



中华人民共和国通信行业标准

YD/T 2772-2014

手机支付 基于 2.45GHz RCC(限域通信)技术的 非接触射频接口技术要求

Mobile payment
technical requirements for contactless radio frequency interface
based on 2.45GHz range controlled communication technology

2014-12-24 发布

2014-12-24 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 术语和定义	1
3 缩略语	2
4 概述	3
5 协议层次	3
5.1 协议划分	3
5.2 协议层次关系	4
6 物理层	6
6.1 磁通道	6
6.2 射频通道	8
7 数据链路层	9
7.1 磁通道	9
7.2 射频通道	10
8 传输层	15
8.1 包格式	15
8.2 包传输	17
9 会话层	18
9.1 消息	18
9.2 协议会话流程	20
9.3 通信会话命令	29
附录A (规范性附录) RF通信参数计算	41
附录B (规范性附录) 密码相关算法定义	43
附录C (资料性附录) 磁通道通信原理说明	47

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准是手机支付系列标准之一。该系列标准的名称预计如下：

1. 手机支付 术语和定义
2. 手机支付 总体技术要求
3. 手机支付 基于13.56MHz近场通信技术的移动终端技术要求
4. 手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块技术要求
5. 手机支付 基于2.45GHz RCC（限域通信）技术的智能卡技术要求
6. 手机支付 基于13.56MHz近场通信技术的非接触式销售点终端技术要求
7. 手机支付 基于2.45GHz RCC（限域通信）技术的非接触式读写器终端技术要求
8. 手机支付 基于13.56MHz近场通信技术的非接触射频接口技术要求
9. 手机支付 基于2.45GHz RCC（限域通信）技术的非接触射频接口技术要求
10. 手机支付 智能卡和内置模块安全技术要求
11. 手机支付 移动终端安全技术要求
12. 手机支付 多应用管理技术要求
13. 手机支付 基于13.56MHz近场通信技术的移动终端测试方法
14. 手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块测试方法
15. 手机支付 基于2.45GHz RCC（限域通信）技术的智能卡测试方法
16. 手机支付 基于13.56MHz近场通信技术的非接触式销售点终端测试方法
17. 手机支付 基于2.45GHz RCC（限域通信）技术的非接触式读写器终端测试方法
18. 手机支付 基于13.56MHz 的非接触射频接口测试方法
19. 手机支付 基于2.45GHz RCC（限域通信）技术的非接触射频接口测试方法
20. 手机支付 智能卡和内置模块安全测试方法
21. 手机支付 移动终端安全测试方法
22. 手机支付 多应用管理测试方法

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、国民技术股份有限公司、中国移动通信集团公司、中国联合通信有限公司、中国电信集团公司。

本标准主要起草人：杨军、袁琦、吕松栋、杨贤伟、李美祥、黄鹏、葛欣、李铭轩、张强、王兆申、吴淳、戴军尧、王逊。

手机支付

基于 2.45GHz RCC（限域通信）技术的非接触射频接口技术要求

1 范围

本标准规定了基于2.45GHz RCC（限域通信）技术的近距离无线通信接口及信息交换协议，包括磁通道与射频通道的协议层次模型、协议物理层、链路层、传输层和会话层所传输处理的数据单元，以及协议基本流程、协议防冲突机制和协议消息命令等。

本标准适用于基于2.45GHz RCC（限域通信）技术的手机支付系统。

2 术语和定义

下列术语和定义适用于本文件。

2.1

限域通信 Range Controlled Communication

通信距离范围可控的无线近距离通信技术。

2.2

发起方 Initiator

2.45GHz手机支付系统距离控制通信的发起方。

2.3

响应方 Target

2.45GHz手机支付系统对发起方命令请求做出响应的通信方。

2.4

接入标识码 Access Identifier

用于标识不同的接入响应会话。

2.5

多响应方冲突 Multi Target Collision

多个响应方位于同一个发起方的可接入范围内，发起方将随机地选择任意一个响应方进行接入，使得用户无法直观判断出被接入的响应方，从而造成本次交易具有不确定性。

2.6

冲突检测码 Collision Detect Code

用于冲突检测的识别码。

2.7

响应方随机标识 Target Random Identifier

用于冲突检测关闭时，响应方进行连接确认的随机识别码。

2.8

冲突响应时间窗 Collision Response Time Window

响应方在检测到MTC冲突后连续发送冲突响应消息的时间段。

2.9

会话命令超时时间 Session Command Timeout

响应方接收超时：发起方应当在规定的超时时间内发出相应的会话命令，否则响应方认为该次会话发起方超时。

发起方接收超时：响应方应当在规定的超时时间内对发起方的命令做出响应，否则发起方认为该次会话响应方超时。

2.10

磁通道基本消息 Magnetic Channel Message

在磁通道上传输的长度不大于15字节的消息。

2.11

磁通道扩展消息 Extended Magnetic Channel Message

在磁通道上传输的长度大于15字节的消息。

2.12

磁场场强变化率调制 Magnetic Field Strength Slope Modulation

以磁场的场强变化率 dH/dt 来表示符号“1”和符号“0”。

3 缩略语

3DES	Triple Data Encryption Standard	三重数据加密标准
ACK	Acknowledgment	RF应答帧
AES	Advanced Encryption Standard	高级加密标准
AID	Access ID	接入标识码
APDU	Application Protocol Data Unit	应用协议数据单元
CBC	Cipher Block Chaining	密文块链接模式
CDC	Collision Detect Code	冲突检测码
CRC	Cyclic Redundancy Check	循环冗余校验
DES	Data Encryption Standard	数据加密标准
DME	Differential Manchester Encoding	差分曼彻斯特编码
ECB	Electronic Cipher Book	电子密码本模式
EIRP	Equivalent Isotropically Radiated Power	有效全向辐射功率
GFSK	Gaussian Frequency-Shift Keying	高斯频移键控
LMF	Long Message Format	长消息编码格式
LSB	Least Significant Bit	最低有效位
MAC	Message Authentication Code	消息认证码
MC	Magnetic Channel	磁通道
MCF	Magnetic Channel Frame	磁通道帧
MCM	MC Message	磁通道基本消息

MCMc	Extended MC Message	磁通道扩展消息
MCP	MC Packet	磁通道数据包
MFSSM	Magnetic Field Strength Slope Modulation	磁场场强变化率调制
MPDU	MC Protocol Data Unit	磁通道协议数据单元
MSB	Most Significant Bit	最高有效位
MTC	Multi Target Collision	多响应方冲突
PRBS	Pseudorandom Binary Sequence	伪随机二进制序列
RC	RF Channel	射频通道
RCC	Range Controlled Communication	限域通信
RCF	RF Channel Frame	射频通道帧
RCM	RF Channel Message	射频通道消息
RCP	RF Channel Packet	射频通道数据包
RF	Radio Frequency	射频
RMS	Root Mean Square	均方根
RPDU	RC Protocol Data Unit	射频通道协议数据单元
SM4	-	商用密码算法
SMF	Short Message Format	短消息编码格式
TRI	Target Random Identifier	响应方随机标识

4 概述

本标准采用RCC（限域通信）技术，将磁通道（MC）和2.45GHz射频通道（RC）进行绑定，共同完成近距离通信功能。磁通道利用准静态磁场，以耦合方式完成可靠距离控制；射频通道采用2.45GHz工业、科学和医疗（ISM）频段，以电磁场发射接收方式完成高速数据交换。协议会话层采用密码技术对射频通道交换的应用协议数据单元（APDU）的数据进行加密传输，加解密操作对上层应用完全透明。

5 协议层次

5.1 协议划分

本标准协议共划分为四层，分别定义如下：

- 物理层。规定磁通道和射频通道的物理接口特性，包括磁通道的编码方式、调制方式、磁场强度要求，以及射频通道的频段和信道、调制方式、发射参数等物理特性。
- 数据链路层。规定磁通道和射频通道的帧格式、组帧和解帧以及帧的发送和接收。
- 传输层。规定磁通道和射频通道的数据包格式、分包和组包以及包的发送和接收。
- 会话层规定消息格式、消息功能定义、消息交互流程、应用与业务的接口。

本标准协议层次划分如图1所示。

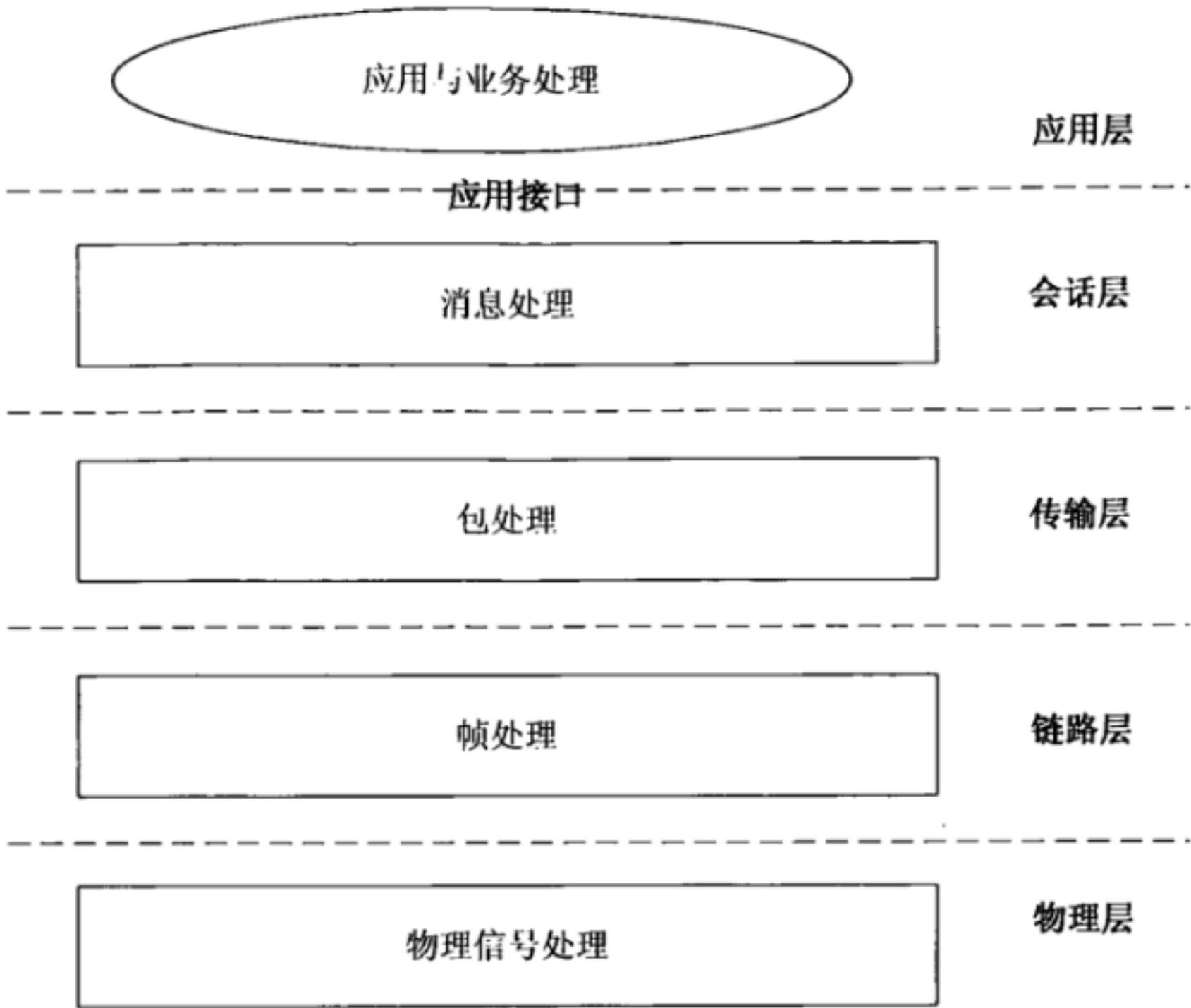


图1 协议层次划分

5.2 协议层次关系

5.2.1 协议数据单元

协议各层定义的数据单元如下：

- 帧。定义为链路层最小数据处理的单位，链路处理行为均基于帧进行处理，对有效数据进行扩展，形成信道能够稳定传输的机制。
- 包。定义为传输层处理的最小数据单位，传输层处理行为均基于包进行处理，对有效帧进行扩展，从而形成批量数据的传输机制。
- 消息。定义为会话层处理的最小数据单位，会话层处理行为均基于消息进行处理，对包进行扩展，并提供应用层的相关接口。

