAN 存在以下特点：使用无导向超高压比上个月照顾，物理层实现技术复杂，采用 CSMA/CA 介质访问控制协议，一般只能工作在单双工模式下，这些特征为 WLAN 的技术实现带来了苦难和挑战。

本文结合课堂听讲、课外辅导材料查找和自修进行深度学习探索，就 WLAN MAC 层的隐蔽站点问题进行研究，通过发现和确定符合运行环境需求的 MAC 层规范，以减少和避免冲突的产生，增强网络的服务效能，提高 WLAN 的工作效率。

第2章　IEEE802.11

2.1　IEEE 802.11 WLAN 概述

无线局域网以其具有独特的巨大优势，广阔的应用前景范围和人类的需求不断地推动无线局域网协议的出现。在 1997 年 6 月 26 日，国际电气和电子工程师联合会（IEEE）制定完成标准协议规范，并于同年 11 月 26 日正式对外公布，其逻辑结构图如图 1 所示。IEEE802.11 是第一代无线局域网标准之一，也是发布的第一个无线局域网标准，其承袭 IEEE802 标准系列。由于无线信道与有线信道的差异及其特有的特性，所以其物理层和上层的数据链路层协议需要重新制定，而高层协议规范沿袭标准规范协议系列。

与有线局域网标准一样，IEEE802.11 无线局域网（WLAN）只涉及 OSI 网络模型中的最低两层：物理层（PHY）和数据链路层（DLC），网络结构相对简单。其中数据链路层又可被分成逻辑链路控制子层（Logical Link Control，LLC）和媒介访问控制子层（Medium Access Control，MAC）。由于 IEEE802.11 使用的是与 IEEE802.2 完全相同的 LLC 层，并且采用协议中的 48 位 MAC 地址，所以使得无线网络与传统的有线网络之间的链接变得非常方便。

以太网一样，WLAN 也采用了 CSMA（载波侦听多路访问）介质访问控制方式来共享下信道。不过，为了避免冲突（collisions）造成的资源浪费，WLAN 并未采用以太网的 CSMA/CD（载波侦听多路访问/冲突检测），而是采用了 CSMA/CA（载波侦听多路访问/冲突避免）介质访问控制协议。

图 1: IEEE802.11 逻辑结构图

2.2　IEEE802.11 MAC 简介

无线局域网中所有站点共享同一个无线信道，网络中某一个站点发出的数据能被站点接收，由于共享无线信道引起访问冲突，因此必须要解决信道访问控制问题，即解决多个用户竞争信道使用权的问题，而将传输媒介高效合理的分配给各个站点叫做媒介访问控制（Medium Access Control，MAC）。

IEEE802.11 定义了两种 MAC 接入方式：分布式协调功能（Distributed Coordination Function，DCF），点协调是功能（Point Coordination Function，PCF）。

分布式协调功能：是 IEEE802.11MAC 的基本媒介访问方法，提供基于竞争服务，在发送数据之前，工作站会检查信道是否处于空闲状态，若忙，则会随机的选择一定的退避时间来避免冲突发生。

点协调式功能：提供无竞争服务，采用中心控制模式，基于优先级访问控制，适用于安装点控制器的网络。其采用特定的轮询算法依次询问网络中每个站点是否将有数据要发送，由于完全控制了各个站点的发送顺序，因此不会发生冲突，处于此服务中的工作站点只需经过一定的时间就可以发送数据。

由于无线网络可能会遭遇到诸多无线电波传播上的问题，此外还有站点竞争信道造成的冲突问题，因此无线传输信道被认为是不可靠的，无线网络必须验证所接收的帧，防止数据在传送中丢失。采用肯定性确认来解决这些问题，以牺牲一些带宽确保数据帧的传送。只有发送站点在规定时间内收到来自接收站点确认帧（Acknowledge，ACK）才认为此次数据发送成功完成；否则，重新发送。

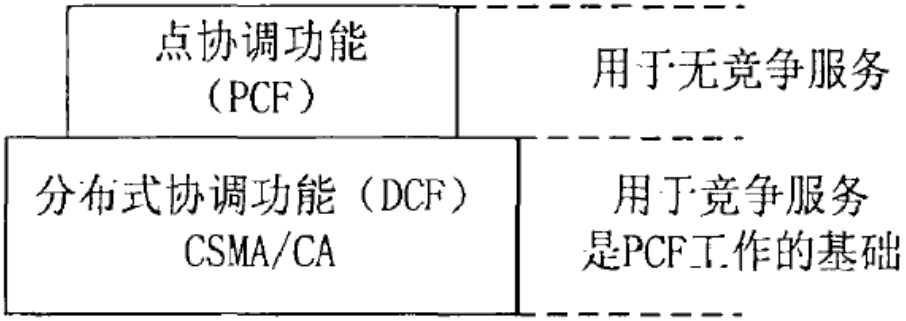


图 2: DCF 与 PCF 关系图

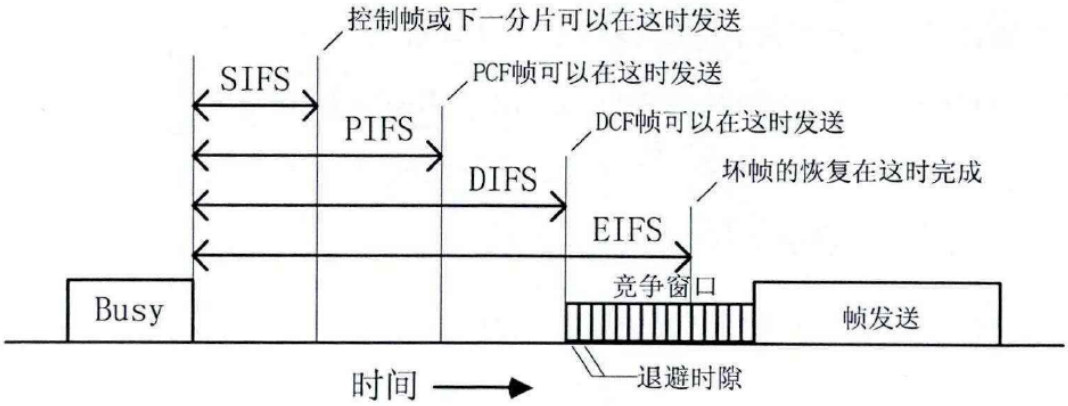


图 3: 四种帧间隔示意图

2.2.1　帧间隔

其中所有的 IEEE802.11 网络实现必须支持 DCF，而 PCF 为可选的。PCF 建立在 DCF 的基础上，并且 DCF 和 PCF 可以同处于一个网络中，如图 2 所示。为此 IEEE802.11 提供了一种简单方法实现，通过定义不同的帧间隔来实现。所谓帧间隔是指：某一帧被传输后有一段空闲时间，不允许任何站点发送数据，必须等待该间隔时间后，才能允许发送下一帧，这段时间称为帧间隔。IEEE802.11 规定了四种帧间隔长度如图 3 所示。其中间隔越短优先级越高，按照优先级由高到低排列如下：

短中贞间间隔（Short InterFrame Space，SIFS）：允许正处在会话中的站点优先发送，如允许收到 RTS 的站点发送一个 CTS，允许收到数据的站点发送一个 ACK，允许收到 ACK 的站点继续发送后继帖片段而不用重发 RTS。作为最小帧间隔，具有最高优先级，确保正在当前

以 DCF 模式通信的站点不会被打断。

帧间隔（PCF InterFrame Space，PIFS）：在间隔 SIFS 后只有一个站点允许发送，如果该站点没有发送，那么在空闲时间到达 PIFS 后，控制站点可以发送一个轮询帧，这是为 PCF 提供的，使得采用 PCF 模式比 DCF 模式拥有更高的优先级，可见 PCF 是在 DCF 之上。