5.2.2 MPDU

5.2.2.1 Type1-MPDU

Type1-MPDU包括磁通道帧（MCF）和磁通道消息（MCM），如图2所示。

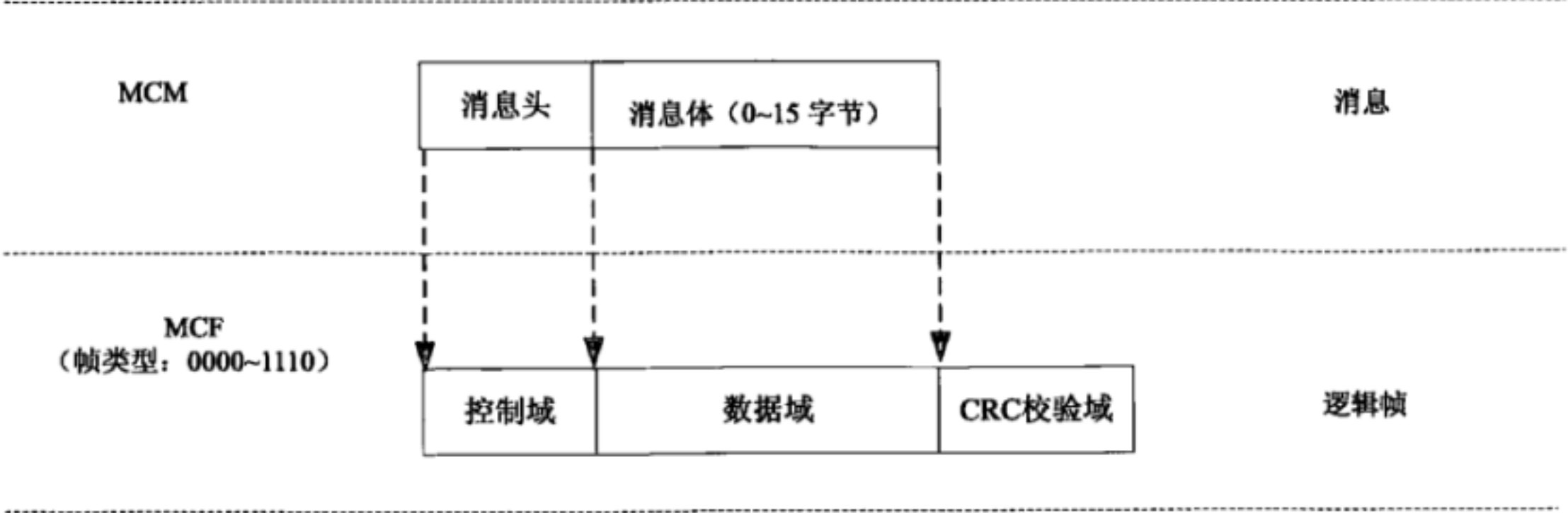


图2 Type1-MPDU（MCF、MCM）及其关系

MCF为磁通道链路层处理的数据单元，用于传输无需分包处理的磁通道基本消息MCM。MCF帧类型为：0000b~1110b。

MCM为磁通道会话层处理的数据单元，MCM使用SMF格式编码，直接通过一个MCF来传输。

MCM消息头通过MCF控制域传输，MCM消息体通过MCF帧数据域传输。

5.2.2.2 Type 2-MPDU

Type2-MPDU包括磁通道帧（MCF）、磁通道包（MCP）和磁通道扩展消息（MCMe），如图3所示。

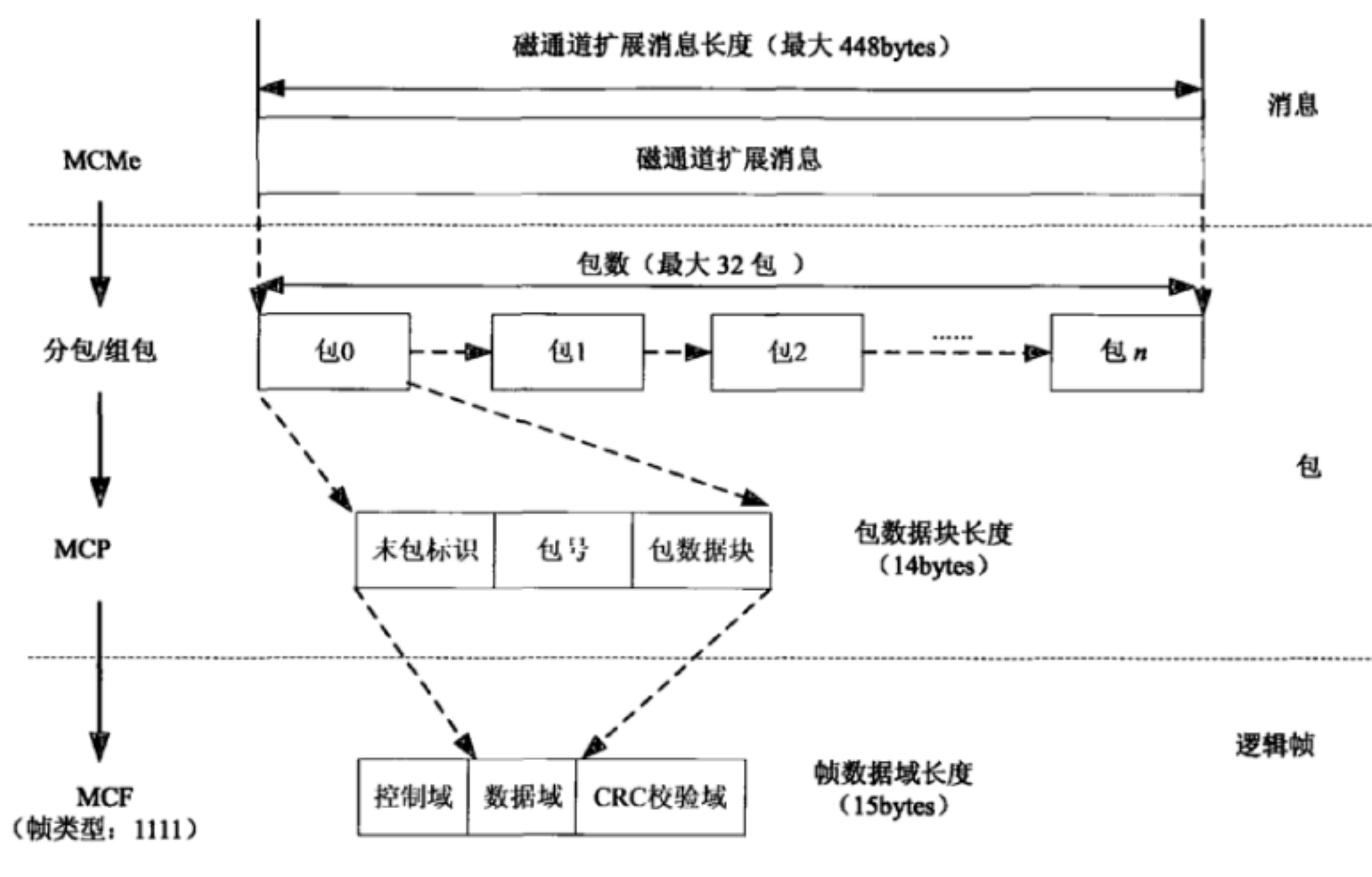


图3 Type2-MPDU (MCF、MCP、MCMe) 及其关系

MCF为磁通道链路层处理的数据单元，用于传输MCP。此类MCF帧的类型为1111b。

MCP为磁通道传输层处理的数据单元，每个MCP通过一个帧类型为1111b的MCF进行传输。

MCMe为磁通道会话层处理的数据单元，MCMe使用LMF格式编码，采用分包处理机制处理后通过一个或多个MCP进行传输。

5.2.3 RPDU

本标准定义的射频通道协议数据单元（RPDU）包括射频通道帧（RCF）、射频通道包（RCP）、射频通道消息（RCM），如图4所示。

RCF为射频通道链路层处理的数据单元，用于传输RCP。

RCP为射频通道传输层处理的数据单元，每个RCP通过一个RCF进行传输。

RCM为射频通道会话层处理的数据单元，RCM使用LMF格式编码，采用分包处理机制处理后通过一个或多个RCP进行传输。

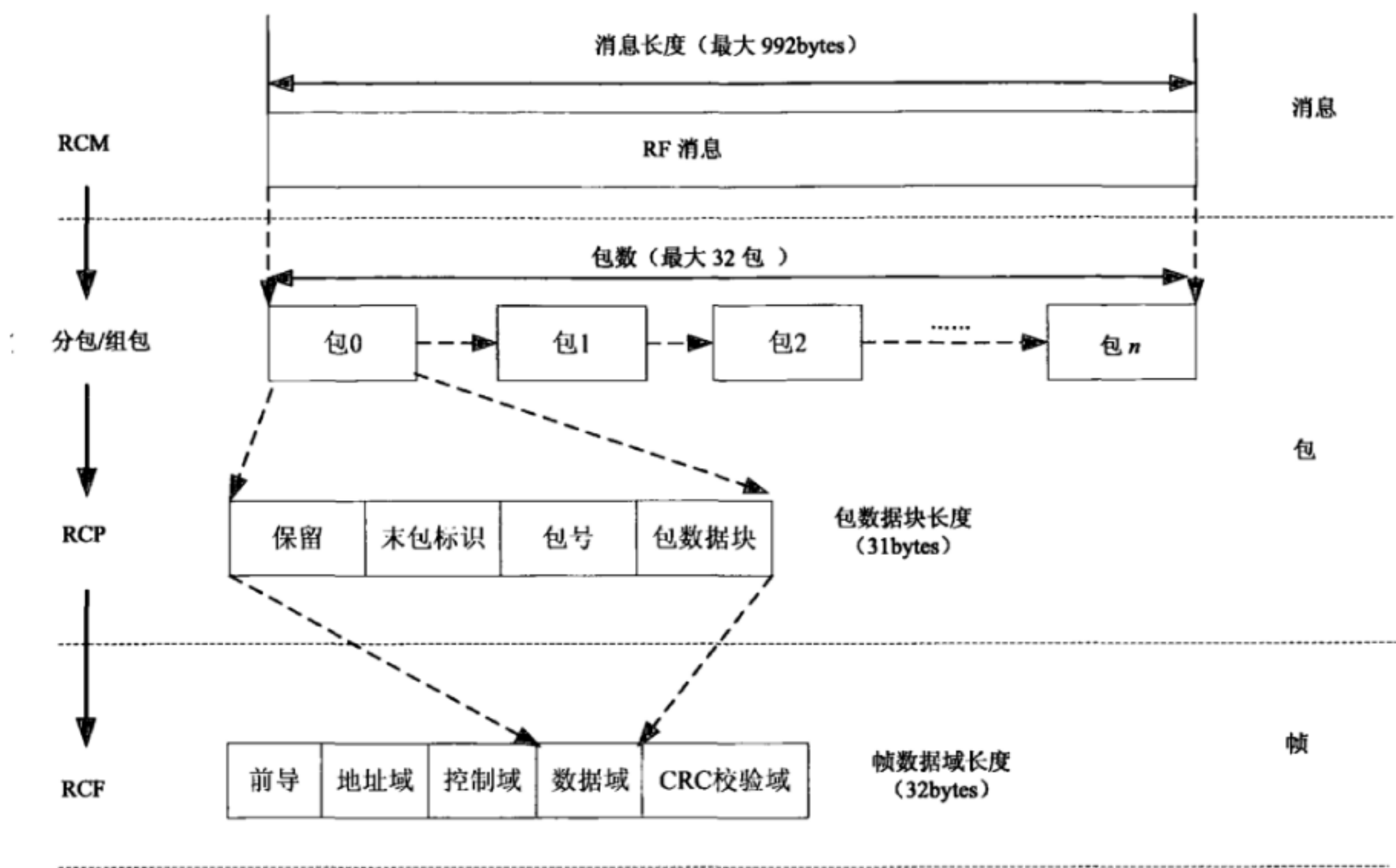


图4 RPDU (RCF、RCP、RCM) 及其关系

6 物理层

6.1 磁通道

6.1.1 磁通道通信概述

磁通道用于进行通信距离限制和数据传输。发起方发射出经过编码和调制的磁场信号，响应方检测磁场信号强度，实现通信距离限制；对接收到的磁场信号进行解调和解码，实现磁通道数据传输。

6.1.2 数据编码符号率

磁通道数据编码符号率为4kS/s，符号率容许偏差范围为±5%。

6.1.3 数据编码方式和调制方式

6.1.3.1 编码方式

磁通道数据编码采用差分曼特斯特编码（DME），如图5所示。

每个数据位由2个符号组成的序列表示，每个数据位的符号序列必须为“10”或“01”。

数据位“1”的符号序列与前一个数据位的符号序列相反，数据位“0”的符号序列与前一个数据位的符号序列相同。

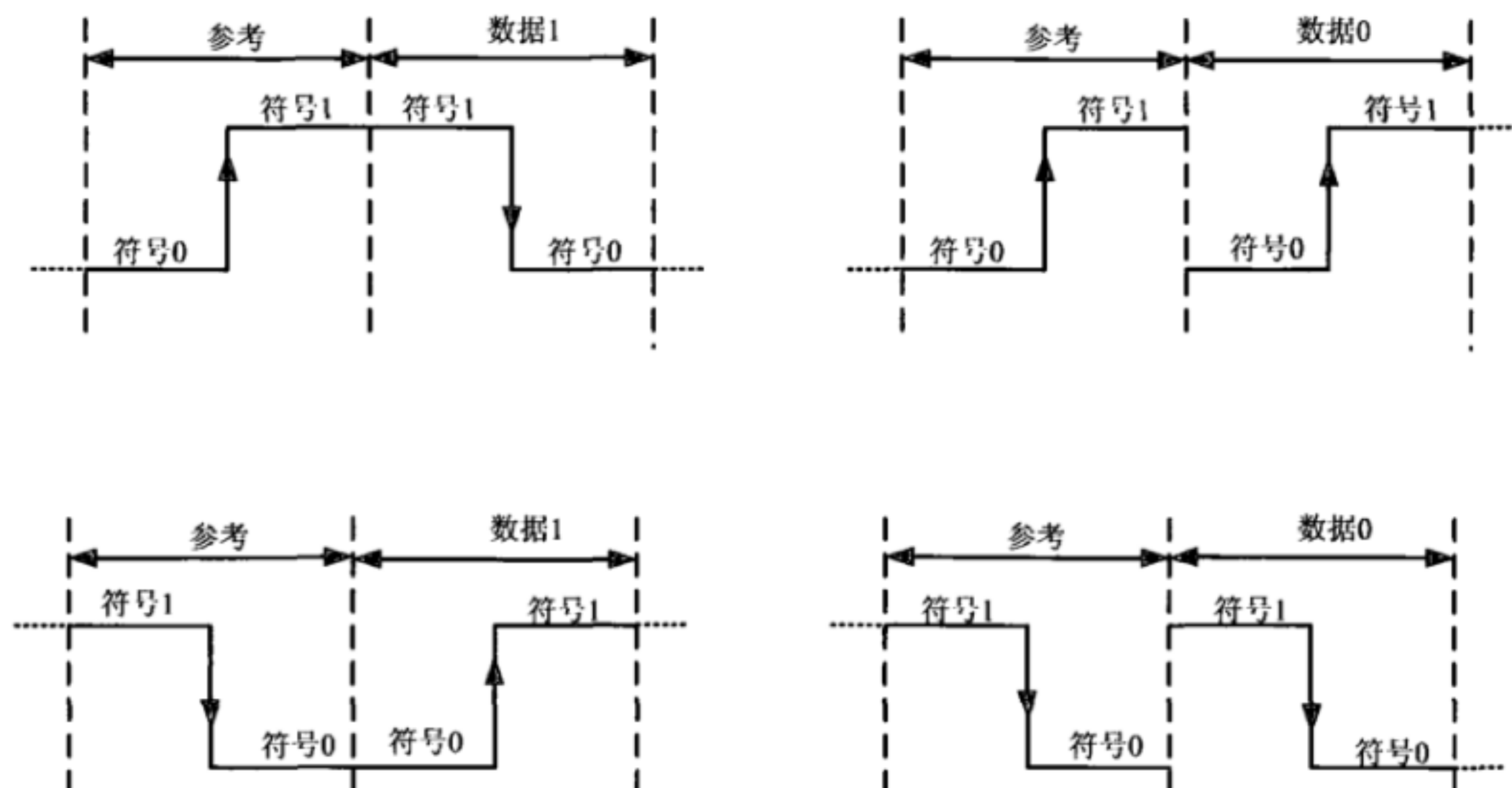


图5 差分曼特斯特编码

6.1.3.2 调制方式

磁通道信号采用磁场强度变化率调制，如图6所示。磁通道通信原理说明详见附录C。

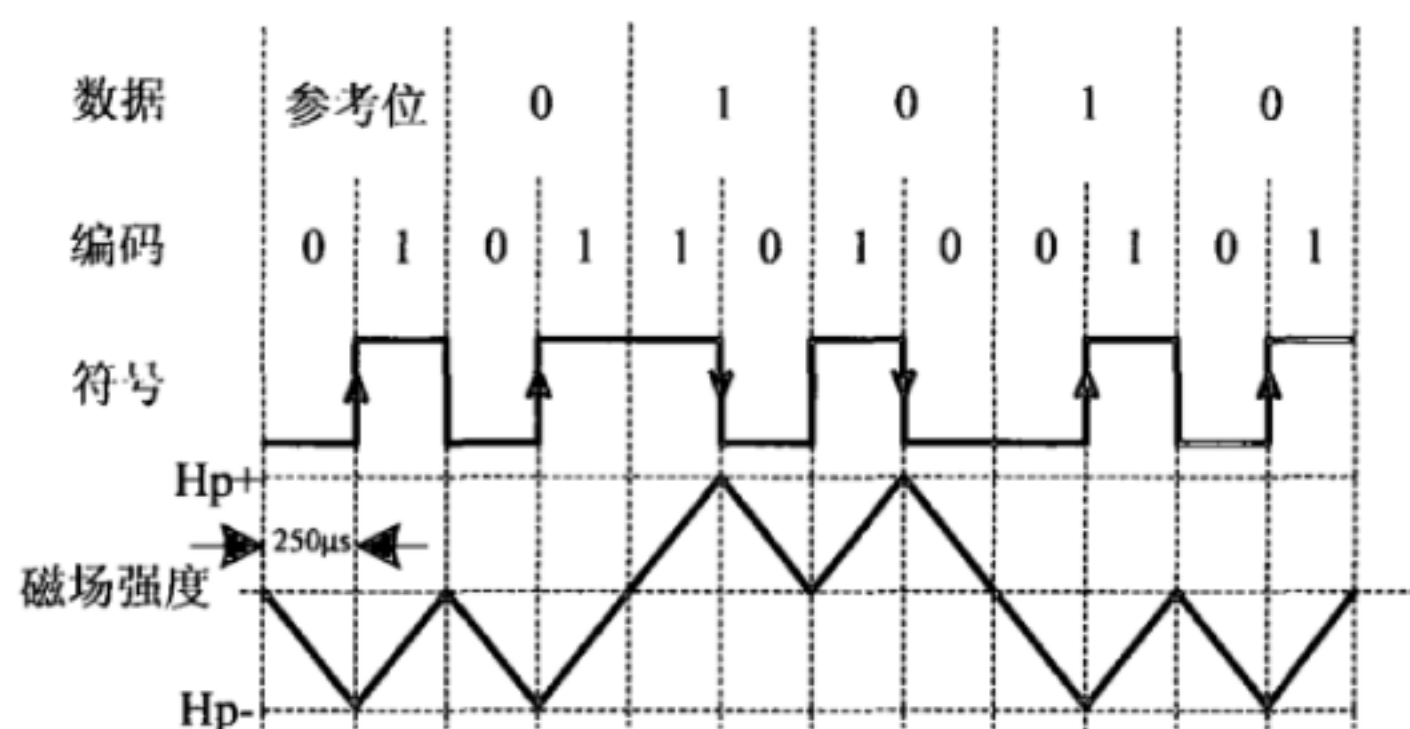


图6 磁场强度变化率调制

符号“1”的场强变化率与符号“0”的场强变化率应为相反关系，且变化率大小相等并保持恒定。
 H_p 为发起方磁场信号强度峰值。

6.1.4 发起方磁场信号强度

以发起方设备工作位置中心为基准，工作方向设备表面垂直距离0cm处磁场信号强度峰值应不小于160A/m且不大于300A/m；设备表面垂直距离10cm处磁场信号强度峰值应小于4.2A/m。

6.1.5 响应方磁场信号强度门限

响应方设备置于发起方设备的磁场信号工作区域，在磁场信号强度峰值 H_p 不小于6.7A/m时，响应方应能够与发起方建立并保持连接；

响应方设备置于发起方设备的磁场信号工作区域，在磁场信号强度峰值 H_p 不大于4.2A/m时，禁止响应方与发起方建立或保持连接。

6.1.6 磁场信号符号周期抖动

磁场信号各个符号周期对理想值（250μs）的偏离范围为磁场信号符号周期抖动。磁场信号符号周期抖动应不大于60μs。

6.2 射频通道

6.2.1 频段和信道分配

射频通道工作频率范围为2400 MHz~2483.5MHz。射频信道间隔为1MHz,各信道标称中心频率见表1。

表1 射频频段范围和信道中心频率

射频频段范围	射频信道标称中心频率 F_c
2400MHz~2483.5 MHz	$F_c=2400+k$ MHz, $k=1,2,\cdots,83$

信道划分如图7所示。

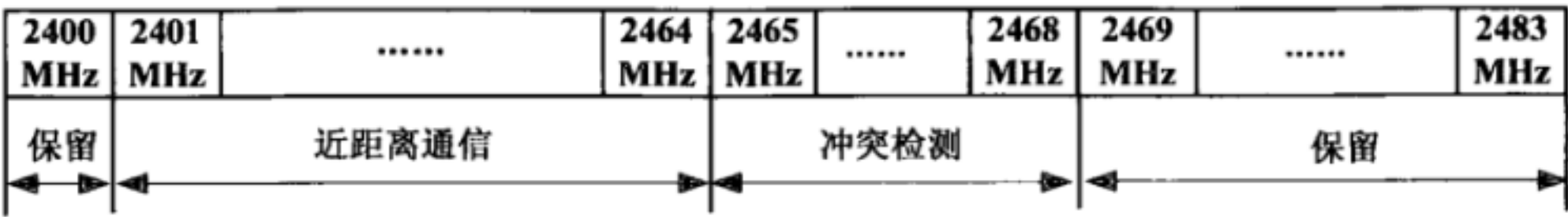


图7 信道划分

6.2.2 射频特性

6.2.2.1 发射功率

各射频信道传导发射功率最大不得超过+3dBm，有效全向辐射功率（EIRP）不得超过10mW。

6.2.2.2 射频频率容限

发射载波的初始中心频率 F_t 应在本信道标称中心频率 F_c 的 ± 75 kHz频率范围内，即：

$F_c - 75\text{ kHz} \leq F_t \leq F_c + 75\text{ kHz}$ 。

注： ± 75 kHz不包括数据发送过程中的频率漂移。

在一个数据帧传输时间内，发射载波中心频率累积漂移量应在 ± 20 kHz之内。

6.2.2.3 调制参数

射频通道信号调制方式为高斯移频键控（GFSK），带宽与码元宽度的乘积参数BT为0.5，符号率为1MS/s，调制指数应在0.27~0.55，即频率偏移幅度应在135kHz~275kHz。数据位“1”以正频偏表示，数据位“0”以负频偏表示。如图8所示，在1010数据序列传输中对应的最小频率偏移幅度 F_{\min} 应当不小于 $\pm 80\%$ 的00001111数据序列传输中的频率偏移幅度 F_d 。在任何情况下，最小频率偏移不应小于115kHz。

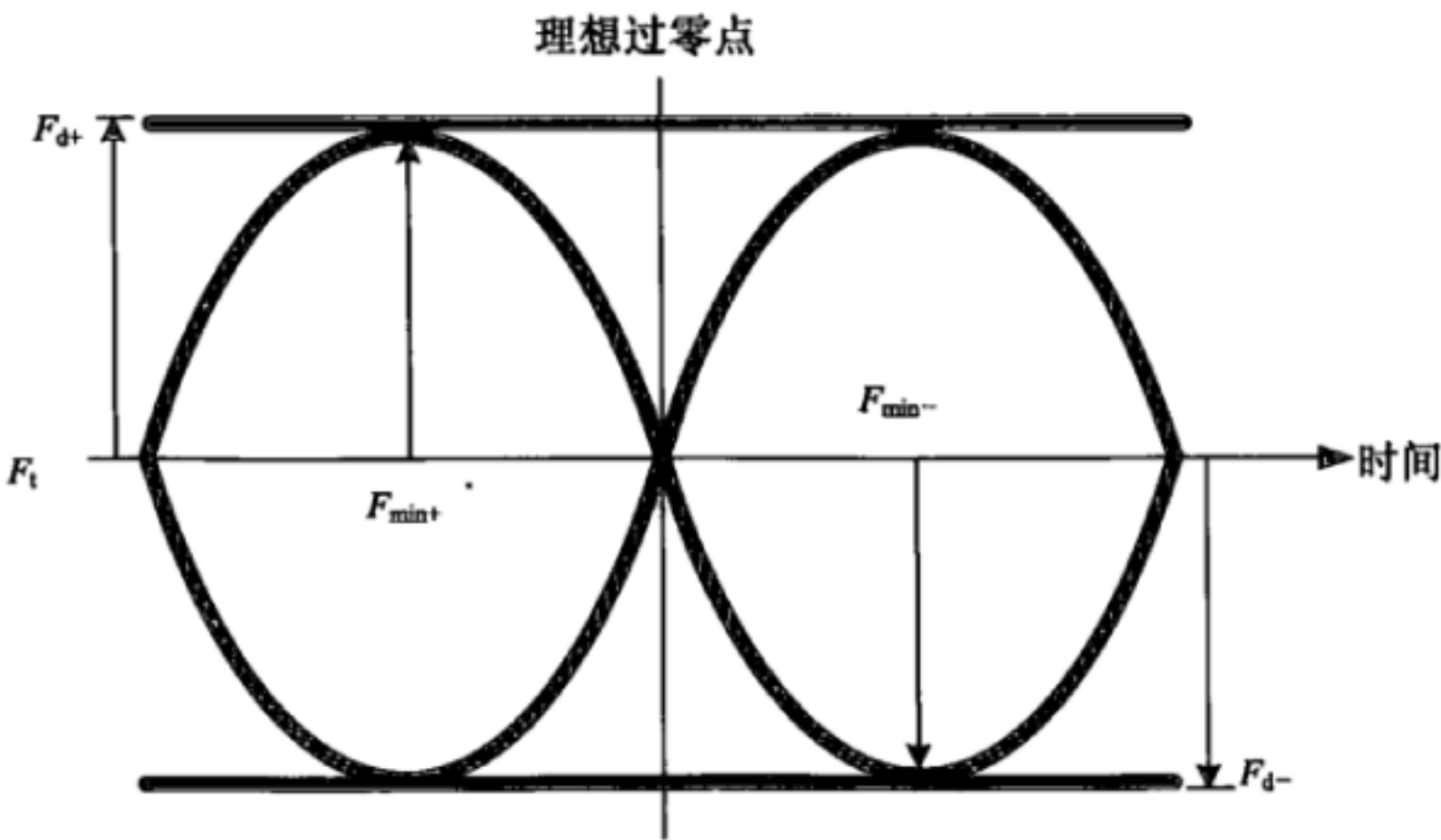


图8 GFSK 调制方式

6.2.2.4 杂散辐射

6.2.2.4.1 带内杂散

带内杂散功率应符合表2的最大限值要求，其中第 M 信道为射频信号发射信道，第 N 信道为相邻信道。

表2 发射频谱带内杂散

相邻信道间隔	杂散功率最大限值
2MHz($ M-N =2$)	-20dBm
≥ 3 MHz($ M-N \geq 3$)	-30dBm

6.2.2.4.2 带外杂散

带外杂散应符合表3的要求。

表3 发射频谱带外杂散

频率范围	测试带宽 (RBW)	限值 (绝对值)	检波方式
30MHz~1GHz	100kHz(3dB)	-36dBm	有效值
1GHz~12.75GHz	1MHz(3dB)	-30dBm	有效值

7 数据链路层

7.1 磁通道

磁通道数据链路层帧分为逻辑帧和物理帧，如图9所示。逻辑帧定义了磁通道数据的逻辑结构，通过对逻辑帧数据进行位填充，并增加同步码形成在磁通道上传输的物理帧。



图9 逻辑帧和物理帧的关系

7.1.1 物理帧

对逻辑帧进行位填充后得到物理帧，物理帧包括帧同步码和经过位填充的逻辑帧。

7.1.1.1 同步码

用于磁通道数据帧同步的位序列：字段长度为9比特；同步码的值为111111110b。

7.1.1.2 位填充码

从逻辑帧起始处开始向后检索，出现位流1111111b时，填充1位“0”形成11111110b。

7.1.1.3 物理帧帧间空闲

如果在磁通道上任意两个有效物理帧位流之间存在空闲时间间隔，则发起方必须发送全“1”比特流填充序列。

7.1.2 逻辑帧

7.1.2.1 MCF 帧结构

MCF采用变长编码格式，其帧结构包括控制域（包括帧类型、帧数据长度）、帧数据域和CRC校验，如图10所示。

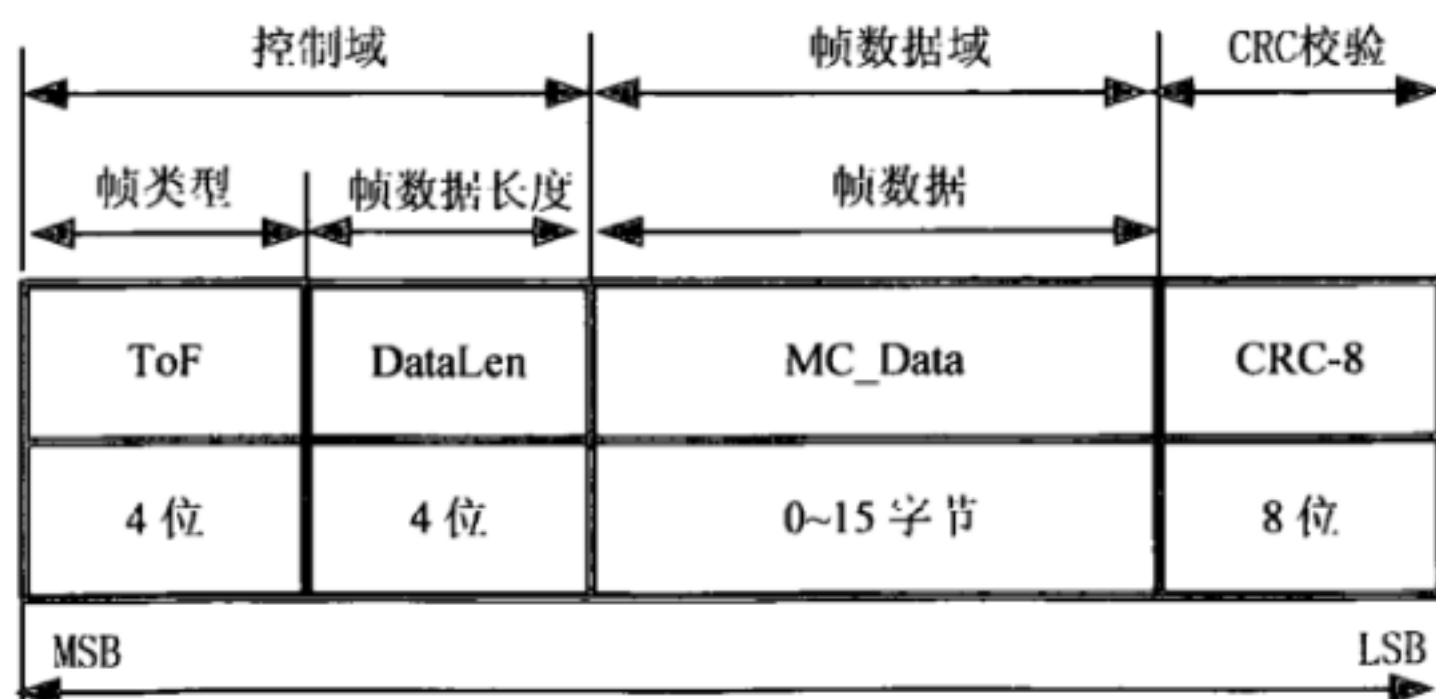


图10 MCF 帧格式

MCF帧控制域如表4所示。

表4 MCF 控制域

字段	长度 (位)	定义值	说明
ToF	4	0000b~1110b: 磁基本帧	帧类型, 用于标识不同类型的磁通道帧, 包括直接用于传输 MCM 的磁通道基本帧, 用于传输 MCMe 的磁通道扩展帧
		1111b: 磁扩展帧	
DataLen	4	0000b~1111b	帧数据域的字节长度

MCF帧数据域如表5所示。

表5 MCF 数据域

字段	长度 (字节)	定义值	说明
MC Data	由 DataLen 字段值定义	帧数据	MCF中传输的数据

MCF帧校验域如表6所示。

表6 MCF 校验域

字段	长度 (位)	定义值	说明
CRC-8	8	00h~FFh	<p>帧校验，表示MCF的8位CRC校验码。</p> <p>CRC-8计算方法如下：</p> <ul style="list-style-type: none"> — MCF帧的CRC-8计算包含了帧结构中的控制域和数据域； — 8位CRC校验的多项式是：$X^8 + X^2 + X + 1$； — 8位CRC校验初始值为：00h

7.2 射频通道

7.2.1 RF 帧结构

7.2.1.1 RCF 帧结构

RCF采用变长编码格式，其帧结构包括前导码、地址、控制域（包括数据长度、帧标识、应答标识）、数据域和CRC校验，如图11所示。

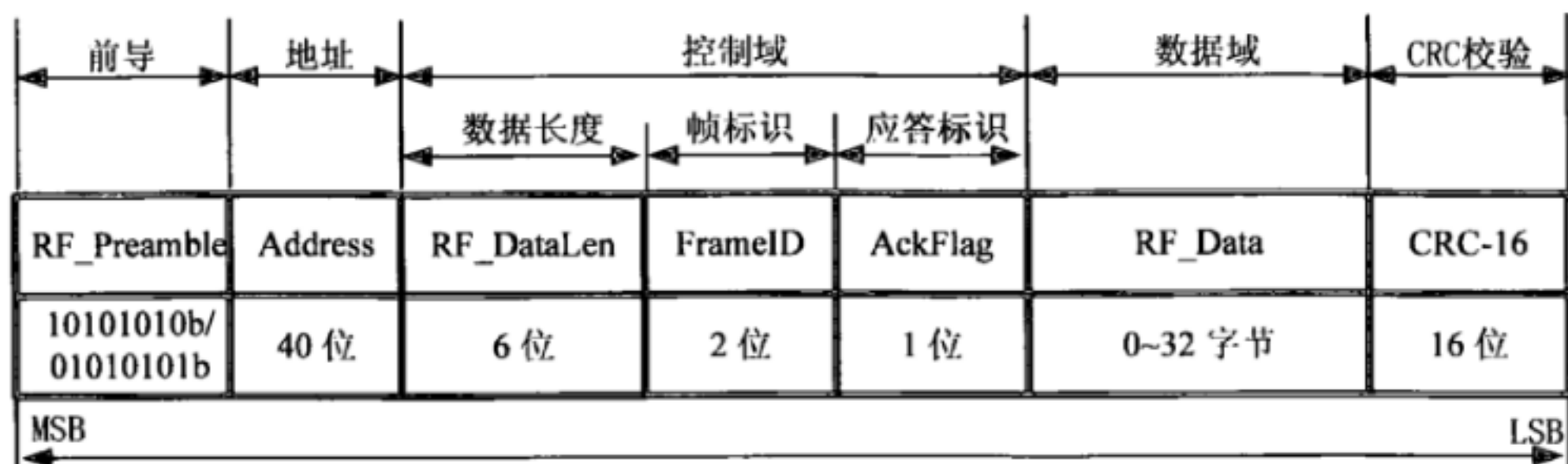


图11 RCF 编码格式

RCF前导域如表7所示。

表7 RCF 前导域

字段	长度（位）	定义值	说明
RF_Preamble	8	01010101b: 如果地址Address域最高位为0, 则RCF前导码为01010101b	前导码, 用于 RCF 同步
		10101010b: 如果地址Address域最高位为1, 则RCF前导码为10101010b	

RCF地址域如表8所示。

表8 RCF 地址域

字段	长度（位）	定义值	说明
Address	40	0000000000h~FFFFFFFFFh	用于RCF接收的识别地址

RCF控制域如表9所示。

表9 RCF 控制域

字段	长度（位）	定义值	说明
RF_DataLen	6	000000b~100000b	数据长度, 表示RCF数据（含RCF数据的包头字节）的字节长度。 RF_DataLen为0的帧仅限用于RF通道的ACK
FrameID	2	00b~11b	帧标识, 用于区分不同的RCF。相邻不同RCF的帧标识应当不同
AckFlag	1	0b: RCF的接收方不发送ACK	应答标识, 用于RCF的接收方判断是否应当发送ACK
		1b: RCF的接收方自动发送一个ACK	

RCF数据域如表10所示。

表10 RCF 数据域

字段	长度（字节）	定义值	说明
RF_Data	由 RF_DataLen 字段值定义	帧数据	表示在RCF中传输的数据

RCF帧校验域如表11所示。

表11 RCF 校验域

字段	长度（位）	定义值	说明
CRC-16	16	0000h~FFFFh	帧校验表示RCF的16位CRC校验码。 CRC-16计算方法定义如下： — MCF 帧的 CRC-16 计算包含了 RCF 结构中除前导 RF_Preamble 和 CRC-16 本身之外所有的域。 — 16 位 CRC 校验的多项式是： $X^{16} + X^{12} + X^5 + 1$ 。 — 16 位 CRC 校验初始值为：FFFFh

7.2.2 帧类型

7.2.2.1 数据帧

按RCF帧结构编码, 其中AckFlag为1, 表示需要RCF的接收方自动发送一个ACK。

7.2.2.2 应答帧

按RCF帧结构编码, 其中RF_DataLen为0, AckFlag为0, 无RF_Data。

7.2.3 组帧与解帧

7.2.3.1 组帧

RCF组帧过程如图12所示。按照规定的帧结构将数据组织在一起形成一个帧，并经过物理层处理后形成射频信号，然后进行发送。帧的发送顺序为最先发送前导域，最后发送CRC校验域。

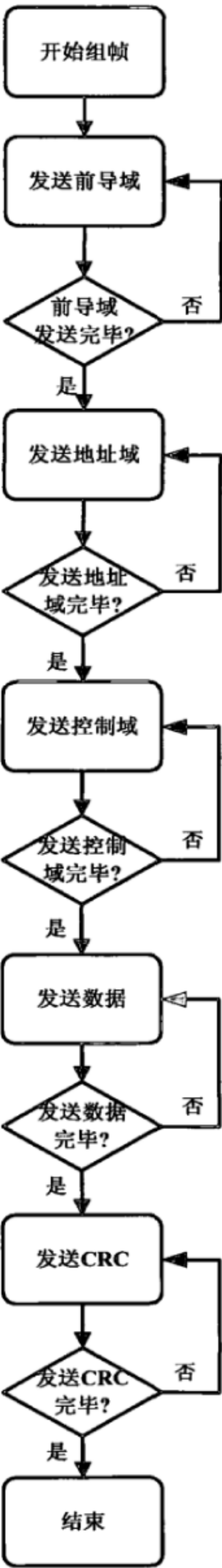


图12 组帧过程

7.2.3.2 解帧

RCF解帧过程如图13所示。将物理层接收到的射频信号解调成数字单比特信号后，按照帧结构进行解析，解出有效的帧数据。



图13 解帧过程

7.2.4 帧的收发

7.2.4.1 帧收发时序图

射频帧的收发处理时序如图14所示。

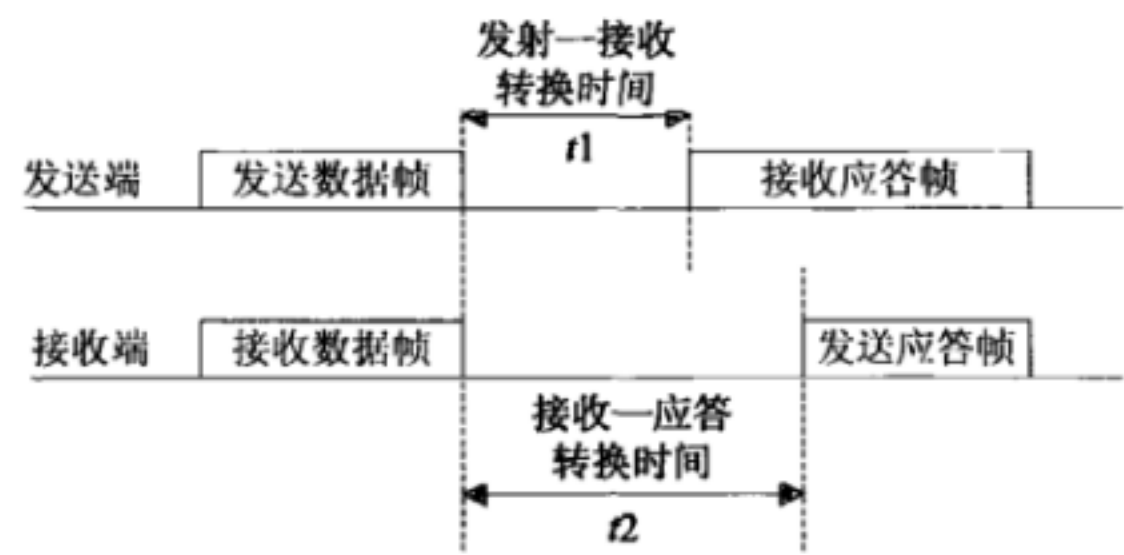


图14 射频帧收发处理时序

7.2.4.2 发射—接收转换时间

发送方在完成数据帧发送后，必须在 $t1$ 时间内切换到应答帧接收状态 ($t1 \leq 130\mu s$)。

7.2.4.3 接收—应答转换时间

接收方在收到一个数据帧后，必须在 $t2$ 时间内发送一个应答帧进行响应 ($130\mu s < t2 < 150\mu s$)。

7.2.4.4 帧传输

帧的传输过程包括一个数据帧发送和一个应答帧接收。发送方发送一个数据帧，并在 $t1$ 时间内切换到应答帧接收状态，如果成功接收到应答帧，则判断一次帧传输成功。如果未接收到应答帧则判断帧传输失败。帧的发送处理过程如图15所示。