DIFS（DCF InterFrame Space）：如果没有站点发送那么在 DIFS 间隔后任何试图发送数据站点都可以来竞争信道以便发起新的一次数据交换。

扩展帧间隔（Extended InterFrame Space，EIFS：被用来报告坏帧，只有刚刚接收到坏帧或未知帧的站点会使用这个帧间隔。

2.2.2 CSMA/CA

DCF 是 IEEE802.11 标准中规定的 MAC 访问控制方法，也是无线局域网最基本的访问控制方式。DCF 协议和 IEEE802.11 标准的 MAC 协议类似，都是解决多用户共享一个信道，如果一个设备在发送数据，其他设备就不能发送数据，否则就会发生冲突。由于在无线环境中，要是设备一边发送数据信号，又要一边检测是否有冲突这是无法实现的，一次 IEEE802.11MAC 协议不同于 IEEE802.3 中采用的 CSMA/CD（Carrier Sense Multiple with Collision Detection，载波侦听多路访问/冲突检测）协议，而采用 CSMA/CA（Carrier Sense Multiple with Collision Avoidance，载波侦听多路访问/冲突避免）协议。

CSMA/CD 是指个站点在发送数据前先监听想到是否空闲，仅处于空闲时才开始发送，并且继续监听信道，检测到冲突后立即停止发送；若信道忙，则继续等待，监听到空闲时才可发送。

CSMA

CSMA/CA 是指：一方面，监听当前信道是否空闲；另一方面，避免冲突，通过随机退避一段时间，使站点间产生冲突的概率降低到最小。在 IEEE802.11 中，站点要确定无线信道是否被占用比较困难，物理层载波侦听不像 IEEE802.3 网络中那么有效，因此站点检测信道空闲状态有两种方法：物理载波检测和虚拟载波检测。其中物理载波检测是通过接收信号的能量检测，载波检测和能量载波混合检测来实现的；而虚拟载波检测是通过检查网络分配矢量（NAV）实现，它指示信道将被网络中站点占用多久时间。某个站点若要发起通信时，会预估其将会占用信道的时间长度，并将该值放入 MAC 帧结构中持续时间字段，而每个站点都独立维护自己的 NAV 矢量，在接收到任何目的地址不是自己的合法帧后，会比较所接收的帧的持续时间字段与当前 NAV 值，只有当字段值大于当前 NAV 值，才更新 NAV 值为字段值，否则，不予更新。NAV 类似于倒数计数器，当 NAV 变为 0，且载波侦听也为空闲，则表明当前信道空闲，才可发送数据。若信道繁忙，则执行二进制指数退避算法来避免各个站点可能造成的冲突。

CA

其中冲突避免是依赖于二进制指数退避实现。一个站点若要占用信道，先侦听信道的忙闲状态，若信道空闲就直接发送，否则推迟发送，当前退避窗口为最小退避窗口，执行退避过程按时间先后顺序如下：

Step1. 从当前退避窗口中随机选择一个退避数置入退避计数器中；

Step2. 站点持续检测信道的空闲状态，若空闲时间持续 DIFS 间隔后，则每经过一个空闲的系统时隙，退避计数器的值减 1;

Step3. 若在退避过程中检测到信道忙，则冻结当前退避计数器，并回到状态 Step2;

Step4. 等到退避计数器的值变为 0 时，站点才开始发送。若发送失败，当前退避窗口加倍（直到达到最大退避窗口值），并返回到状态 Step1。

当一个站点要有数据发送而占用信道时，必须要执行退避算法。仅在以下情形除外：检测到信道是空闲的，并且这个数据帧是其发送的第一个数据帧。执行二进制指数退避算法减少了网络中多个站点同时占有空闲信道，从而使得网络中站点冲突概率最小化。

除此以外的所有情况, 都必须使用退避算法。具体来说，以下几种情况必须使用退避算法（1）在发送第一个帧之前检测到信道处于忙态；（2）每一次的重传；（3）每一侧的成功发送后再要发送下一帧。

2.2.3 DCF 模式

DCF 接入机制分为两种接入方式：基本接入方式和可选的 RTS/CTS 接入方式。

2.2.4 基本接入方式

基本接入方式即 CSMA/CA。如图 4 所示，一个站点在发送数据帧之前，检测信道是否空闲：若为空闲，且持续时间大于 DIFS，则发送数据帧；若信道忙，则持续监听信道，直到信道空闲时间大于，随机选择一个退避数，保存在退避计数器中，此后每经过一个空闲时隙，退避数减 1，若在退避过程中，检测信道忙，退避计数器冻结，直到信道空闲时间再次大于 DIFS，再恢复退避计数器，当退避计数器变为 0 时，站点发送数据帧；只有正确接收数据帧后，目的站点在经过 SIFS 时间后，向源站点回复 ACK。仅在源站点在超时时间内接收目的站点的 ACK 才认为这次发送操作正确完成；否则，发送失败，竞争窗口加倍，重复上述过程，直到失败次数达到最大重传次数，丢弃该帧。

2.2.5 RTS/CTS 接入方式

RTS/CTS 是一种握手协议，主要用来解决如下问题：隐蔽站点问题；当所要传输分组大于阀值时，启用 RTS/CTS 交换。

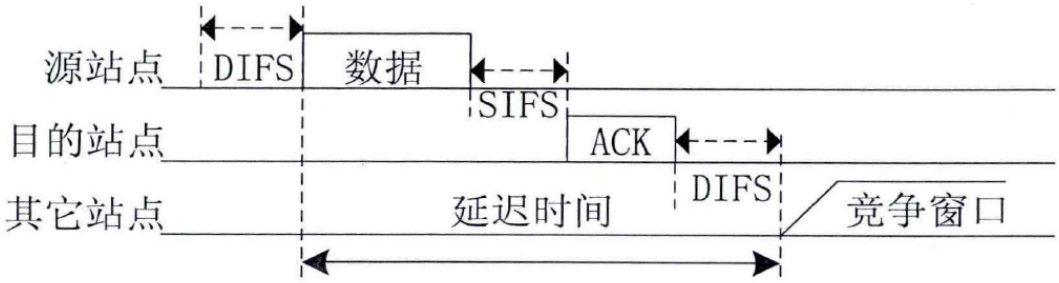


图 4: 基本机制时序图

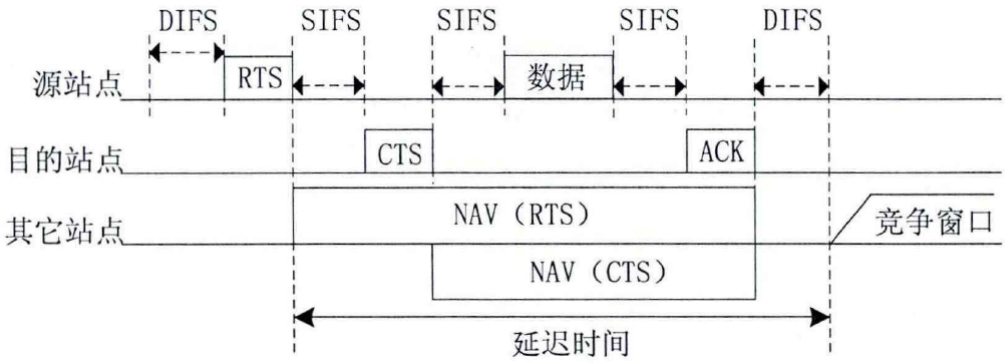


图 5: RTS/CTS 机制时序图

RTS/CTS 一次成功交换过程按时间先后顺序为：源站点发送 RTS 帧；目的站点发送 CTS 帧；源站点发送数据帧；目的站点发送 ACK 帧。

并且在每次发送 RTS 帧之前，都要执行退避算法。只有在上述 4 个步骤正确完成后，才认为此次发送成功；否则，退避窗口加倍，执行退避算法，重复上述 4 个步骤。直到发送失败次数达到最大发送次数时候，丢弃该发送帧。

如图 5 所示，原站点若有数据要发送，使用和基本计入方式同样的退避机制，在获得信道占有权后不是立即发送数据帧，取而代之的是先发送 RTS 帧，目的站点在正确接收后，经过 SIFS 时间，发送 CTS 帧，如果，源站点在超时时间内未接收到 CTS，则认为发送失败，退避窗口加倍，重复上述过程；若正确接收，在经过 SIFS 后，源站点发送数据帧，目的站点在正确接收数据帧后，同样经过 SIFS 后，发送 ACK 帧，只有源站点正确接收 ACK 帧，才认为整个传送过程成功完成，否则，退避窗口加倍，重复上述整个过程。