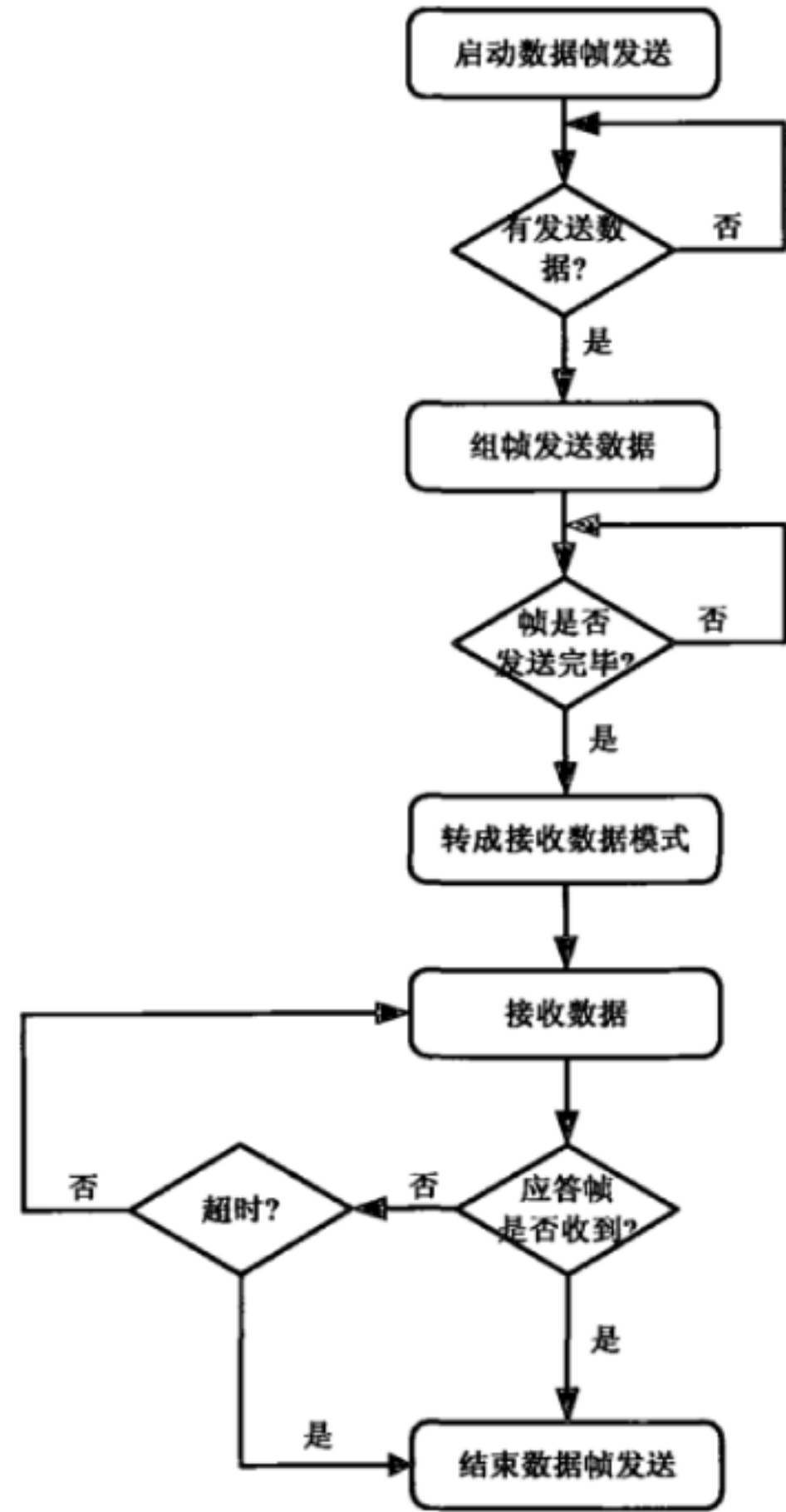


图15 帧的发送处理

接收方在收到相同的数据帧后，应当丢弃并继续接收。帧的接收处理过程如图16所示。

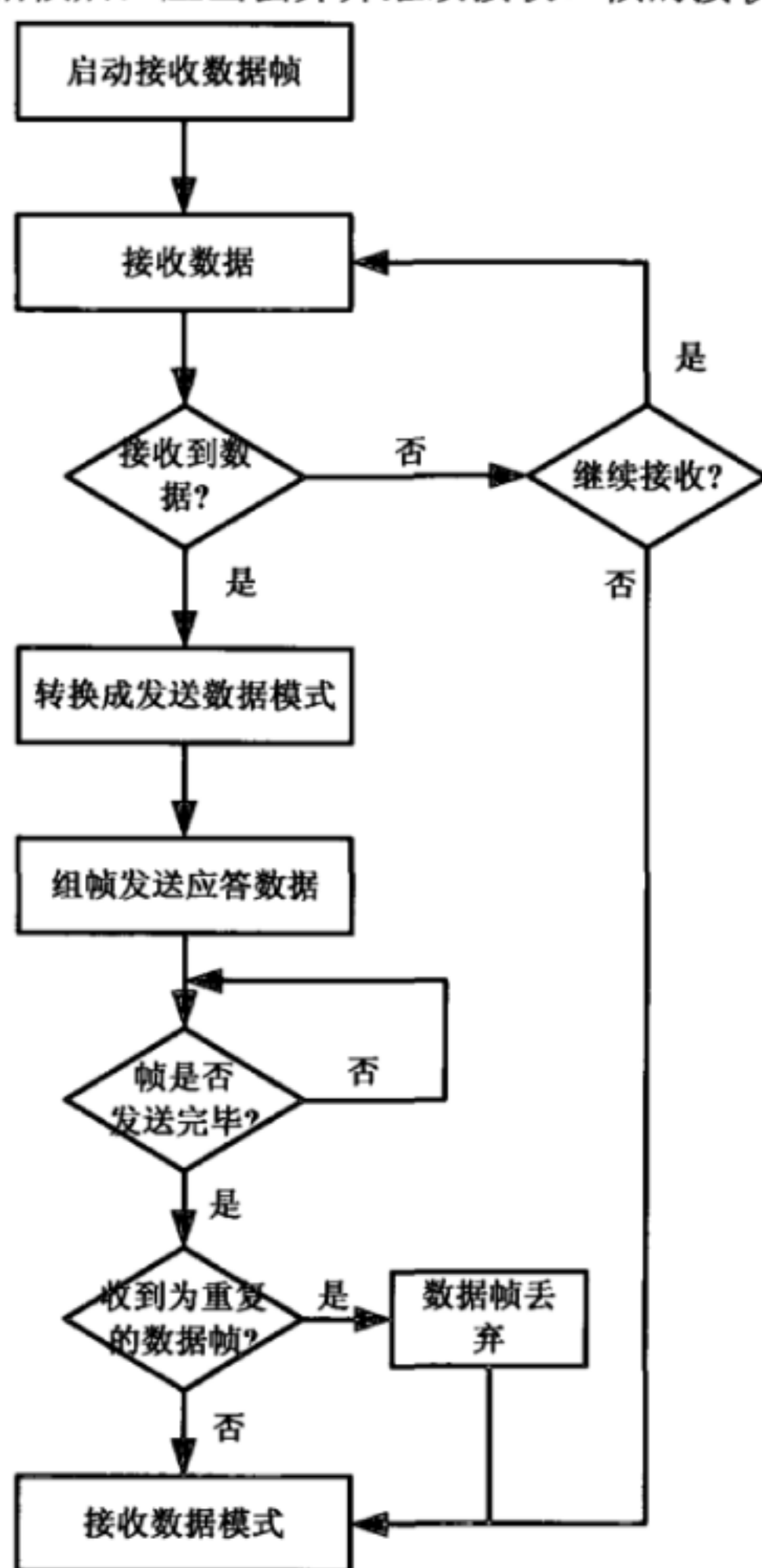


图16 帧的接收处理

8 传输层

8.1 包格式

8.1.1 磁通道 MCP 格式

MCP采用变长编码格式，包括MCP头和MCP数据两个部分，如图17所示。

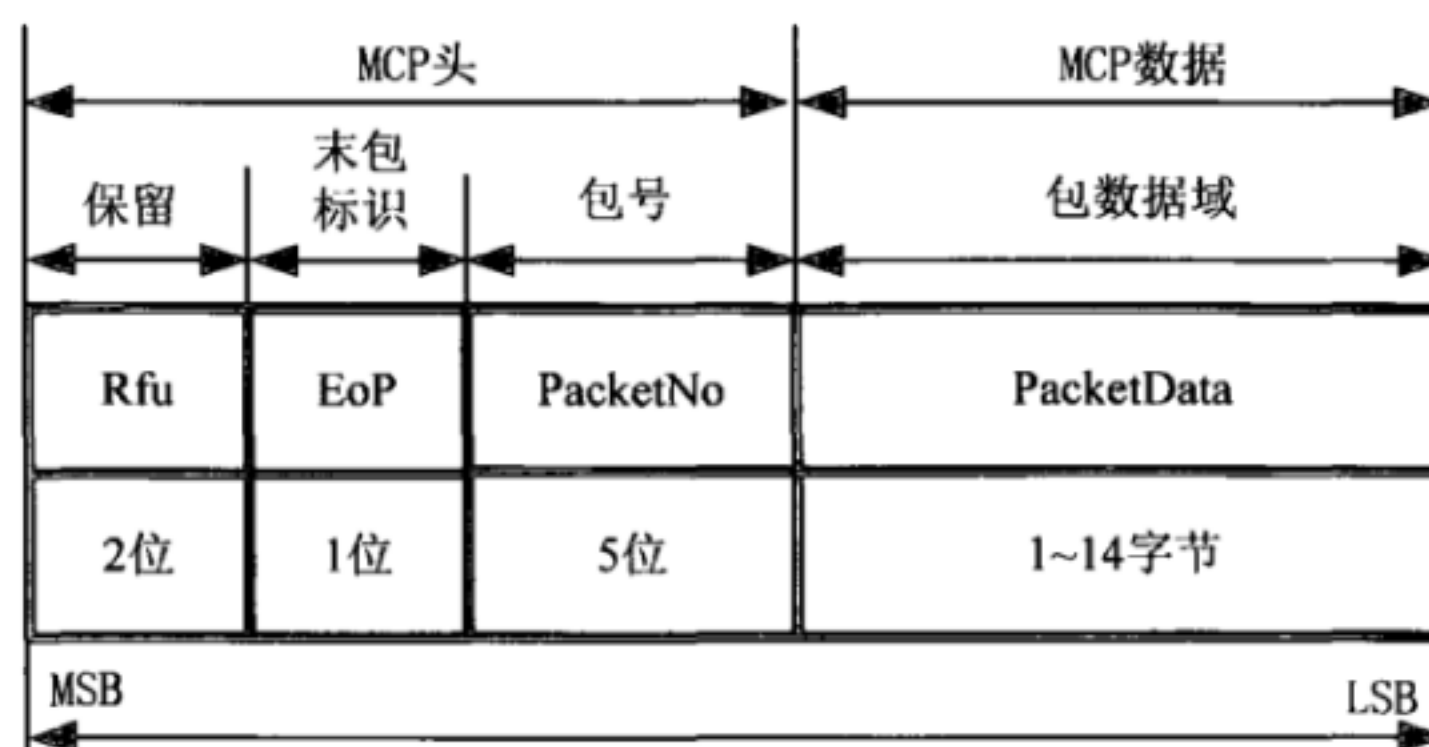


图17 MCP 编码格式

MCP头如表12所示。

表12 MCP 头

字段	长度（位）	定义值	说明
Rfu	2	00b	保留，缺省为“0” 0b
EoP	1	0b: 非最末包	末包标识，用于区分本 MCP 是否为最后一个包
		1b: 最末包	
PacketNo	5	00000b: 为第1个包	包号，表示 MCP 包序列的顺序编号，最多支持 32 个包
		00001b: 为第2个包	
		00010b: 为第3个包	
		
		11111b: 为第32个包	

MCP数据域如表13所示。

表13 MCP 数据域

字段	长度（字节）	定义值	说明
Packet_Data	1 ~ 14	包数据	MCP包的有效数据

8.1.2 射频通道 RCP 格式

RCP采用变长编码格式，包括RCP头和RCP数据两个部分，如图18所示。

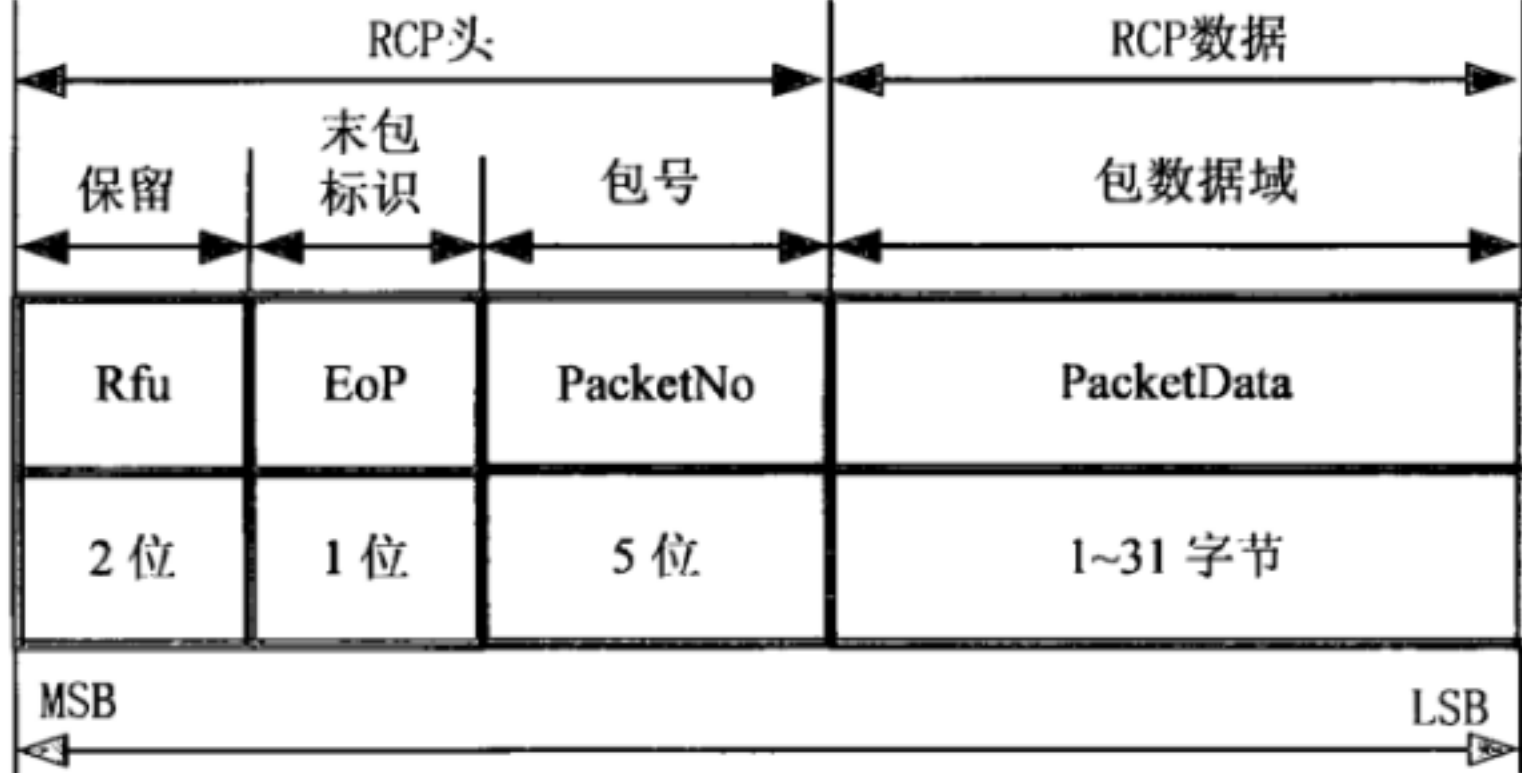


图18 RCP 编码格式

RCP头如表14所示。

表14 RCP 头

字段	长度（位）	定义值	说明
Rfu	2	00b	保留，缺省为“0” 0b
EoP	1	0b: 非最末包	末包标识，用于区分本 RCP 是否为最后一个包
		1b: 最末包	
PacketNo	5	00000b: 为第1个包	包号，表示 RCP 包序列的顺序编号，最多支持 32 个包
		00001b: 为第2个包	
		00010b: 为第3个包	
		