第 3 章　隐蔽站点问题

3.1　IEEE 802.11 MAC 层存在的隐蔽站点问题

3.1.1　隐蔽站点问题

由于在一个 BSS（Basic Service Set）中，工作在无线环境中的各个站点共享同一个无线通信信道，存在信道分配和竞争问题，为了提高利用率，站点的发射功率都比较低，并且电磁波信号易受到无线信道中的各种噪声，信道衰落和障碍物等因素的影响，因此站点的通信距离有限，一个站点发出的信号，并不是网络中的每一个站点都能检测到。例如图 6 中，A 和 C 检测不到彼此的无线信号，都以为 B 是空闲的，因而都向 B 发送数据，结果发生碰撞。站点 A 正在向站点 B 发送数据，但此时站点 C 也想发送数据给 B。当站点 C 在监听信道时，由于不知道站点 A 正在与站点 B 通信，所以得出错误的结论：站点 B 空闲，现在可以发送数据给站点 B。其结果是产生冲突这种未能检测出媒体上已存在的信号的问题叫做隐蔽站问题（hidden station problem）。

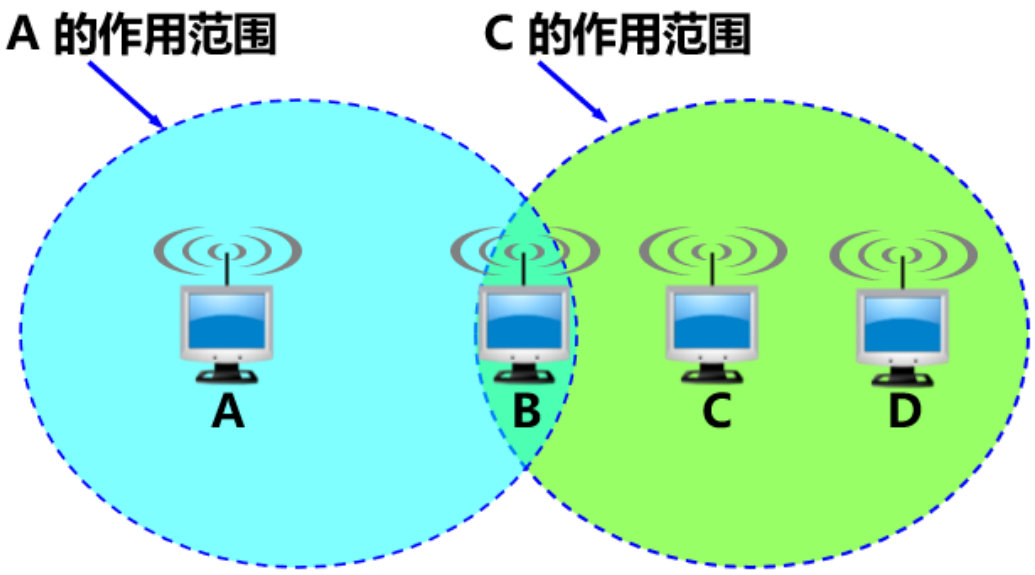


图 6: 隐蔽站点问题

当前无线局域网最主要的应用是使用便携式无线设备通过 AP 连接到传统有线网络，即网络的拓扑结构为基础型。在基础型网络中由于所有站点之间不能直接通信，都需要通过中心接入点进行中继转发，每个站点均可以和位于网络中心区域的接入点相互通信，若两个站点位于

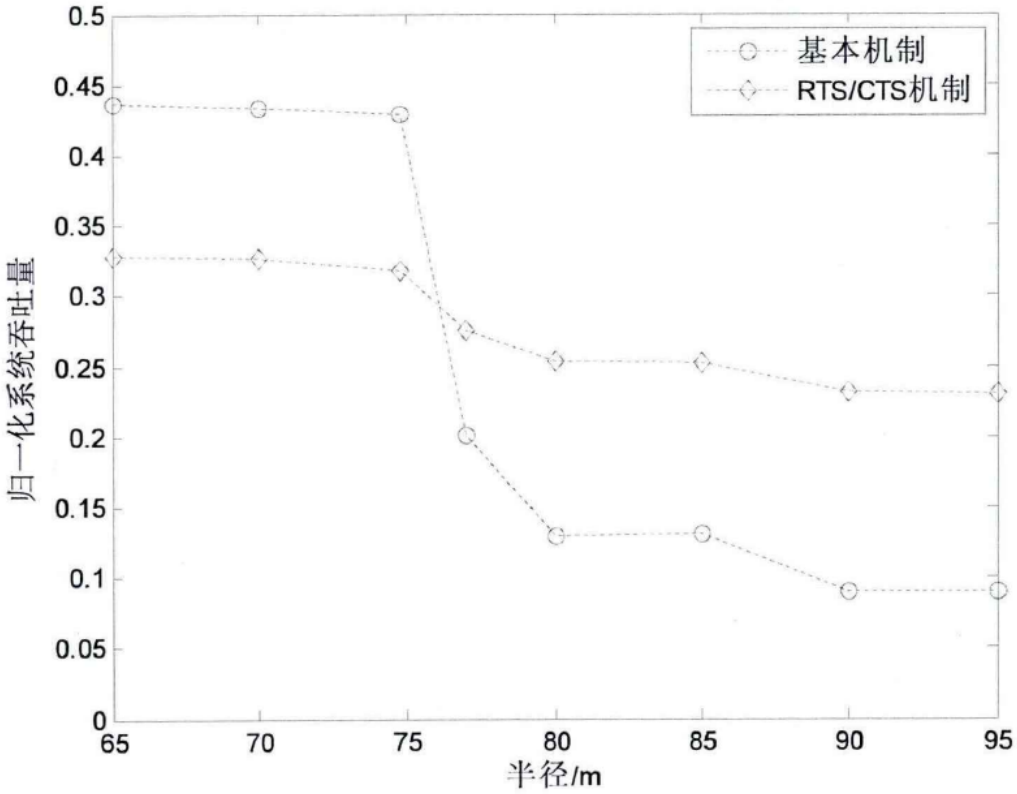


图 7: 仿真结果图

网络相反方向的边界区域，且它们之间距离远，虽然它们可以通过 AP 进行通信，但是此时这两个站点可能够侦听不到对方存在，便形成一对隐蔽站点。所以，在基础型网络中有可能会出现隐蔽站点。

3.1.2　隐蔽站点问题解决措施

IEEE802.11 中 DCF 模式下启动 RTS/CTS 握手协议消除隐蔽站点的干扰。当站点 A 要想站点 B 发送数据之前，先发送一个控制报文 RTS（请求发送），站点 B 收到 RTS 保温后，向站点 A 回应 CTS（允许发送）控制报文；只有当站点 A 收到 CTS 后才向 B 发送数据，如果 A 没有收到 CTS，站点 A 认为发生了冲突，退避一段时间重发 RTS；若隐蔽的站点 C 收到 B 向 A 发送的 CTS，知道有站点向 B 发送数据，站点 C 延迟发送，这样克服了隐蔽站点的干扰。

图 7 显示了通过 NS2 仿真软件，使用 RTS/CTS 机制有助于克服隐蔽站点的影响。当距离大于 75m 时，存在隐蔽站点，随着距离的增加，冲突概率叶随之增加，基本机制的性能急剧

下降，而采用 RTS/CTS 机制虽然性能有所下降，但是明显高于基本机制；距离小鱼 75m 时，不存在隐蔽站点，由于 RTS/CTS 才产生额外的控制开销，所以其性能明显低于基本机制.