		11111b: 为第32个包	

RCP数据域如表15所示。

表15 RCP 数据域

字段	长度(字节)	定义值	说明
Packet_Data	1~31	包数据	RCP包的有效数据

8.2 包传输

采用顺序分包方式传递一个MCMe消息或RCM消息。

首包序号为0, 发送方从首包开始按包序号递增顺序逐包发送, 接收方收到数据包后按顺序重新组合成一个完整的消息。

消息分包方式如图19所示。



图19 协议消息的分包方式

包的发送处理过程如图20所示。

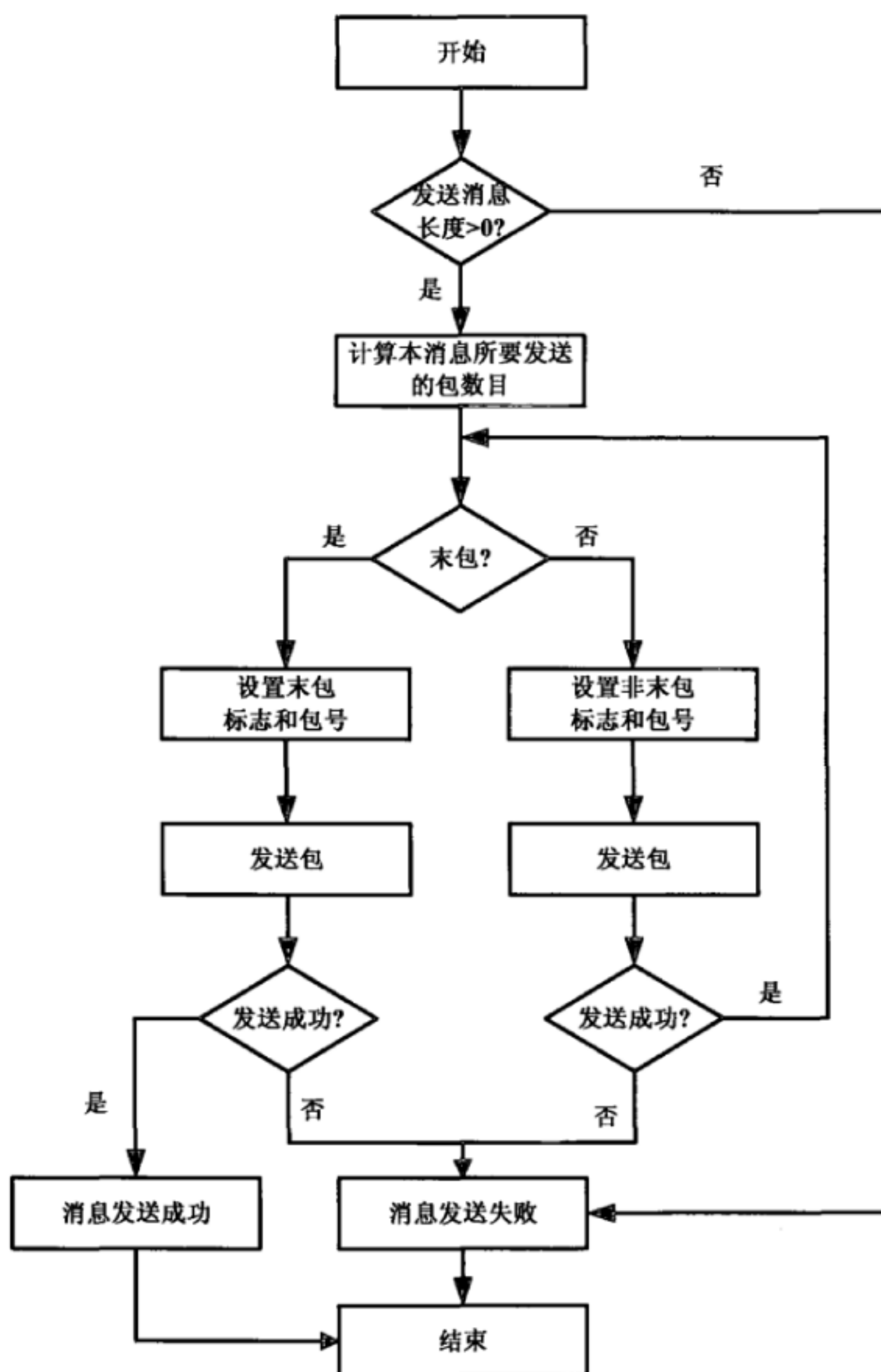


图20 包的发送处理

接收方收到数据包后按顺序重新组合成一个完整的消息。
接收方收到的RCP包与当前已收到的RCP包的包号相同时，应当丢弃并继续接收。
包的接收处理过程如图21所示。

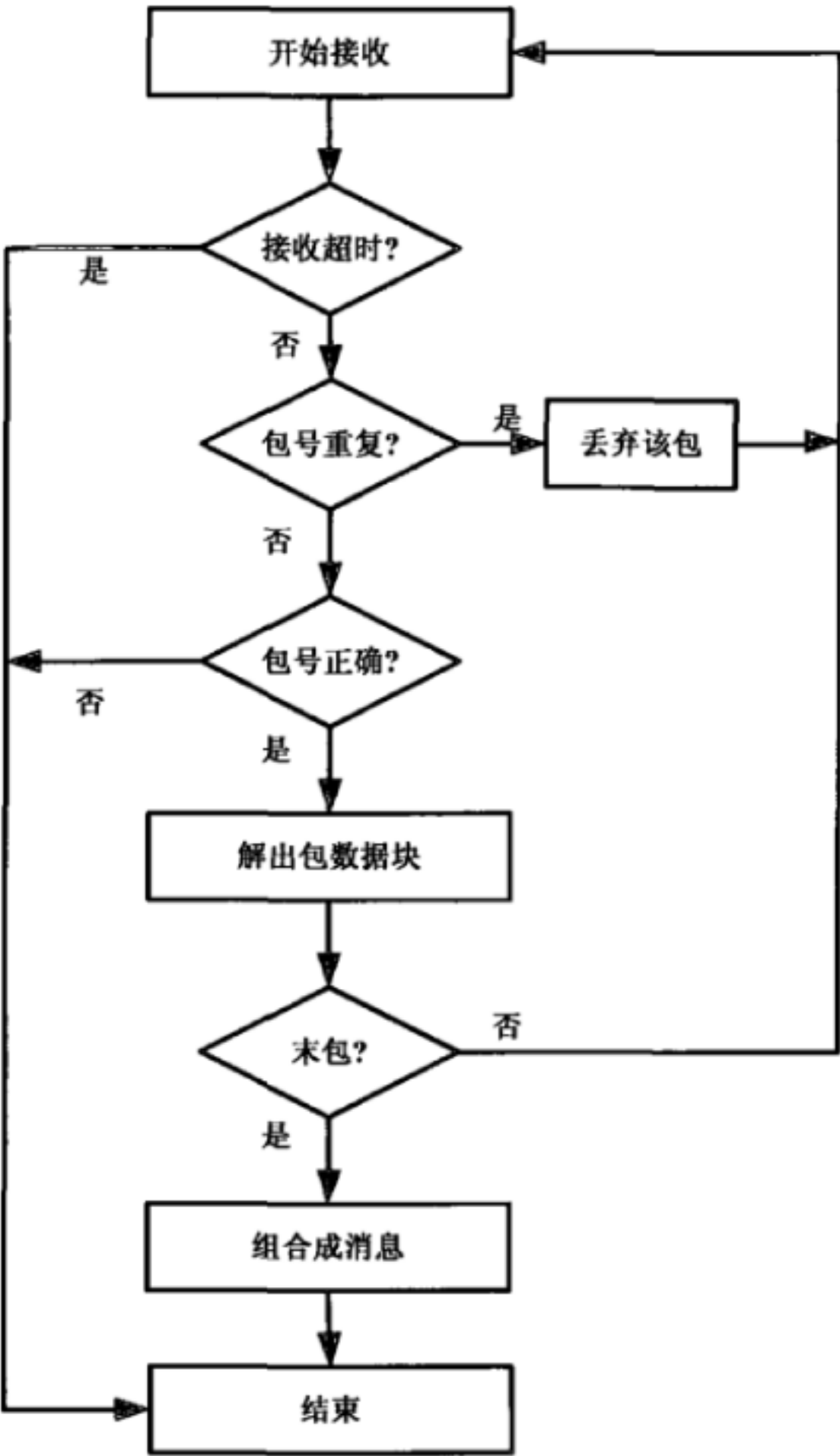


图21 包的接收处理

9 会话层

9.1 消息

9.1.1 短消息格式

短消息格式（SMF）用于传输MCM消息。SMF格式如图22所示。

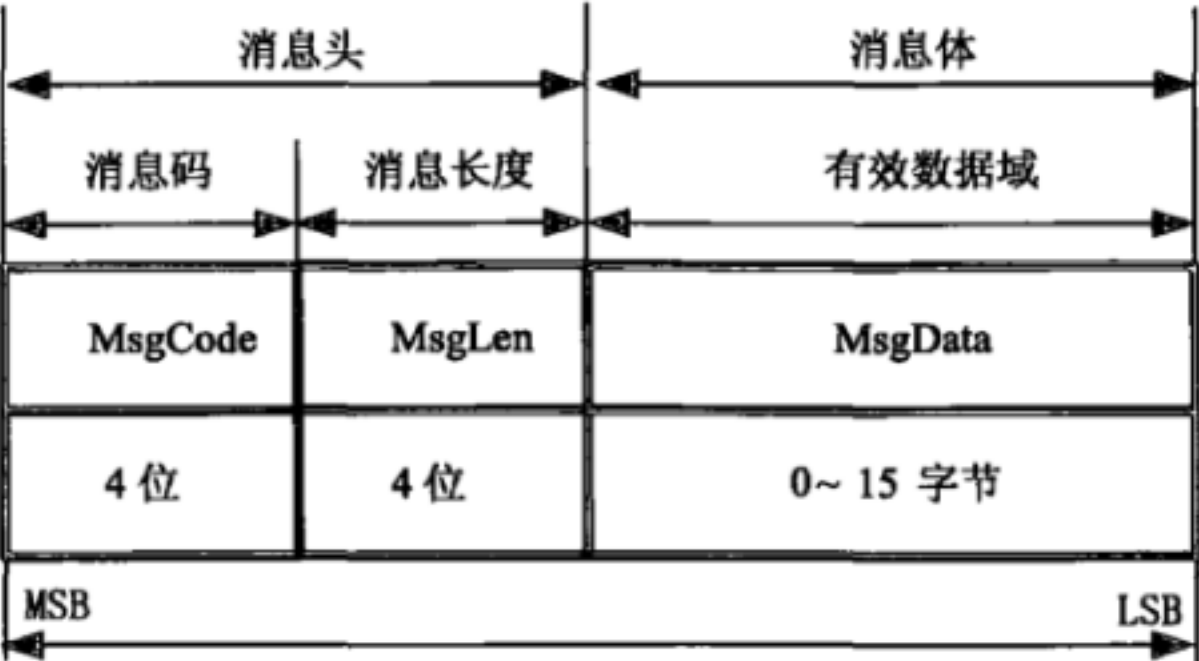


图22 SMF 格式

SMF消息头如表16所示。

表16 SMF 消息头

字段	长度 (位)	定义值	说明
MsgCode	4	0000b~1111b	消息码, 用于标识一个短格式消息
MsgLen	4	0000b~1111b	消息长度, 表示消息体的字节长度

SMF消息体如表17所示。

表17 SMF 消息体

字段	长度 (字节)	定义值	说明
MsgData	由 MsgLen 字段值定义	消息数据	用于承载消息所要传递的有效数据

9.1.2 长消息格式

长消息格式（LMF）用于传输RCM消息和MCMe消息。LMF格式如图23所示。

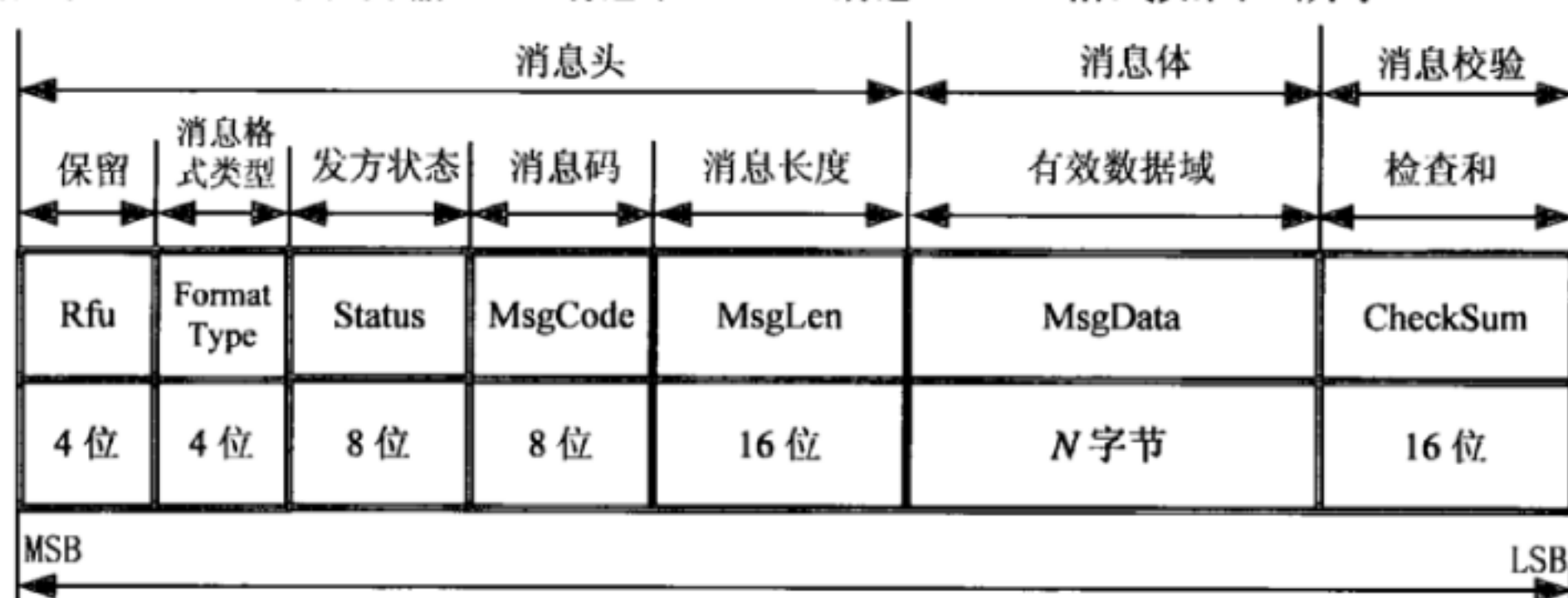


图23 LMF 格式

LMF消息头如表18所示。

表18 LMF 消息头

字段	长度 (位)	定义值	说明
Rfu	4	0000b	保留位, 缺省为“0”000b
FormatType	4	000b~0111b: 私有格式	表示消息的编码格式类型
		1000b: 本编码格式	
		1001b~1111b: 保留	
Status	8	00h: 正常	发送方状态, 表示消息发送方的当前状态
		01h: 连接异常	
		02h: 响应方在 RF 发送时移出允许的交易距离范围	
		82h: 响应方在 RF 接收时移出允许的交易距离范围	
		D0h~FFh: 自定义状态	
		其他: 保留	
MsgCode	8	10h~FFh	消息码, 用于标识一个长格式消息
MsgLen	16	0~288	表示消息体的字节长度 (不包含消息校验字节)

LMF消息体如表19所示。

表19 LMF 消息体

字段	长度（字节）	定义值	说明
MsgData	由 MsgLen 字段值定义	消息数据	用于承载消息所要传递的有效数据

LMF消息校验如表20所示。

表20 LMF 消息校验

字段	长度（字节）	定义值	说明
Checksum	2	消息校验和	用于对消息头和消息体数据进行 CheckSum校验

9.1.3 消息码定义

本标准定义的消息码如表21所示。

表21 消息码定义

序号	消息	说明	消息码	备注
MC消息				
1	INQUIRY	激活请求消息	0	
2			1	保留
3	CHECK1_REQ	冲突检测请求消息	2	
4	CHECK2_REQ	连接确认请求消息	3	
5			4-11	保留
6			12-14	自定义
7			15	MC扩展消息
RF消息				
1	ATI	激活响应消息	16	
2	CONNECT_REQ	连接请求消息	17	
3	CONNECT_RSP	连接响应消息	18	
4	APDATA_REQ	数据交换请求消息	19	
5	APDATA_RSP	数据交换响应消息	20	
6			21	保留
7	LINKCTL_REQ	维持连接请求消息	22	
8	LINKCTL_RSP	维持连接响应消息	23	
9	CHECK_RSP	冲突检测响应消息	24	
10	LTW	响应方要求等待消息	25	
11	CLOSE_REQ	关闭连接请求消息	26	
12	CLOSE_RSP	关闭连接响应消息	27	
13			28~239	保留
14			240~255	自定义

9.2 协议会话流程

9.2.1 会话流程图

发起方与响应方之间的基本通信会话流程如图24所示。

发起方在连接和交易过程中必须维持磁场存在，响应方在发送任何响应之前，必须确定其处于设定的磁场强度范围内。

会话层消息的发送方在消息发送完成后应当立即转换为消息接收状态，并按照会话命令规定的时间内进行接收。

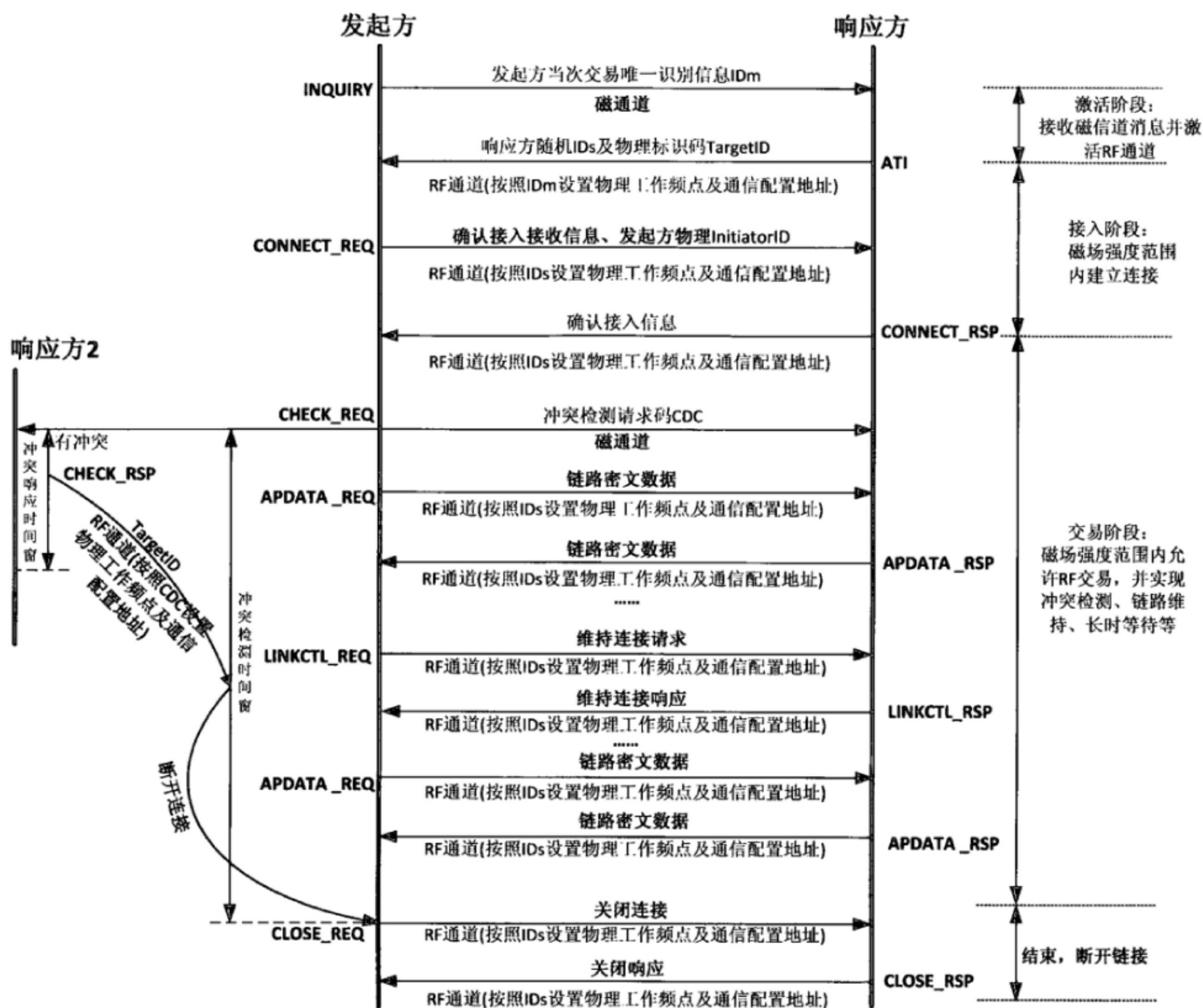


图24 基本会话流程

协议会话的工作流程通常包括激活、接入、交易和结束四个阶段。

9.2.2 激活阶段

9.2.2.1 激活

—— 发起方操作

- 发起方在激活阶段通过磁通道发送 INQUIRY，然后通过 RF 通道接收 ATI。
- 发起方在发送 INQUIRY 之前，根据自己生成的 IDm 计算激活响应 (ATI) 频点并确认该频点是否可用，如果该频点当前已被占用，则需要重新生成 IDm 直到选择的 ATI 频点空闲为止。
- 发起方如果接收到错误的 ATI、或者 ATI 中的 Mac 验证失败、或者接收超时 ($>8\text{ms}$)，则发送新的 INQUIRY。

① 发起方在接收到第一个正确的 ATI 之后进入接入阶段。

—— 响应方操作

- 响应方在激活阶段通过磁通道接收 INQUIRY，然后通过 RF 通道发送 ATI。
- 响应方如果接收到错误的 INQUIRY 或者未接收到 INQUIRY，则继续接收 INQUIRY。
- 响应方在接收到第一个正确的 INQUIRY 之后被激活，然后在 8ms 内通过 RF 通道做出 ATI 响应。

- 响应方在发送 ATI 之前, 根据自己生成的 IDs 计算后续接入/交易频点并确认该频点是否可用, 如果该频点当前已被占用, 则需要重新生成 IDs 直到选择的接入/交易频点空闲为止。
- 响应方在发送完 ATI 之后进入接入阶段。

—— 处理流程

激活阶段处理流程如图25所示。

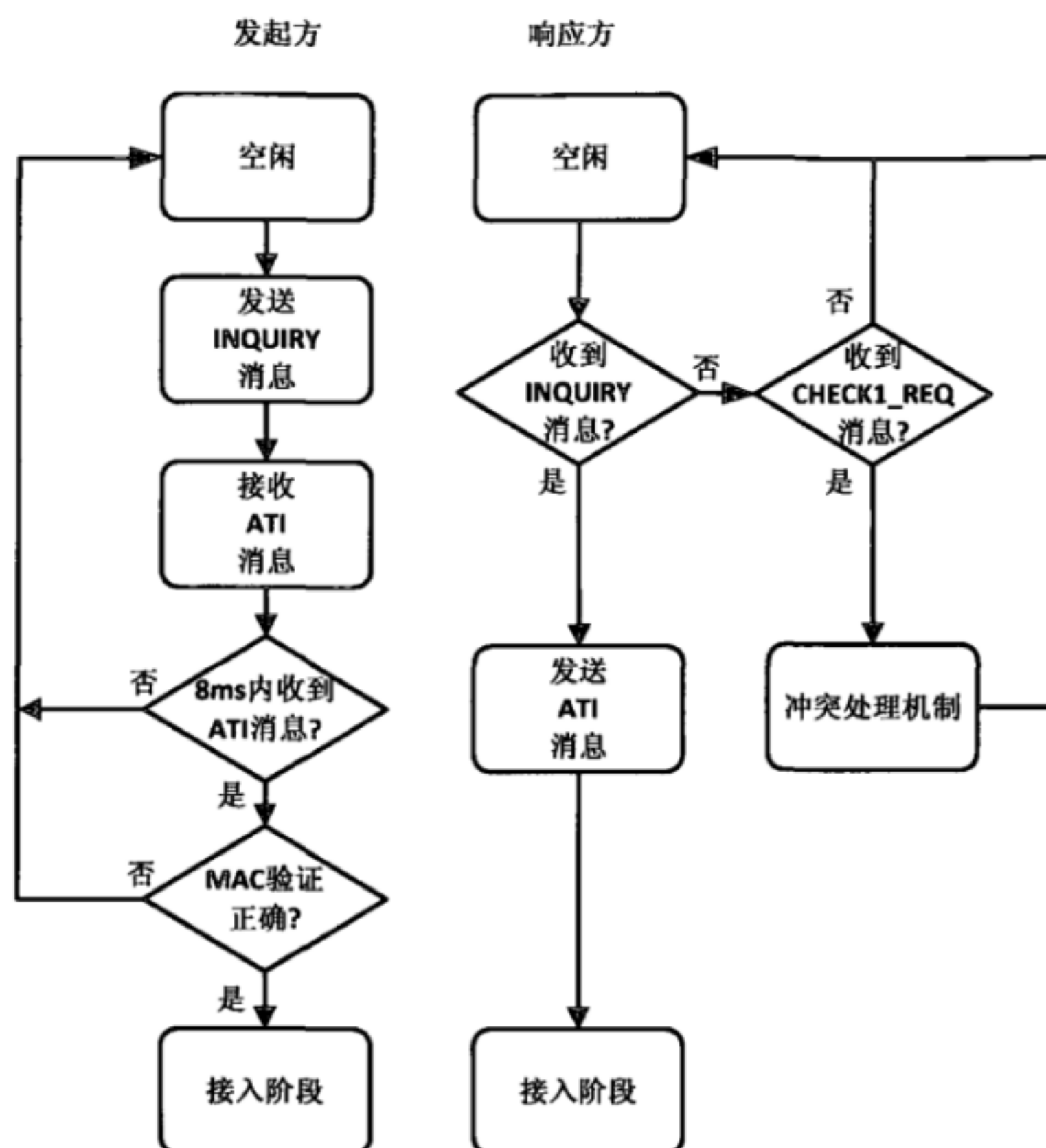


图25 激活阶段处理流程

9.2.3 接入阶段

9.2.3.1 建立连接

—— 发起方操作

● 发起方在接入阶段通过 RF 通道发出 CONNECT_REQ 连接请求, 然后通过 RF 通道接收 CONNECT_RSP 响应。

- 发起方如果接收到错误的 CONNECT_RSP 或者接收超时 ($>8\text{ms}$), 则返回激活阶段。

- 发起方在接收到第一个正确的 CONNECT_RSP 之后进入交易阶段。

—— 响应方操作

● 响应方在接入阶段通过 RF 通道接收 CONNECT_REQ, 然后通过 RF 通道发送 CONNECT_RSP 进行响应。

- 响应方如果接收到错误的 CONNECT_REQ 或者接收超时 ($>8\text{ms}$), 则返回到激活阶段。

- 响应方在发送完 CONNECT_RSP 之后进入交易阶段。

—— 处理流程

接入阶段处理流程如图 26 所示。

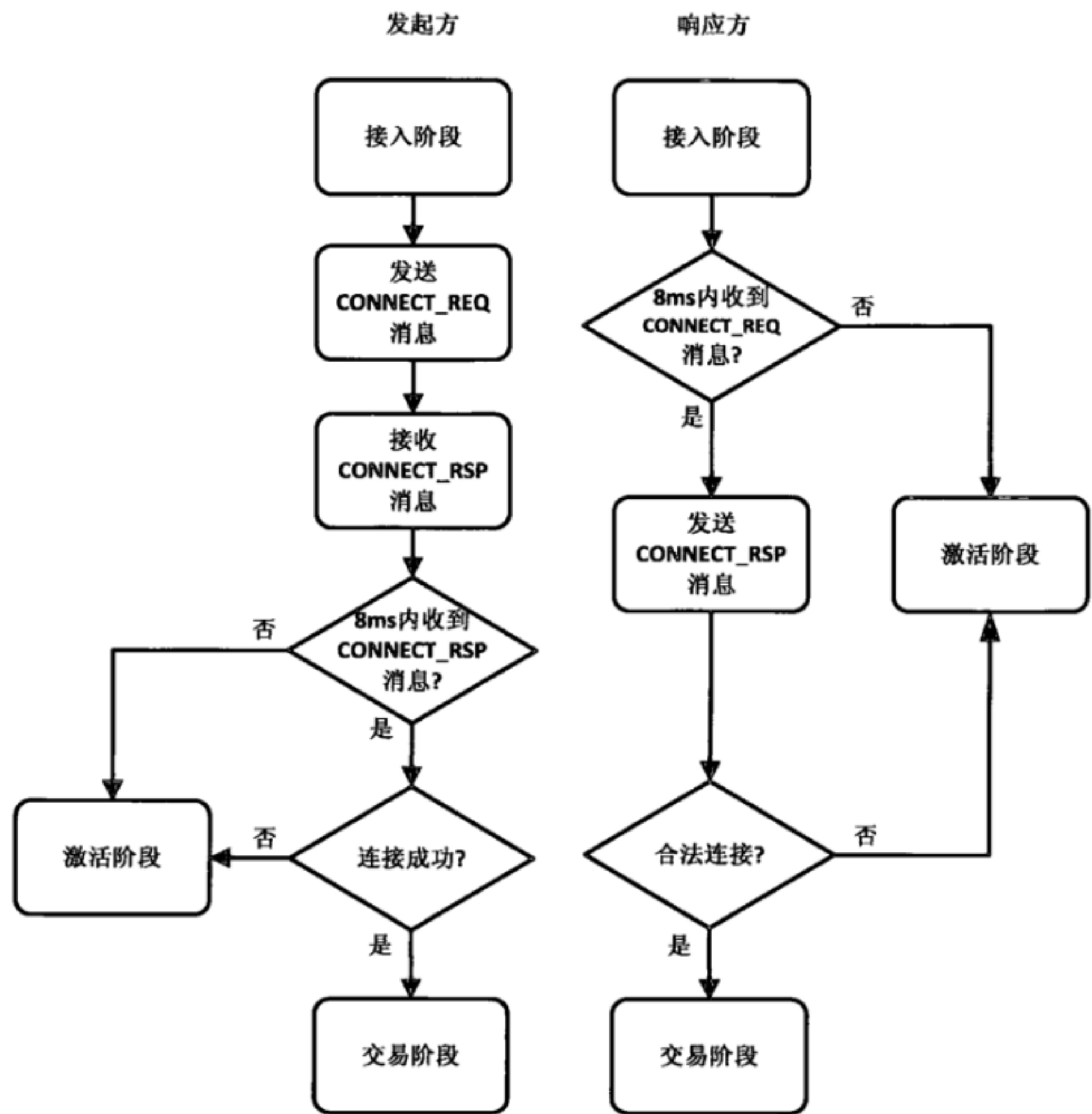


图26 接入阶段处理流程

9.2.4 交易阶段

本阶段完成的操作包括：数据交换、链路维持、冲突检测和长时等待。

9.2.4.1 数据交换

—— 发起方操作

- 发起方在交易阶段通过 RF 通道发送 APDATA_REQ 数据交换请求，然后通过 RF 通道接收 APDATA_RSP 响应或者 LTW 长时等待消息。
- 发起方如果接收到错误的 APDATA_RSP/LTW 或者接收超时（>500ms），则返回激活阶段。
- 发起方如果接收到正确的 APDATA_RSP/LTW，则继续维持交易阶段。

—— 响应方操作

- 响应方在交易阶段等待接收 APDATA_REQ，解析和执行封装在 APDATA_REQ 中的 APDU 命令，然后把对 APDU 命令的响应封装在 APDATA_RSP 中发送给发起方。
- 响应方如果接收到错误的 APDATA_REQ 或者接收超时（>100ms），则返回激活阶段。
- 响应方应该在 500ms 内发送 APDATA_RSP，或者 LTW 长时等待消息给发起方。
- 响应方在发送完 APDATA_RSP 或 LTW 后，继续维持交易阶段。

—— 处理流程

数据交换处理流程如图 27 所示。

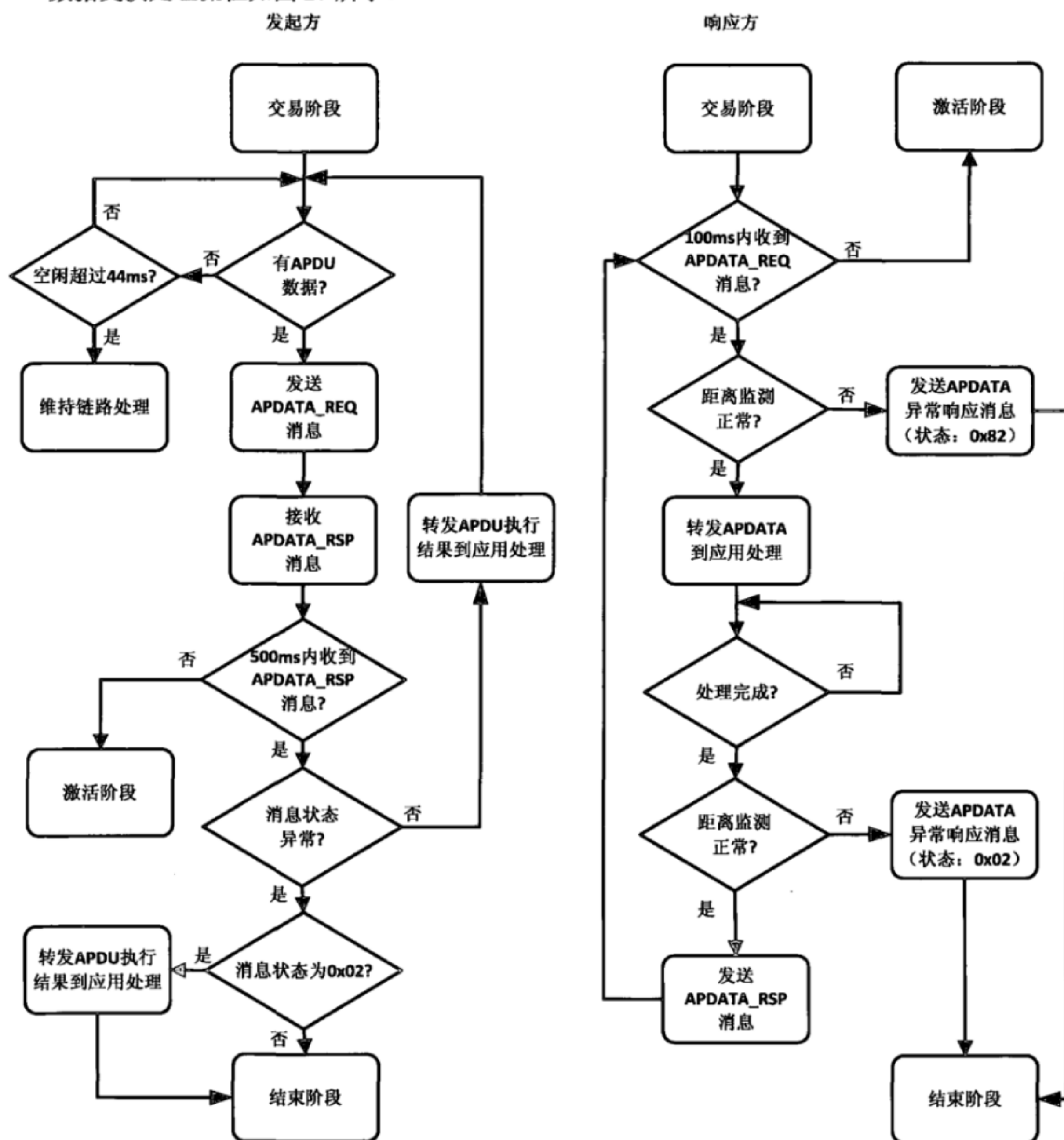


图27 数据交换处理流程

9.2.4.2 链路维持

—— 发起方操作

• 发起方在交易阶段的空闲时间里应当每隔 44ms 通过 RF 通道发送 LINKCTL_REQ, 然后通过 RF 通道接收 LINKCTL_RSP 以维持连接。

• 发起方在发送 LINKCTL_REQ 后, 如果在 8ms 内接收到正确的 LINKCTL_RSP 响应且响应方状态正常, 则继续维持与响应方的连接; 如果发起方连续 10 次在发送 LINKCTL_REQ 后均无法正确收到 LINKCTL_RSP 响应则认为响应方已断开连接, 发起方返回激活阶段。

—— 响应方操作

- 响应方在交易阶段如果接收到正确的 LINKCTL_REQ 命令请求, 并确认磁通道收到 CHECK1_REQ 或者 CHECK2_REQ 消息, 且 CDC 或者 TRI 正确无误, 则应当在 8ms 内发送 LINKCTL_RSP 做出响应。
- 响应方在交易阶段如果连续三次在接收到正确的 LINKCTL_REQ 命令请求后, 都没有从磁通道收到 CHECK1_REQ 或者 CHECK2_REQ 消息, 则应当先更新响应方连接状态为异常, 并在 8ms 内发送 LINKCTL_RSP, 做出响应。
- 响应方如果接收到错误的 LINKCTL_REQ, 或者超过 100ms 仍未接收到任何命令, 则响应方返回激活阶段。

—— 处理流程

链路维持处理流程如图28所示。

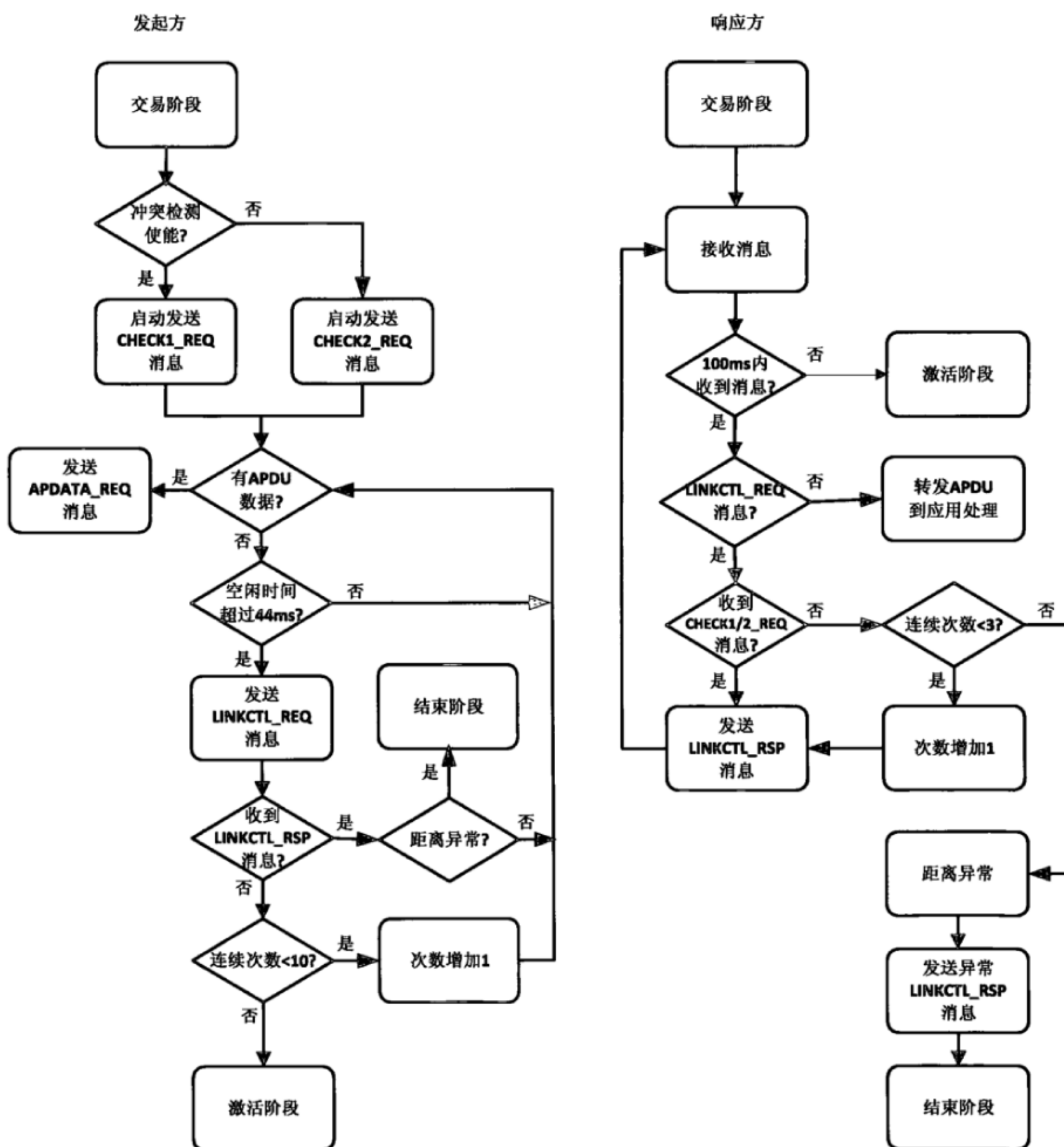


图28 链路维持处理流程

9.2.4.3 冲突检测

当发起方检测到MTC冲突发生时,发起方不能进行任意一个响应接入,且应结束与当前响应方的连接。MTC冲突如图29所示。

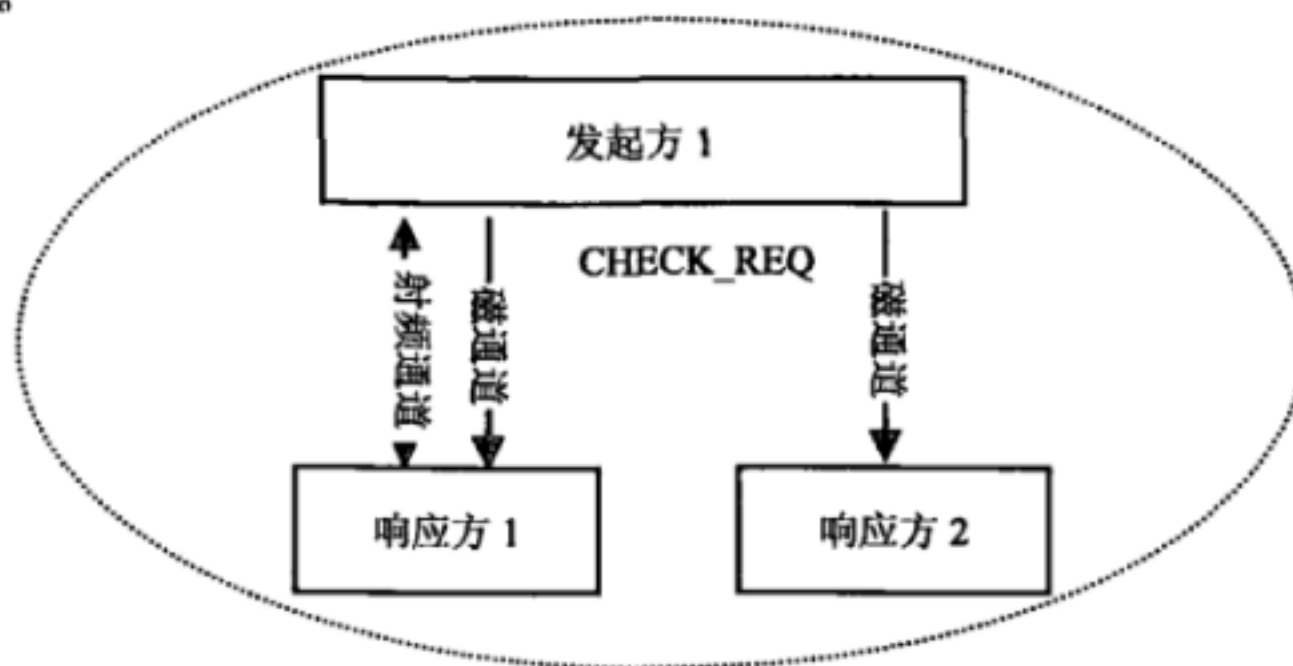


图29 MTC 冲突

—— 发起方操作

- 发起方可以通过外部配置确定是否支持 MTC 冲突检测。
- 支持冲突检测的发起方在建立连接后的整个交易阶段通过磁通道持续发送 CHECK1_REQ 消息。
- 发起方建立连接后,在射频通道空闲期间(没有维持连接和 APDU 收发任务时)以 $t_2(t_2 \geq 4\text{ms})$ 为一个最小接收时间单元,持续于冲突响应信道上接收 CHECK_RSP 消息。
- 发起方如果接收到 CHECK_RSP,并且其中 TargetID 字段与当前连接的响应方 TargetID 不相符,则认为发生了 MTC 冲突。
- 当发起方检测到 MTC 冲突后,应当立即发送 CLOSE_REQ 指令,结束与当前响应方的连接。