可见，当存在隐蔽站点时，使用 RTS/CTS 交换有助于提高系统云图两；而当不存在隐蔽站点时，使用 RTS/CTs 交换使吞吐量降低，提高网络传输效率的关键是要能够检测到网络中隐蔽的站点，来决定是否启用 RTS/CTS 交换。

第 4 章　隐蔽站点静态检测法及其局限性

该方法仅适用站点静止的应用环境，而在站点移动环境下不仅不能提高反而可能降低网络性能

4.1　隐蔽站点的静态检测方法介绍

该算法定义了两种无线传输半径，有效传输半径 Rx，侦听半径 Rc。Rx 和 Rc 大小取决于数据发送速率，天线等因素，且 Rc 大于 Rx，以站点为圆心，半径 Rx 的圆形区域为有效传输范围；以站点为圆心，内圆半径为 Rx，外圆半径为 Rc 的唤醒区域为载波侦听范围。

数据传输范围表示：在该区域内，站点能够接收并且正确解码传输帧。载波侦听范围表示：在该区域内，站点能够物理地侦测出传输媒介忙，但是不能正确解码传输帧。

图 9 显示了发送站点（TX STA）以一定速率发送一个数据帧，接受站点（RX STA）在正确接收后，经过 SIFS 时间间隔后回复 ACK 帧。其中：大小许仙元分别表示 TX STA 的 Rc 与 Rx，大小实线圆分别表示 RX STA 的 Rc 与 Rx。图中所标示的数字 1-8 表示网络中其他站点可能所处的位置。

图 4.3 显示了网络中其他站点在这次成功过程中的接收状态，分别为：

（1）位于区域 1 站点，既能侦听到又能正确解码 TX STA 发送的数据帧和 RX STA 回复的 ACK 帧。TX STA 对此区域中的站点不构成隐蔽。

（2）位于区域 1 站点，既能侦听到又能正确解码 TX STA 发送的数据帧；RX STA 发送的 ACK 帧，虽然可以侦听到，但是解码出错。TX STA 对此区域中站点不构成隐蔽。

（3）位于区域 3 站点，既能侦听到又能正确解码 TX STA 发送的数据帧；侦听不到 RX STA 发送的 ACK 帧。TX STA 对此区域中站点不构成隐蔽。

（4）位于区域 4 站点，虽然不能正确解码 TX STA 发送的数据帧，但是可以侦听到该帧；对于 RX STA 发送的 ACK 帧，既不能正确解码，也不可侦听其发送国耻，TX STA 对此区域中站点不构成隐蔽。

（5）位于区域 5 站点，TX STA 发送的数据帧和 RX STA 发送的 ACK 帧，都仅仅能够侦听到而不可以正确解码接受。TX STA 对此区域中站点不构成隐蔽。

（6）位于区域 6 站点，TX STA 发送的数据帧可以被侦听到，但是解码错误；RX STA 发送的 ACK 帧，技能被侦听到又能被正确解码。TX STA 对此区域中站点不构成隐蔽。