—— 响应方操作

- 响应方在未连接状态下通过磁通道接收到 CHECK1_REQ 消息则认为发生了 MTC 冲突。
- 响应方两次收到 CHECK1_REQ 消息的最大时间间隔定义为一个冲突响应时间窗 T ,本标准中 $T=22\text{ms}$ 。
- 响应方检测到 MTC 冲突后,在冲突响应时间窗中,以 t_1 为冲突响应时间间隔(t_1 最大为 4ms)。 t_1 被划分为 1 个或多个响应时隙(每个时隙 $400\mu\text{s}$)。冲突响应方在 t_1 时间内随机选择一个时隙发送冲突响应消息。冲突检测处理时序如图 30 所示。
- 冲突响应消息发送频点和地址由 CHECK1_REQ 消息中的 CDC 字段决定。

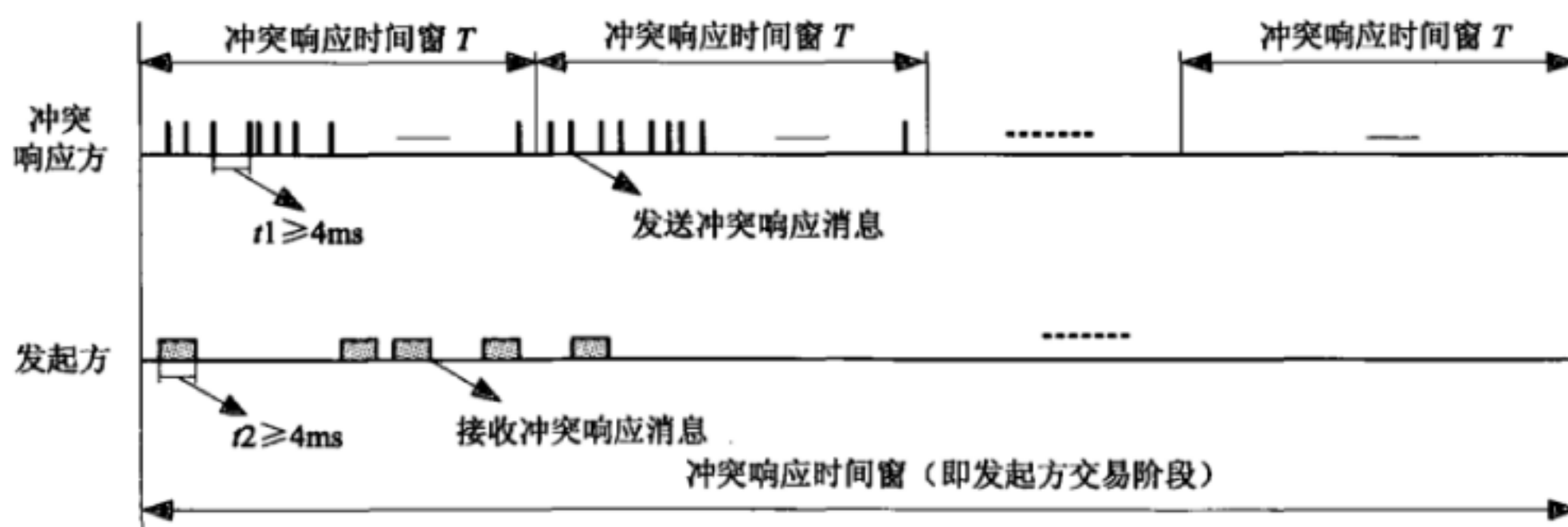


图30 冲突检测处理时序

—— 处理流程

冲突检测处理流程如图31所示。

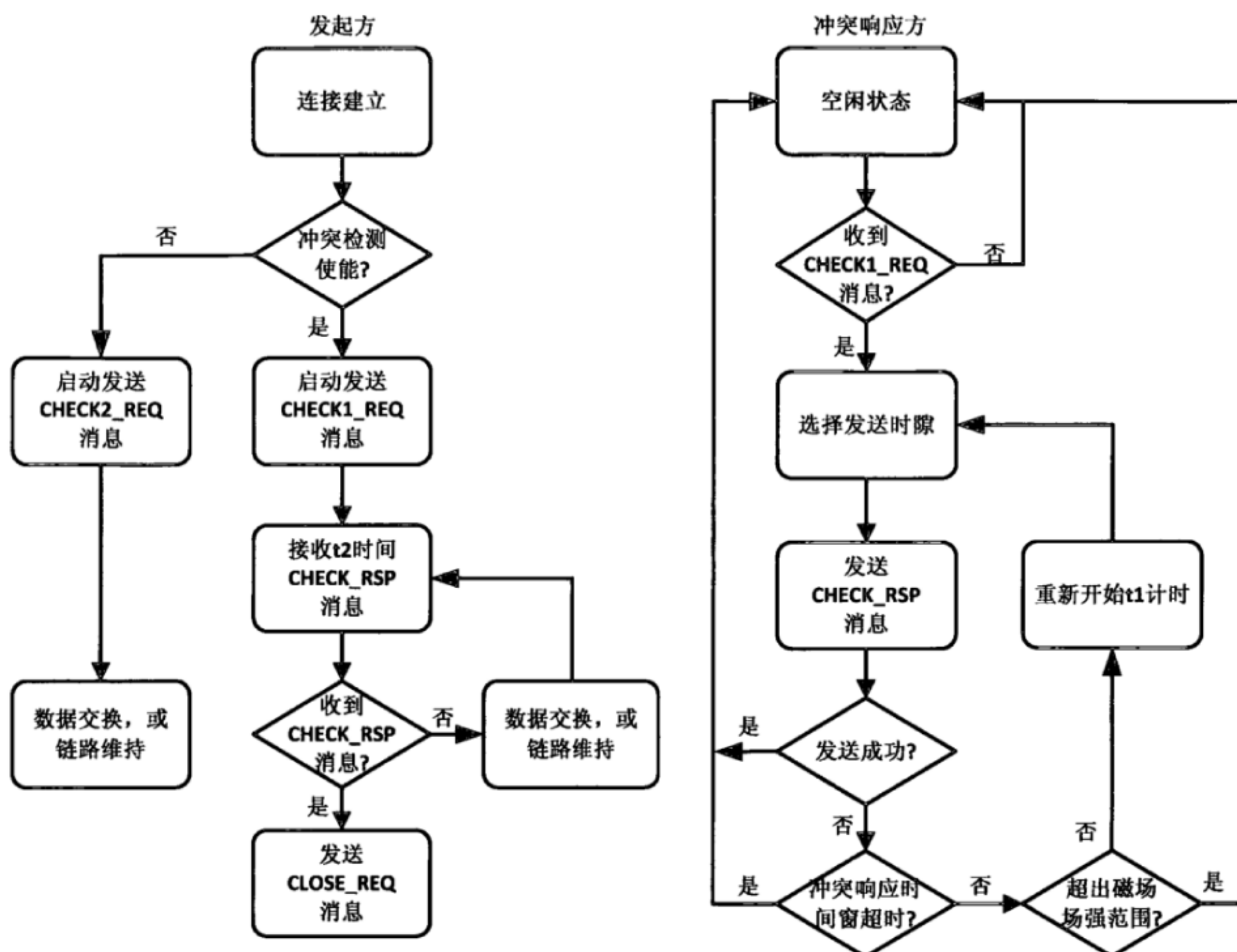


图31 冲突检测处理流程

9.2.4.4 连接确认

—— 发起方操作

• 如果冲突配置项为关闭，则发起方在整个交易阶段通过磁通道发送 CHECK2_REQ 连接确认请求。

—— 响应方操作

• 如果响应方在交易阶段通过磁通道接收到 CHECK2_REQ 连接确认请求，则根据 TRI 是否正确，相应地更新响应方的当前连接状态。该状态信息将在响应方下一条 RF 响应消息中返回给发起方。

9.2.4.5 长时等待

—— 发起方操作

• 发起方在交易阶段等待响应方的 APDATA_RSP 命令响应期间，如果接收到来自响应方的正确的 LTW，则继续等待 500ms，直到接收到 APDATA_RSP 或下一个 LTW 或者接收超时 (>500ms)。

• 发起方如果接收到错误的 LTW，则返回激活阶段。

—— 响应方操作

• 响应方若不能在一个 500ms 时间内处理完成发起方的一个 APDATA_REQ 中包含的命令请求，则必须在 500ms 内通过 RF 通道向发起方发送一个 LTW 长时等待消息，以通知发起方再等待 500ms；若

响应方在下一个 500ms 内仍不能处理完成发起方的 APDATA_REQ 命令请求, 则继续在每个 500ms 内发送一个 LTW, 直到响应方处理完该交易后做出 APDATA_RSP 响应为止。

- 响应方发送完 LTW 之后, 继续维持交易过程。

—— 处理流程

长时等待处理流程如图32所示。

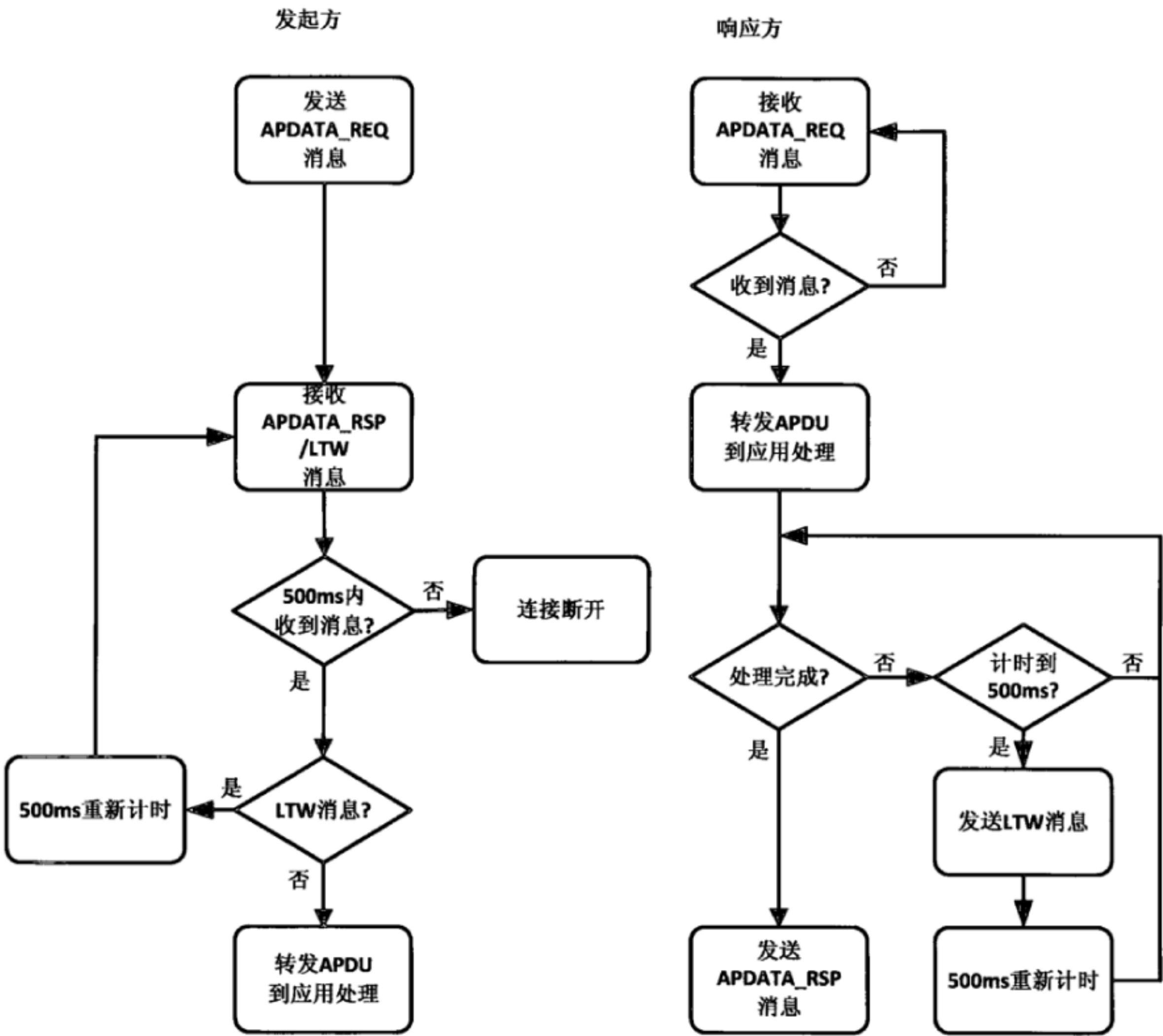


图32 长时等待处理流程

9.2.5 结束阶段

9.2.5.1 关闭连接

—— 发起方操作

- 如果发生下列情况之一, 发起方必须通过 RF 通道发出 CLOSE_REQ 关闭连接请求。
 - a) 交易正常结束;
 - b) 响应方状态不正常, 即接收到的响应消息中的状态字段值不是0x00;
 - c) 发生MTC冲突, 即接收到CHECK_RSP。
- 发起方应当在 CLOSE_REQ 请求中对于是否要求响应方做出回应给出明确的指示。

• 发起方如果要求响应方回应，则继续等待，直到接收到 CLOSE_RSP 或接收超时(>500ms)之后才返回激活阶段；否则发起方在发送完 CLOSE_REQ 后立即返回激活阶段。

—— 响应方操作

• 响应方在接收到第一个正确的 CLOSE_REQ 后，应当立即结束交易，并根据 CLOSE_REQ 中的指示来决定是否发送 CLOSE_RSP 响应。

• 如果发起方要求回应，则响应方应当在 500ms 内发送完 CLOSE_RSP，然后返回激活阶段；否则响应方在接收到 CLOSE_REQ 后立即返回激活阶段。

—— 处理流程

结束阶段处理流程如图33所示。

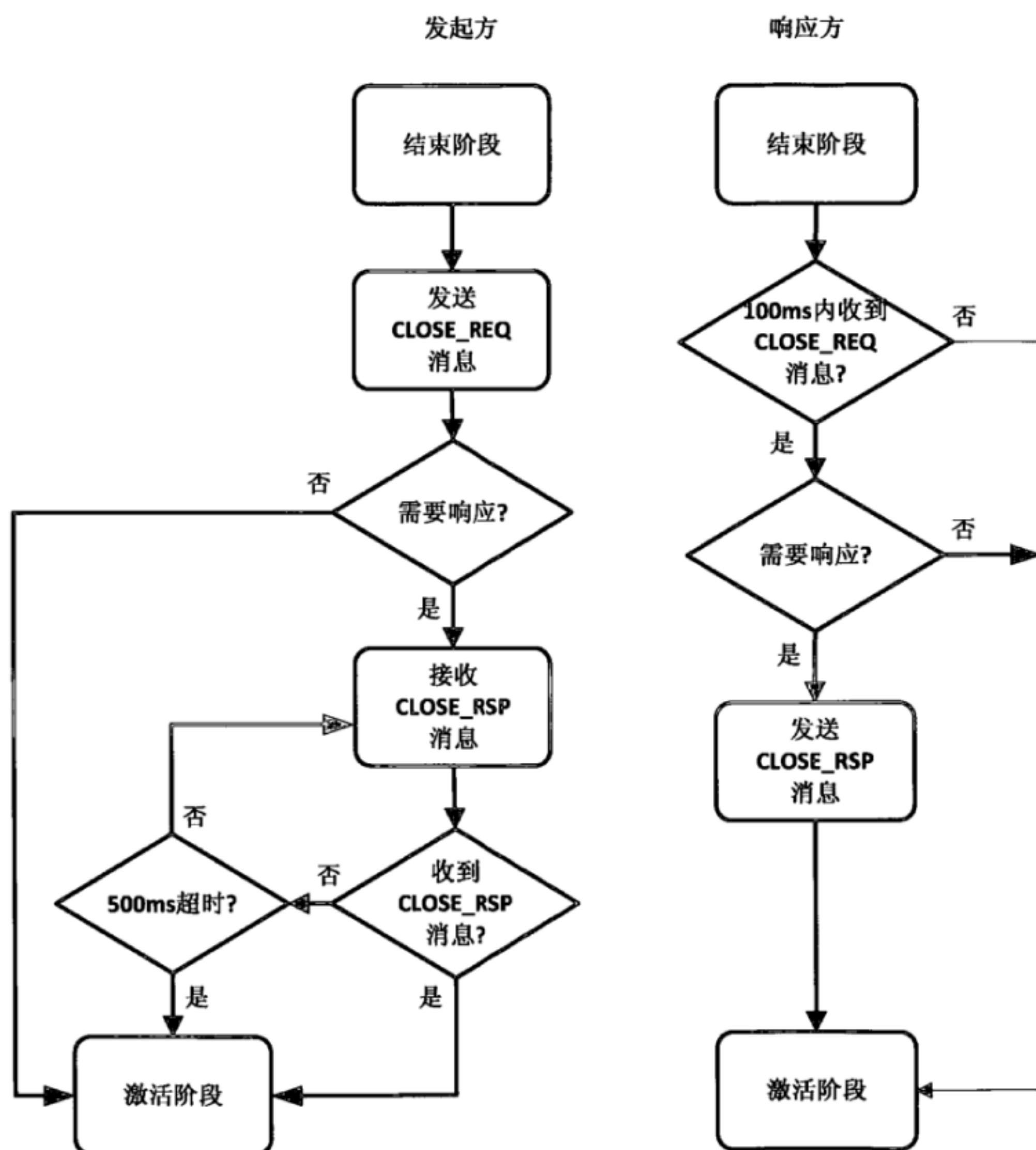


图33 结束阶段处理流程

9.3 通信会话命令

9.3.1 命令集

会话命令通过发起方和响应方之间传递的消息来实现。表22为本标准定义的全部会话命令消息集合。

表22 命令集

序号	命令分类	命令名称	命令功能	方向	信道	必选/可选
1	激活	INQUIRY	激活请求	发起方→响应方	MC	必选
		ATI	激活响应	响应方→发起方	RC	
2	连接	CONNECT_REQ	连接请求	发起方→响应方	RC	必选
		CONNECT_RSP	连接响应	响应方→发起方	RC	
3	数据交换	APDATA_REQ	数据交换请求	发起方→响应方	RC	必选
		APDATA_RSP	数据交换响应	响应方→发起方	RC	
4	维持连接	LINKCTL_REQ	维持连接请求	发起方→响应方	RC	必选
		LINKCTL_RSP	维持连接响应	响应方→发起方	RC	
5	冲突检测	CHECK1_REQ	冲突检测请求，用于冲突检测和连接确认	发起方→响应方	MC	必选
		CHECK_RSP	冲突响应	响应方→发起方	RC	
6	连接确认	CHECK2_REQ	连接确认请求，冲突检测关闭时，用于连接确认	发起方→响应方	MC	必选
7	长时等待	LTW	响应方要求等待	响应方→发起方	RC	必选
8	关闭	CLOSE_REQ	关闭连接请求	发起方→响应方	RC	必选
		CLOSE_RSP	关闭连接响应	响应方→发起方	RC	