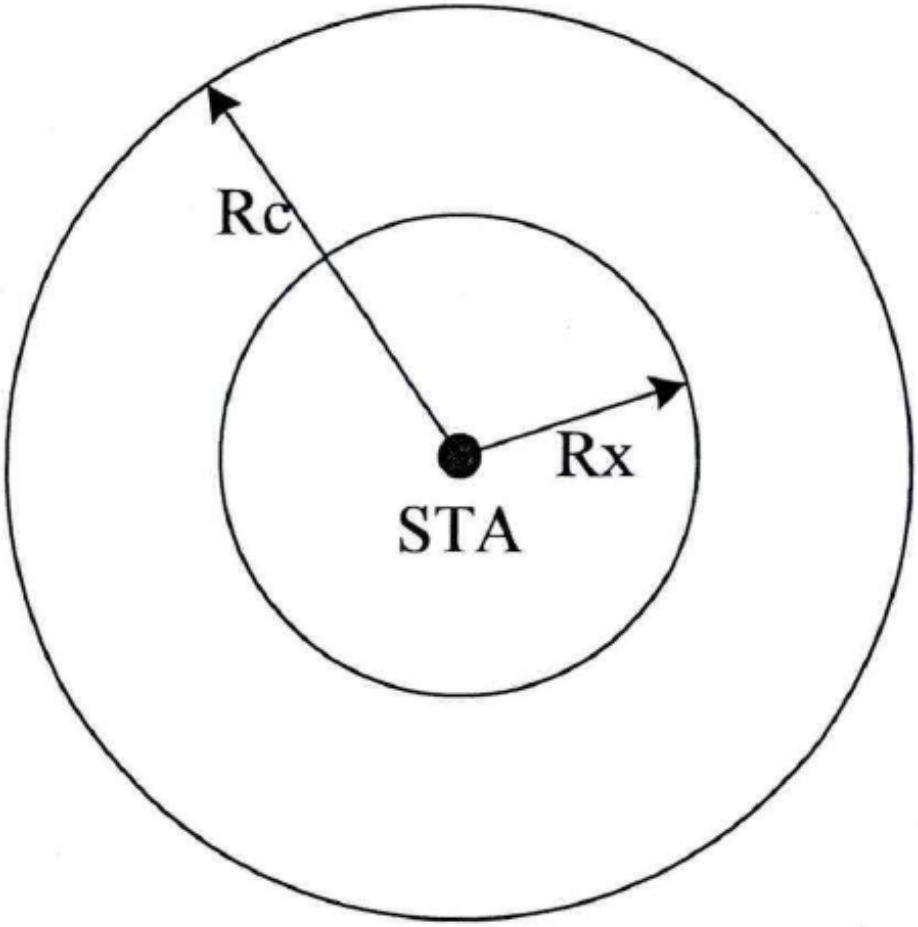


图 8: Rx 与 Rc 示意图

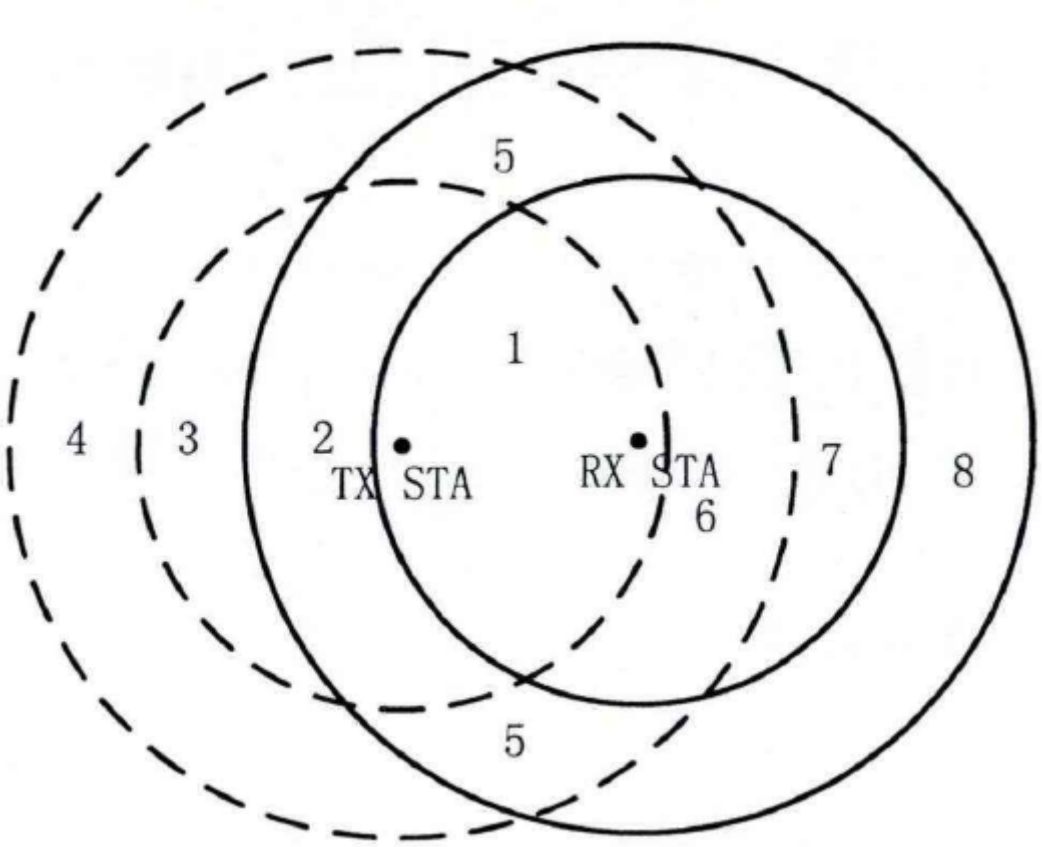


图 9: TX STA 与 RX STA 间一次有效传输过程

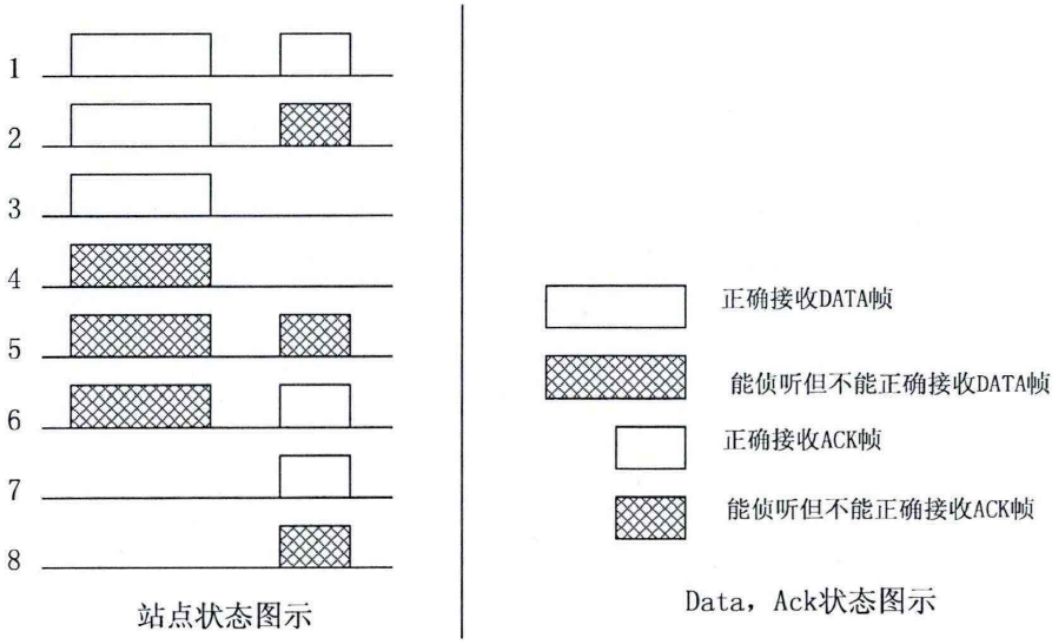


图 10: 站点接收状态

（7）位于区域 7 站点，TX STA 发送的数据帧既不能正确解码接收也不可以侦听到；RX STA 发送的 ACK 帧，既可以侦听到，又可正确解码，TX STA 对此区域中站点构成隐蔽；

（8）位于区域 8 站点，TX STA 发送的数据正既不能正确解码接收也不可以侦听到；RX STA 发送的 ACK 帧，仅能侦听到而不可以正确解码，TX STA 对此区域中站点构成隐蔽。

从（7）和（8）可以看出，当站点收到 ACK 帧而没有检测到前面数据时，站点就可以推断网络中存在对其隐蔽的站点。

当站点收到 ACK 帧售后，它可能成功地解码 ACK 帧中 PSDU 部分，从而根据 MAC 帧结构中的类型字段来判定这是 ACK 帧；反之，如果解码失败（帧校验错误），虽然此时站点未能判断收到的帧为 ACK，但是可以利用 PLCP 标头来判定收到的帧为 ACK，一位对于 ACK 帧和 CTS 帧，它们具有特定长度值 14 字节，一个站点可以根据下列两种情形中任何一种来判断网络中存在隐蔽站点：

1. 在传输媒介空闲时间超过 SIFS 间隔后收到 ACK 帧；

2. 在传输媒介空闲时间超过 SIFS 间隔后收到校验错误的帧，但是其 PLCP 标头中长度字段为 14 字节。

在这两种情形下，其它的站点都能够检测到该隐蔽的站点的存在。对于第一种情形，站点（位于区域 7）能够从接收到的 ACK 地址字段获得该隐蔽站点的 MAC 地址。对于第二种情形，站点（位于区域 8 中）虽然不能获得该隐蔽站点的 MAC 地址信息，但是这对于判断网络

中存在隐蔽的站点已经足够。同时，不同的物理层，其 PLCP 长度字段具有各不相同的内容：在 IEEE802.11a 中，其长度字段含有字节数用来表明 PSDU 的长度；而在 IEEE802.11b 中，PLCP 长度字段被设置为发送该帧的所需要多少毫秒时间。然而，时间很容易被转换成帧长度，因为可以从 PLCP 的速率字段中获得当前帧的发送速度，很容易计算出发送中帧长度（速率乘以时间）。

在没有改变当前协议标准的情形下，提供了一个隐蔽的站点快速被检测出的方法，根据它相应地决定是否使用 RTS/CTS 交换。其基本思想是：在进入系统初始时刻，站点使用基本接入机制，但是，当检测到隐蔽站点时候切换到 RTS/CTS 机制，并且一直保持下去。判断网络中是否存在隐蔽站点的依据是：收到 ACK 帧之前，信道持续空闲的时间长度。只要站点在正确接收或侦听到 ACK 之前，没有正确接收或侦听到数据帧（即在接收到或侦听到 ACK 之前信道空闲时间大于 SIFS），则可以判定该站点周围存在隐蔽的站点。此判定依据对于采用 RTS/CTS 交换同样也适用，即在接收到或侦听到 CTS 帧之前信道持续空闲时间大于 SIFS，则同样也可以认为该站点周围存在隐蔽的站点。算法流程如图 11 所示：

（1）站点在收到一帧数据后，仅当信道持续空闲时间大于 SIFS 后，站点才开始检测是否存在隐蔽站点；若空闲时间小于 SIFS，则程序返回，不做任何检测；

（2）若空闲时间大于 SIFS，且循环冗余校验正确，则判断帧类型：如果为 ACK 帧，则表明检测到存在隐蔽站点；若不是 ACK 帧，则返回；

（3）若空闲时间大于 SIFS，且循环冗余校验出错，则判断接收的帧物理层是否采用

IEEE802.11a 协议标准：如果是 IEEE802.11a，查看 PLCP 中长度字段是否为 14 字节：若是，表明收到的是 ACK 帧，表明存在隐蔽站点；若不是 IEEE802.11a，则根据 PLCP 中长度值和速率值计算所接收的帖长度，若帧长度为 14 字节，表示接收的帧为 ACK，表明存在隐蔽站点。

4.2　静态检测方法的局限性

[h]

如图 12 所示，图中横坐标表示不同的半径 R，即各个站点与 AP 间距离，纵坐标表示归一化系统吞吐量。随着不同的半径值，系统吞吐量有所不同。当圆半径小于 75m 时，此网络中不存在隐蔽的站点，所以静态检测算法不必切换到 RTS/CTS 机制，所以其获得的性能和基本机制相同而高于使用 RTS/CTS 机制；而当圆半径大于 75m 时候，此时网络中存在隐蔽站点，由于静态检测算法能检测到隐蔽站点后使用 RTS/CTS 交换，所以其性能和 RTS/CTS 机制基本保持一致，但是要优于基本机制具有的性能。但是随着半径不断增加，网络中互为隐蔽站点的对数叶变大，其性能随之降低。图 3.5 也同时表明了在静止情形下，静态检测算法获得了基本接入机制与 RTS/CTS 接入机制间最好的性能。

但是有流程图可以看出，此算法仅仅是解决了监测站点从非隐蔽状态变为隐蔽状态，而从隐蔽状态变为非隐蔽状态并不能检测到，即只能实现从基本介入机制到 RTS/CTS 机制的单向

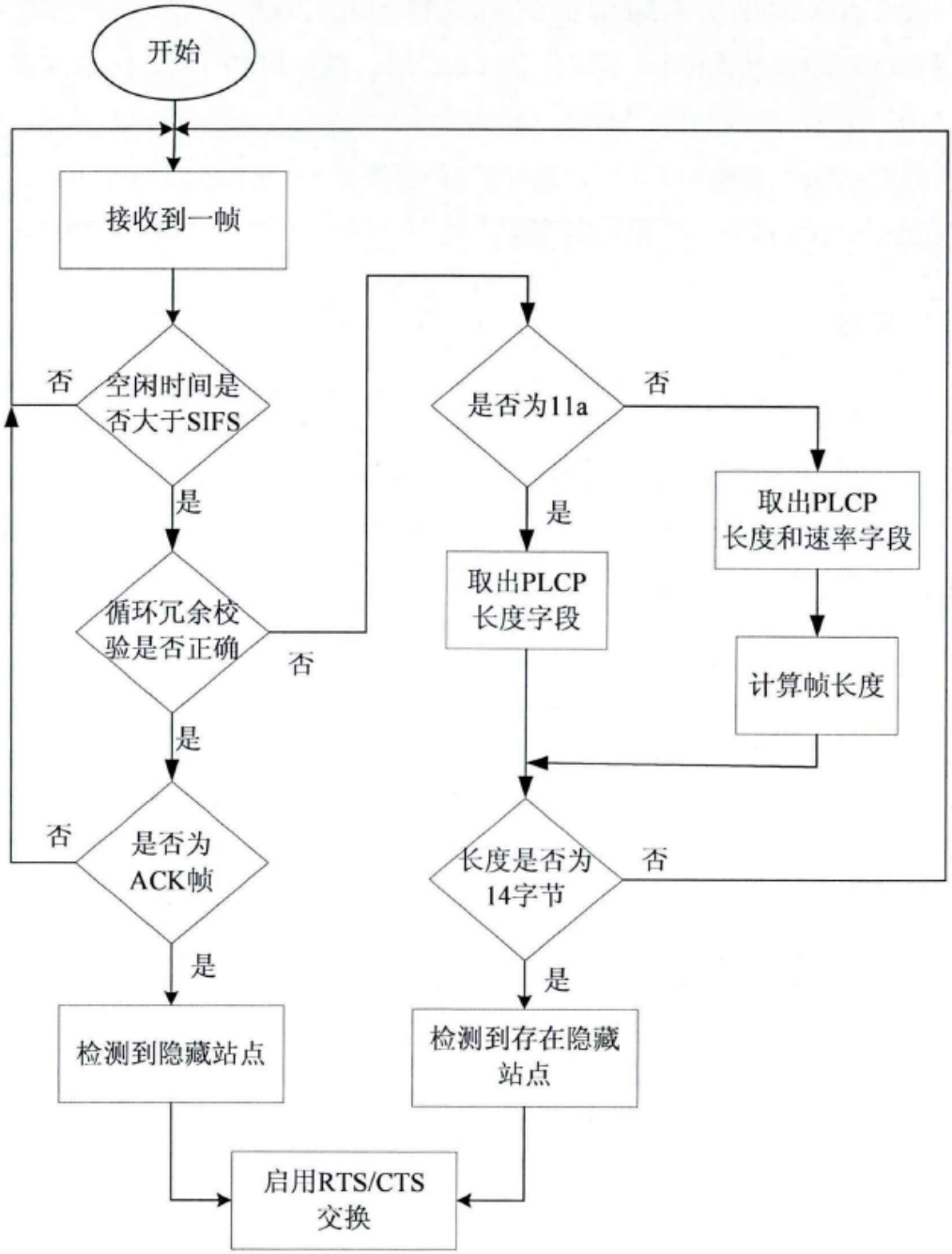


图 11: 静态隐蔽站点检测算法流程图

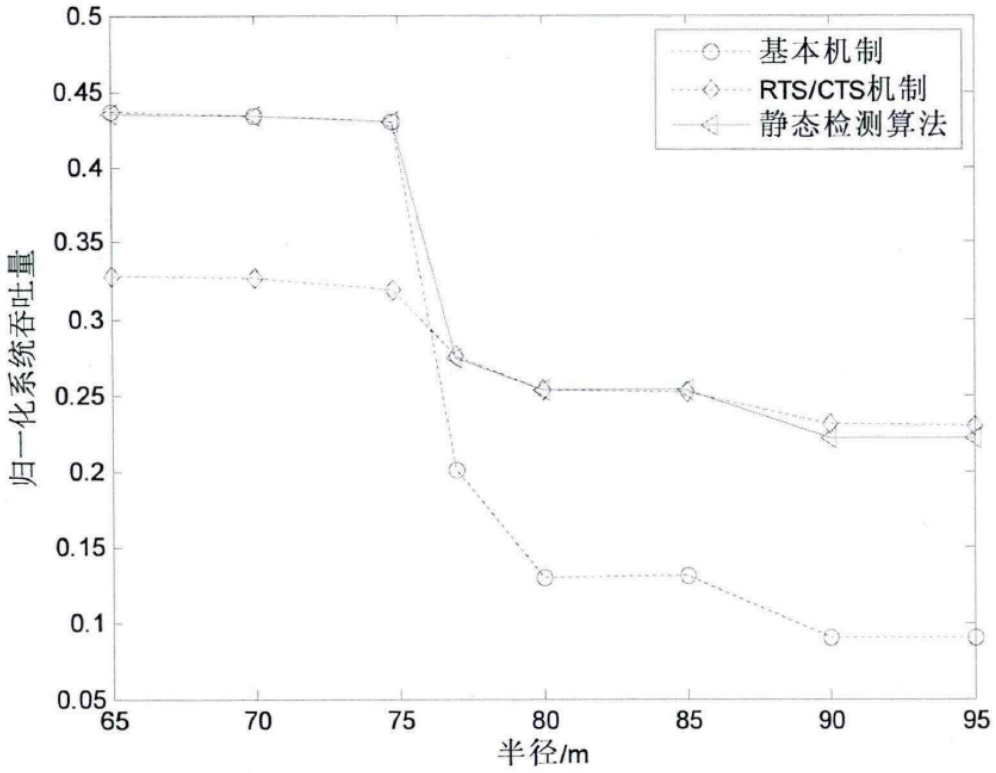


图 12: 静态检测算法站点静止仿真结果

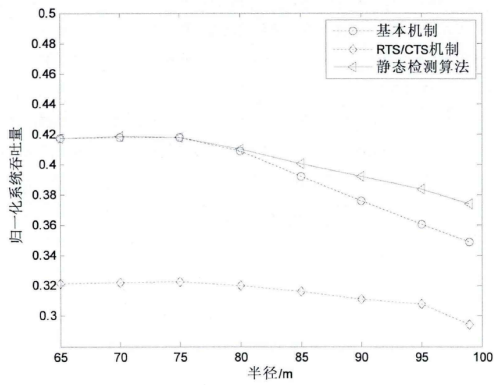


图 13: 静态检测算法站点向外运动仿真结果

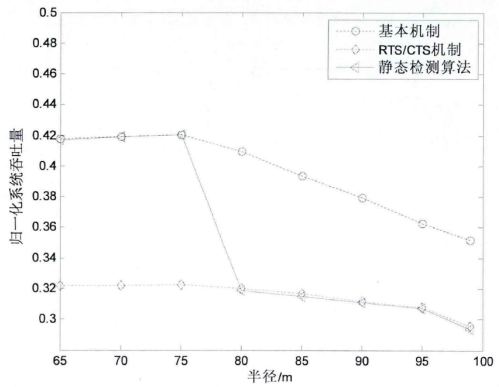


图 14: 静态检测算法站点向中心运动仿真结果

切换，不可以从 RTS/CTS 机制到基本机制的逆向切换。故不适用于站点在移动的环境下，站点在移动时，会出翔两种状态的来回切换，上述算法并不能实现。

因此，静态检测算法只能检测出隐蔽的站点，并未提供当该隐蔽的站点消失后的检测方法，所以适用于静止环境，并不适用于移动环境。

第 5 章　隐蔽站点动态检测法

静态检测算法在静止环境中可以获得很好的性能，而在某些移动环境下并未能提高性能，反而会使之降低，所以较适用于站点静止情况下。针对上述问题，基础型网络的结构特点，对静态检测算法加以改进，提出一种支持站点移动的隐蔽站点动态检测算法。动态检测算法可以实现基本机制与机制之间实时双向切换，从而提高网络性能。

5.1　隐蔽站点的静态检测方法介绍

实时双向基本机制与 RTS/CTS 交换之间动态切换的关键是网络中每个站点能够及时捕捉其周围隐蔽站点的变化情况：在检测到新的隐蔽站点时，必须要确定该站点的身份（地址信息）；当某一隐蔽站点变为非隐蔽站点时同样也必须能确定其份。在基础型网络中，由于所有站点间通信都需要 AP 中继，且能够覆盖所有的站点，所以各站点都能从发送的帧中，获得足够的信息捕捉周围隐蔽站点位置状态的变化。

站点 i 标记为 ST(i)，并假设各站点都具有相同的有效传输半径 Rt（i）与侦听半径 Rs（i）。ST（i）有效传输范围和侦听范围分别为 At（i）与 As（i）。

在基础型网络中，任何一个站点若要发送数据帧，都必须要经过 AP 进行中继转发或桥街道其他类型的网络，假设站点 ST(i) 发送数据，AP 在正确接收到 ST(i) 的数据帧后向其回复 ACK 确认。若在这一次传输的过程中 ST(1) 对 ST(i) 构成隐蔽（i 1），则 ST(i) 可能出现的位置区域如图 4.1 中阴影区域，此时 ST(i) 既不能正确接收也不能侦听到 ST(i) 的数据帧，但是可以正确接收 AP 向 ST(i) 回复的 Ack 帧。由于 ST(i) 在收到 ACK 之前信道空闲时间大于 SIFS，所以 ST(i) 能够判定在网络中存在对其隐蔽的站点。ST(i) 还可以根据 ACK 地址字段确定出隐蔽站点的身份是 ST(i) 并做记录。在基础型网络中，不会出现的一种情形：站点检测到存在隐蔽的站点，却不能够对隐蔽的站点身份就进行确认。

在解决了新增加隐蔽站点身份确认后，接下来讨论当某一个隐蔽站点变为非隐蔽站点状态后，如何检测出站点的这种状态变化和确定该站点的身份。

当 ST(i) 检测到 ST(1) 对其隐蔽后，由于站点的移动性，在经过一段时间后 ST(i) 必然出现在图 4.2 的阴影区域中，ST(i) 实际上已对 ST(i) 不构成隐蔽。此时若 ST(1) 向 AP 发送数据，AP 正确接收后向其回复 ACK 确认。则在不发生冲突情况下，ST(i) 能够侦听到 ST(1) 发送的数据，但是不可正确解码接受，并且可以正确接收 AP 向 ST(1) 回复的 ACK 帧。ST(i) 收到 ACK 之前信道空闲时间小鱼 SIFS（因为侦听到数据帧的发送过程），并且 ACK 的目的地址字段是 ST(1) 的地址。由此 ST(i) 可以判定 ST(1) 已由隐蔽站点变成非隐蔽站点，清楚该站点的隐蔽记录。

上述监测站点由隐蔽状态变成非要比状态以及身份验证的方法是当 ST(i) 位于图 4.2 中阴影区域，ST(1) 必须要向 AP 发送数据帧，AP 正确接收后向其回复 ACK 前提下获得的。若当 ST(i) 移动到此区域后，ST(1) 并未发送任何的数据帧，且 ST(i) 继续移动，直到位于图 17 中

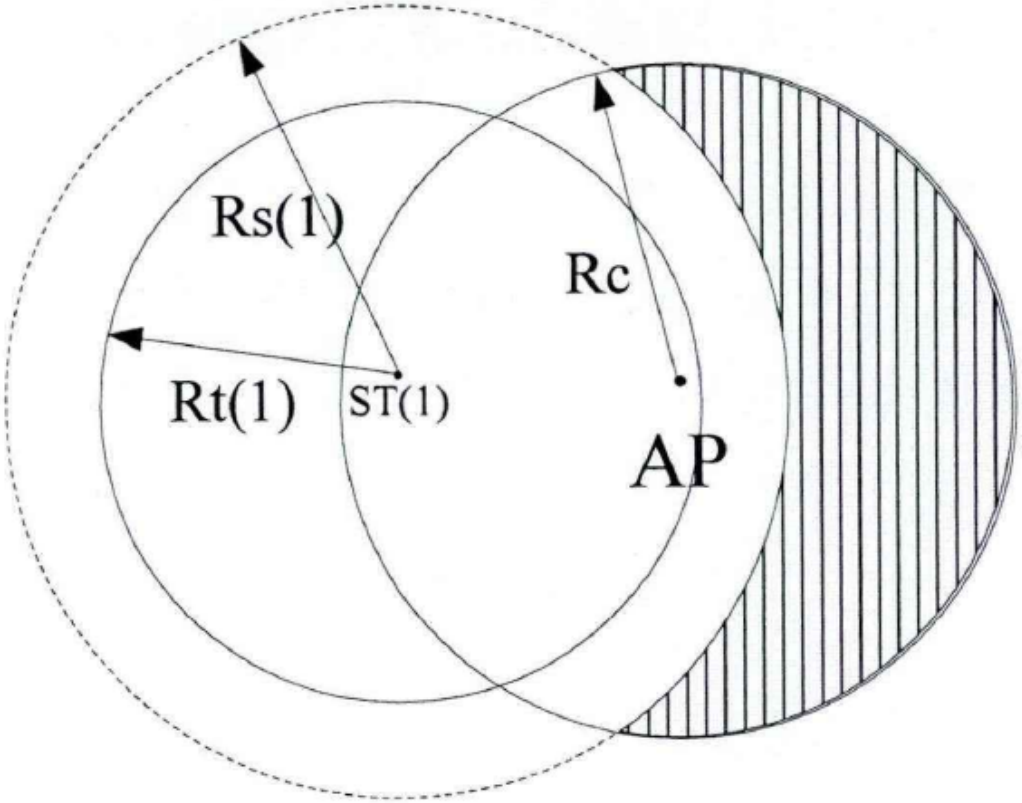


图 15: 隐蔽站点位置示意图

的阴影区域中，此时 ST(i) 不仅能够侦听而且可以正确解码 ST(1) 发送的数据帧。只要 ST(1) 发送数据帧，ST(i) 就可以根据该数据真的源地址字段值来判定 ST(1) 已对其不构成隐蔽。

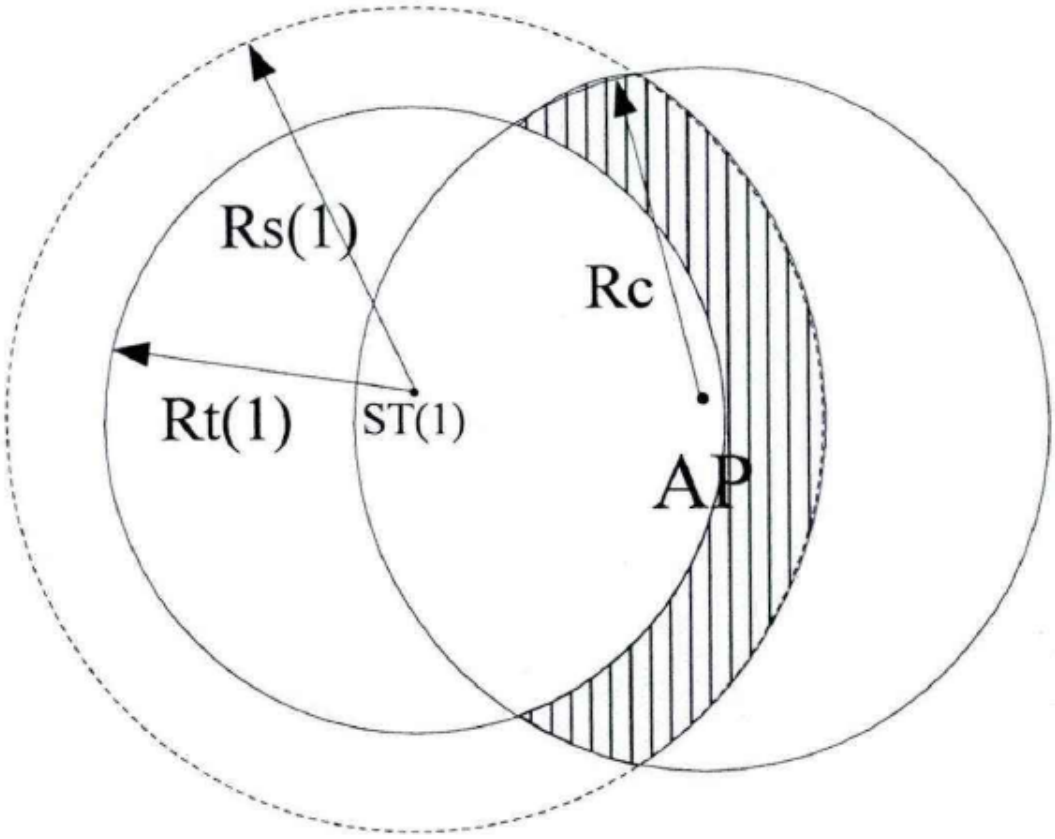


图 16: 站点位于侦听范围内

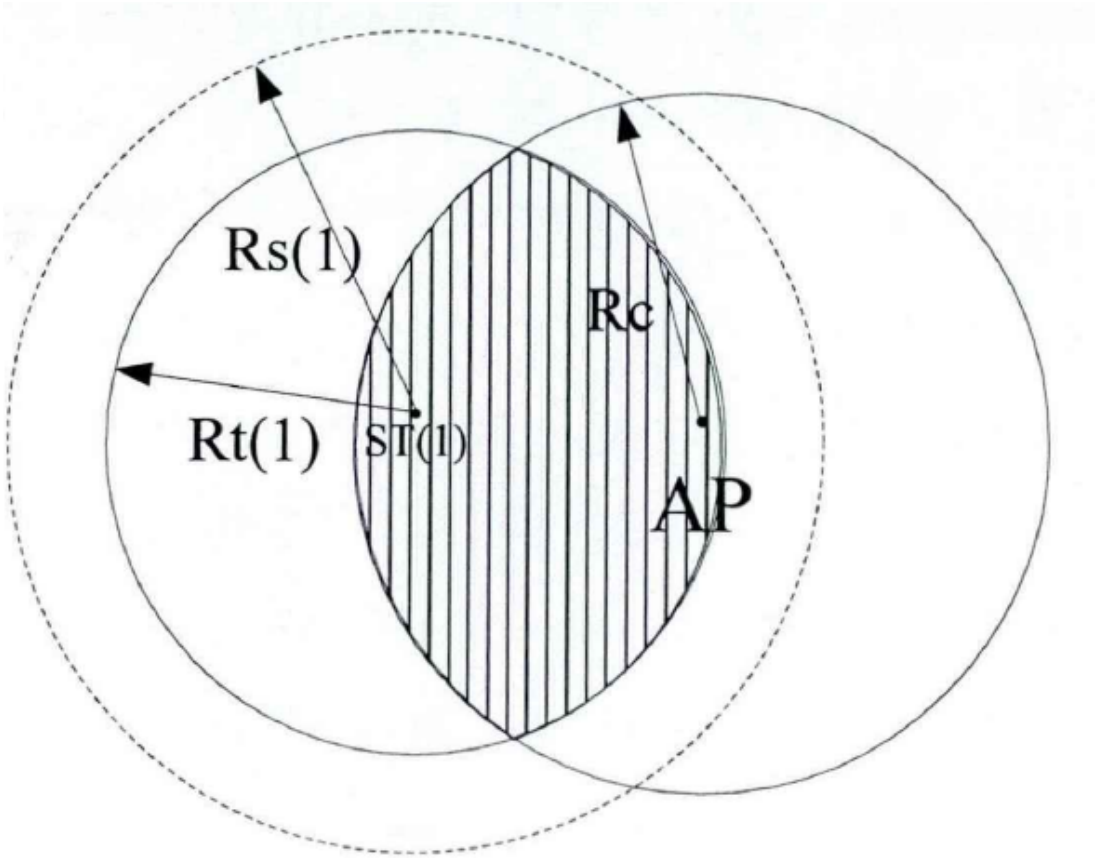
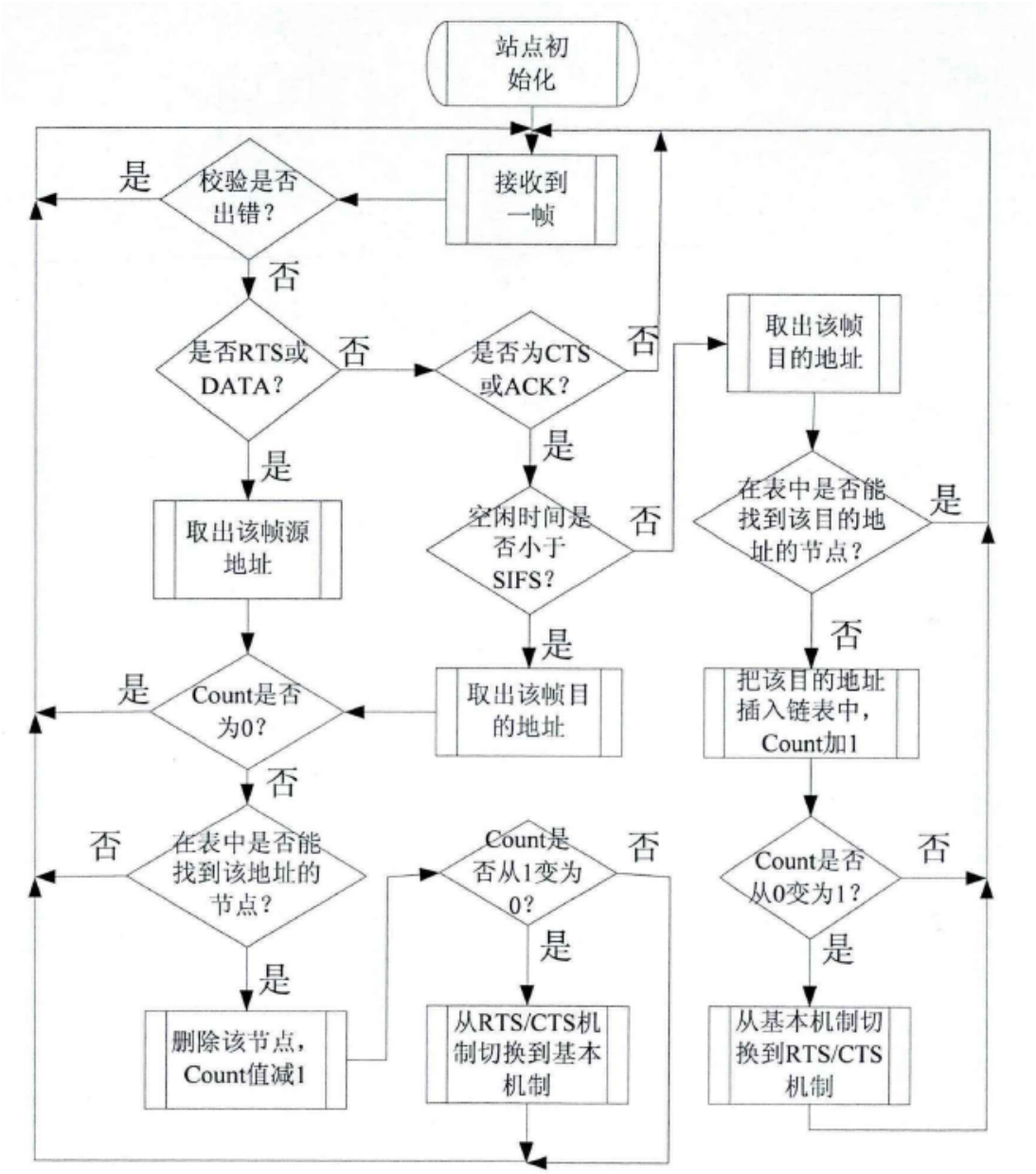


图 17: 站点位于有效传输范围内


站点初始化
接收到一帧
校验是否出错?
是
否
是否RTS或DATA?
否
是否为CTS或ACK?
否
是
取出该帧源地址
空闲时间是否小于SIFS?
否
是
取出该帧目的地址
Count是否为0?
是
否
在表中是否能找到该地址的节点?
否
是
删除该节点，Count值减1
Count是否从1变为0?
否
是
从RTS/CTS机制切换到基本机制
取出该帧目的地址
在表中是否能找到该目的地址的节点?
是
否
把该目的地址插入链表中，Count加1
Count是否从0变为1?
否
是
从基本机制切换到RTS/CTS机制