9.3.2 命令功能描述

9.3.2.1 激活命令

9.3.2.1.1 INQUIRY

命令功能：查询并激活响应方。
传输信道：发起方通过磁通道发送INQUIRY消息。
消息格式：SMF。
消息内容：见表23。

表23 INQUIRY 消息

INQUIRY 消息头			
字段	长度（位）	值	注释
MsgCode	4	0	消息码
MsgLen	4	15	消息体字节长度
INQUIRY 消息体			
字段	长度（位/字节）	值	注释
Rfu	4 位	0000b	保留位
InitiatorVersion	4 位	0011b	发起方协议版本号，本标准协议版本号为 0x03
IDm	14 字节	XX	发起方生成的随机数，用于计算 ATI 接入参数和后续会话密钥

9.3.2.1.2 ATI

命令功能：响应方对INQUIRY的响应。
传输信道：响应方通过RF通道发送（频点=freq1(AID)，地址=addr1（AID），freq1和addr1的算法定义见附录A）。
消息格式：LMF。
消息内容：见表24。

表24 ATI 消息

ATI 消息头			
字段	长度 (位)	值	注释
Rfu	4		保留, 缺省为“0”
FormatType	4	8	消息格式类型
Status	8		响应方当前状态
MsgCode	8	16	消息码
MsgLen	16	24	消息体字节长度
ATI 消息体			
字段	长度 (字节)	值	注释
IDs	5	XX	响应方产生的随机数, 用于双方计算通信参数
TargetID	8		响应方唯一标识
AccessVersion	1		响应方选择的协议版本号: 响应方将 INQUIRY 中 InitiatorVersion 与自身协议版本比较, 将双方同时支持的最高协议版本号通过 AccessVersion 返回给发起方
MacData	4		响应方使用 K0 作为密钥对 (IDs TargetID AccessVersion) 进行 MAC 计算得到 MacData。16 字节 K0 使用 SKG0 中同样的扩展方式由 14 字节 IDm 扩展生成。 MAC 算法见附录 B.5
Reserved	6	0	保留, 缺省为“0”
ATI 消息校验			
字段	长度 (字节)	值	注释
CheckSum	2		校验值

9.3.2.2 建立连接命令

9.3.2.2.1 CONNECT_REQ

命令功能: 发起方连接请求。发起方在发送CONNECT_REQ消息之前, 必须首先验证ATI中的Mac是否正确。发起方必须在CONNECT_REQ消息中指明本次连接中所希望采用的链路安全机制, 包括使用的根密钥、会话密钥生成方式以及加密算法等。

传输信道: 发起方通过RF通道发送 (频点=freq1 (IDs), 地址=addr2 (IDs), freq1和addr2的算法定义见附录A)。

消息格式: LMF。

消息内容: 见表25。

表25 CONNECT_REQ 消息

CONNECT_REQ 消息头			
字段	长度 (位)	值	注释
Rfu	4		保留, 缺省为“0”
FormatType	4	8	消息格式类型
Status	8		发起方当前状态
MsgCode	8	17	消息码
MsgLen	16	24	消息体长度

表 25 (续)

CONNECT_REQ 消息体			
字段	长度 (字节)	值	注释
InitiatorType	1		发起方类型: “A”: 近距离 (10cm) 其他: 保留
InitiatorID	8		发起方唯一标识
RootKeyIndex	1		链路 APDU 数据加密根密钥索引号: RootKeyIndex 值表示所选择的根密钥索引号, 可支持最多 256 组根密钥。 0: 表示选择用 IDm 作为动态根密钥 K0 的有效密钥位, IDm 经位扩展后得到 16 字节 K0; 1: 表示选择第 1 组预置根密钥; 2: 表示选择第 2 组预置根密钥; 255: 表示选择第 255 组预置根密钥
SessionKey	1		发起方支持的会话密钥生成方式: 每个 Bit 代表一种会话密钥生成方式, “0”表示不支持该方式, “1”表示支持该方式, 最少应支持 1 种会话密钥生成方式, 最多可支持 8 种会话密钥生成方式。 SessionKey 定义见表 26 , 其中缺省的会话密钥生成方式 SK0 见附录 B.1
EncAlg	2		发起方支持的链路加密算法模式: 每个 Bit 代表一种链路加密算法模式, “0”表示不支持该算法模式, “1”表示支持该算法模式, 最少应支持 1 种加密算法模式, 最多可支持 16 种加密算法模式。 EncAlg定义见表27, 其中缺省的ALG0算法模式参见附录B.4
MDInfo	5		发起方设备信息, 由厂商自定义
Reserved	6	0	保留, 缺省为“0”
CONNECT_REQ 消息校验			
字段	长度 (字节)	值	注释
Checksum	2		校验值

表26 SessionKey: 会话密钥生成方式

位	密钥生成方式	值	说明
b7	SKG7	0	保留, 缺省为 “0”
b6	SKG6	0	保留, 缺省为 “0”
b5	SKG5	0	保留, 缺省为 “0”
b4	SKG4	0	保留, 缺省为 “0”
b3	SKG3	0	保留, 缺省为 “0”
b2	SKG2	0	保留, 缺省为 “0”
b1	SKG1	0	保留, 缺省为 “0”
b0	SKG0	1	

表27 EncAlg: 链路加密算法

位	链路加密算法模式	值	说明
b15		0	保留, 缺省为“0”
.....		0	保留, 缺省为“0”
b5	SM4-CBC	0/1	
b4	SM4-ECB	0/1	
b3	AES-CBC	0/1	
b2	AES-ECB	0/1	
b1	3DES-CBC	0/1	
b0	3DES-ECB	0/1	

9.3.2.2.2 CONNECT_RSP

命令功能: 响应方连接确认。响应方必须在CONNECT_RSP消息中确认本次连接中的链路安全机制, 包括根密钥使用、会话密钥生成方式以及加密算法的选择等。

传输信道: 响应方通过RF通道发送 (频点=freq1 (IDs), 地址=addr2 (IDs), freq1和addr2的算法定义见附录A)。

消息格式: LMF。

消息内容: 见表28。

表28 CONNECT_RSP 消息

CONNECT_RSP 消息头			
字段	长度 (位)	值	注释
Rfu	4		保留, 缺省为“0”
FormatType	4	8	消息格式类型
Status	8		响应方当前状态
MsgCode	8	18	消息码
MsgLen	16	24	消息体长度
CONNECT_RSP 消息体			
字段	长度 (字节)	值	注释
Result	1		Result 值定义如下: ● 0x00: 连接成功, 响应方继续等待下一步 APDU 指令或维持连接指令。 ● 0x01: 连接失败, 响应方断开连接
RootKeyIndex	1		根密钥索引号: ● 响应方确认使用的根密钥索引号, 最多支持 256 组根密钥; ● 编码格式及定义同 CONNECT_REQ 消息相应字段; ● 如果发起方选择使用动态根密钥 K0, 则响应方 CONNECT_RSP 中的 RootKeyIndex 值返回 0; ● 如果发起方选择使用预置根密钥 Ki (i≠0), 且响应方支持发起方所选择的预置根密钥 Ki (i≠0), 则响应方 RootKeyIndex 返回密钥 Ki 对应的索引值 i; ● 如果发起方选择使用预置根密钥 Ki (i≠0), 但响应方不支持发起方所选择的预置根密钥 Ki (i≠0), 则响应方 RootKeyIndex 值返回 0

表 28 (续)

CONNECT_RSP 消息体			
字段	长度 (字节)	值	注释
SessionKey	1		响应方确认的会话密钥生成方式: ● 每个 bit 代表一种会话密钥生成方式, “0”表示不支持该方式, “1”表示支持该方式, 最多支持 8 种会话密钥生成方式; ● 编码格式及定义同 CONNECT_REQ 消息相应字段; ● 响应方在双方都支持的会话密钥生成方式中选择 1 个会话密钥生成方式, 置位后返回给发起方。若双方同时支持的会话密钥生成方式有多个, 则缺省情况下选择其中最高位所代表的会话密钥生成方式
EncAlg	2		响应方确认的链路加密算法模式: ● 每个 bit 代表一种链路加密算法模式, “0”表示不支持该算法模式, “1”表示支持该算法模式, 最多支持 16 种加密算法模式。 ● 编码格式及定义同 CONNECT_REQ 消息相应字段。 ● 响应方在双方都支持的加密算法模式中选择 1 个加密算法模式, 置位后返回给发起方。若双方同时支持的加密算法模式有多个, 则缺省情况下选择其中最高位所代表的加密算法模式
SDInfo	5		响应方信息, 厂商自定义
SDRand	8		响应方生成的随机数, 用于计算会话密钥
Reserved	6	缺省为 “0”	保留, 缺省为 “0”
CONNECT_RSP 消息校验			
字段	长度 (字节)	值	注释
Checksum	2		校验值

9.3.2.3 数据交换命令

9.3.2.3.1 APDATA_REQ

命令功能: 发起方传递的应用层数据、命令。

传输信道: 发起方通过RF通道发送 (频点=freq1 (IDs), 地址=addr2 (IDs) freq1和addr2的算法定义见附录A)。

消息格式: LMF。

消息内容: 见表29。

表29 APDATA_REQ 消息

APDATA_REQ 消息头			
字段	长度 (位)	值	注释
Rfu	4		保留, 缺省为 “0”
FormatType	4	8	消息格式类型
Status	8		发起方当前状态
MsgCode	8	19	消息码
MsgLen	16	<i>M</i>	消息体字节长度 <i>M</i> ($0 \leq M \leq 288$)

表 29 (续)

APDATA_REQ 消息体			
字段	长度 (字节)	值	注释
EncPayload	M	XX	对明文数据 (长度为 N , $0 \leq N \leq 286$) 加密后得到的密文数据块, 长度为 M : 若 $(N+2)$ 为 8 的整数倍, 则 $M=N+2$; 若 $(N+2)$ 不为 8 的整数倍, 则 $M=[(N+2)/8] \times 8 + 8$
APDATA_REQ 消息校验			
字段	长度 (字节)	值	注释
Checksum	2		校验值

9.3.2.3.2 APDATA_RSP

命令功能: 响应方对APDATA_REQ的响应。

传输信道: 响应方通过RF通道发送 (频点=freq1 (IDs), 地址=addr2 (IDs), freq1和addr2的算法定义见附录A)。

消息格式: LMF

消息内容: 见表30

表30 APDATA_RSP 消息

APDATA_RSP 消息头			
字段	长度 (位)	值	注释
Rfu	4		保留, 缺省为 “0”
FormatType	4	8	消息格式类型
Status	8		响应方当前状态
MsgCode	8	20	消息码
MsgLen	16	M	消息体字节长度 M ($0 \leq M \leq 288$)
APDATA_RSP 消息体			
字段	长度 (字节)	值	注释
EncPayload	M	XX	对明文数据 (长度为 N , $0 \leq N \leq 286$) 加密后得到的密文数据块, 长度为 M : 若 $(N+2)$ 为 8 的整数倍, 则 $M=N+2$; 若 $(N+2)$ 不为 8 的整数倍, 则 $M=[(N+2)/8] \times 8 + 8$
APDATA_RSP 消息校验			
字段	长度 (字节)	值	注释
Checksum	2		校验值

9.3.2.4 维持连接命令

9.3.2.4.1 LINKCTL_REQ

命令功能: 发起方的链路维持请求。用于在链路空闲的状态下发起方与响应方进行连接状态的确认。

传输信道: 发起方通过RF通道发送 (频点=freq1 (IDs), 地址=addr2 (IDs), freq1和addr2的算法定义见附录A)。

消息格式: LMF。

消息内容: 见表31。

表31 LINKCTL_REQ 消息

LINKCTL_REQ 消息头			
字段	长度 (位)	值	注释
Rfu	4		保留, 缺省为 “0”
FormatType	4	8	消息格式类型
Status	8		发起方当前状态
MsgCode	8	22	消息码
MsgLen	16	2	消息体字节长度
LINKCTL_REQ 消息体			
字段	长度 (字节)	值	注释
RandData	1	XX	随机数
Reserved	1		保留, 缺省为 “0”
LINKCTL_REQ 消息校验			
字段	长度 (字节)	值	注释
Checksum	2		校验值

9.3.2.4.2 LINKCTL_RSP

命令功能: 响应方对发起方LINKCTL_REQ命令的响应。

传输信道: 响应方通过RF通道发送 (频点=freq1 (IDs), 地址=addr2 (IDs), freq1和addr2的算法定义见附录A)。

消息格式: LMF

消息内容: 见表32

表32 LINKCTL_RSP 消息

LINKCTL_RSP 消息头			
字段	长度 (位)	值	注释
Rfu	4		保留, 缺省为 “0”
FormatType	4	8	消息格式类型
Status	8		响应方当前状态
MsgCode	8	23	消息码
MsgLen	16	2	消息体字节长度
LINKCTL_RSP 消息体			
字段	长度 (字节)	值	注释
RandData	1	XX	随机数
Reserved	1		保留, 缺省为 “0”
LINKCTL_RSP 消息校验			
字段	长度 (字节)	值	注释
Checksum	2		校验值

9.3.2.5 冲突检测命令

9.3.2.5.1 CHECK1_REQ

命令功能: 冲突检测。

传输信道: 发起方通过磁通道发送CHECK1_REQ消息。

消息格式: SMF

消息内容：见表33

表33 CHECK1_REQ 消息

CHECK1_REQ 消息头			
字段	长度（位）	值	注释
MsgCode	4	2	消息码
MsgLen	4	2	消息体字节长度
CHECK1_REQ 消息体			
字段	长度（字节）	值	注释
CDC	2		冲突检测码CDC：取当前响应方生成的随机数IDs的前2字节。在冲突检测打开的情况下CDC同时作为TRI使用。 响应方接收到CHECK1_REQ后，应当按照如下方式更新自己的当前状态： 如果CDC/TRI与本地IDs前两个字节相同，则响应方认为当前连接状态为正常（0x00）；否则响应方认为当前连接状态为异常（0x01）

9.3.2.5.2 CHECK_RSP

命令功能：冲突响应。

传输信道：响应方通过RF通道发送（频点=freq2（CDC），地址=addr1（CDC），freq2和addr1的算法定义见附录A）。

消息格式：LMF。

消息内容：见表34。

表34 CHECK_RSP 消息

CHECK_RSP 消息头			
字段	长度（位）	值	注释
Rfu	4		保留，缺省为“0”
FormatType	4	8	消息格式类型
Status	8		响应方当前状态
MsgCode	8	24	消息码
MsgLen	16	16	消息体字节长度
CHECK_RSP 消息体			
字段	长度（字节）	值	注释
RandData	1	XX	随机数
TargetID	8		响应方标识
Reserved	7		保留，缺省为“0”
CHECK_RSP 消息校验			
字段	长度（字节）	值	注释
Checksum	2		校验值

9.3.2.6 连接确认消息

9.3.2.6.1 CHECK2_REQ

命令功能：连接确认。如果当前冲突检测配置为关闭，则发起方在建立连接之后持续发送CHECK2_REQ消息。

传输信道：发起方通过磁通道发送 CHECK2_REQ 消息。

消息格式：SMF。

消息内容：见表 35。

表35 CHECK2_REQ 消息

CHECK2_REQ 消息头			
字段	长度（位）	值	注释
MsgCode	4	3	消息码
MsgLen	4	2	消息体字节长度
CHECK2_REQ 消息体			
字段	长度（字节）	值	注释
TRI	2		响应方随机标识码 TRI：取当前响应方生成的随机数 IDs 的前 2 字节。 响应方接收到CHECK2_REQ后, 应当按照如下方式更新自己的当前状态： 如果TRI与本地IDs前两个字节相同，则响应方认为当前连接状态为正常（0x00）；否则响应方认为当前连接状态为异常（0x01）

9.3.2.7 长时等待命令

9.3.2.7.1 LTW

命令功能：响应方发送给发起方的长时交易等待指令。

传输信道：响应方通过RF通道发送（频点=freq1（IDs），地址=addr2（IDs），freq1和addr2的算法定义见附录A）。

消息格式：LMF。

消息内容：见表36。

表36 LTW 消息

LTW 消息头			
字段	长度（位）	值	注释
Rfu	4		保留，缺省为“0”
FormatType	4	8	消息格式类型
Status	8		响应方当前状态
MsgCode	8	25	消息码
MsgLen	16	2	消息体字节长度
LTW 消息体			
字段	长度（字节）	值	注释
RandData	1	XX	随机数
Reserved	1		保留，缺省为“0”
LTW 消息校验			
字段	长度（字节）	值	注释
Checksum	2		校验值

9.3.2.8 关闭连接命令

9.3.2.8.1 CLOSE_REQ

命令功能：发起方断开与响应方的连接。

传输信道：发起方通过RF通道发送（频点=freq1（IDs），地址=addr2（IDs），freq1和addr2的算法定义见附录A）。

消息格式：LMF

消息内容：见表37

表37 CLOSE_REQ 消息

CLOSE_REQ 消息头			
字段	长度（位）	值	注释
Rfu	4		保留，缺省为“0”
FormatType	4	8	消息格式类型
Status	8		发起方当前状态
MsgCode	8	26	消息码
MsgLen	16	4	消息体字节长度
CLOSE_REQ 消息体			
字段	长度（字节）	值	注释
NeedResp	1	0/1	是否需要返回关闭连接确认 0：无需 CLOSE_RSP 响应。 1：需要 CLOSE_RSP 响应。 默认：0
Reserved	3		保留，缺省为“0”
CLOSE_REQ 消息校验			
字段	长度（字节）	值	注释
Checksum	2		校验值

9.3.2.8.2 CLOSE_RSP

命令功能：响应方对CLOSE_REQ的响应确认。只有发起方在CLOSE_REQ中指明需要响应方对关闭连接进行确认（NeedResp=1）时，响应方才做CLOSE_RSP响应确认，否则响应方在关闭连接后即结束，不做CLOSE_RSP响应。

传输信道：响应方通过RF通道发送（频点=freq1（IDs），地址=addr2（IDs），freq1和addr2的算法定义见附录A）。

消息格式：LMF

消息内容：见表38

表38 CLOSE_RSP 消息

CLOSE_RSP 消息头			
字段	长度（位）	值	注释
Rfu	4		保留，缺省为“0”
FormatType	4	8	消息格式类型
Status	8		响应方当前状态
MsgCode	8	27	消息码
MsgLen	16	4	消息体字节长度

表 38 (续)

CLOSE_RSP 消息体			
字段	长度 (字节)	值	注释
CloseResult	1	0/1	关闭结果: 0: 响应方关闭成功。 1: 响应方关闭失败
Reserved	3		保留, 缺省为“0”
CLOSE_RSP 消息校验			
字段	长度 (字节)	值	注释
Checksum	2		校验值

附录 A
(规范性附录)
RF 通信参数计算

A.1 RF频点计算方法

RF频点计算方法如下:

以 N 为模对输入 X 进行求余运算, 即 $(X) \bmod N$, 其中 N 是RF射频频率表支持的最大频点数目, X 为不小于2字节的数据串。

计算得到的余数与频点的对应关系如表A.1所示。

表 A.1 余数与频点的对应关系

频点序号	Ch_1	Ch_2	Ch_3	Ch_{N-1}	Ch_N
余数	0	1	2	$N-2$	$N-1$

表 A.2 工作频点表

频点序号	Ch_1	Ch_2	Ch_3	Ch_{63}	Ch_{64}
频率 (MHz)	2401	2402	2403	2463	2464

表 A.3 冲突响应频点表

频点序号	Ch_1	Ch_2	Ch_3	Ch_4
频率 (MHz)	2465	2466	2467	2468

freq1 算法描述:

用途: 用于计算工作频点。

计算方法:

- (1) X 为不小于2字节的数据串, 取 X 前2字节, 记为 $X2$;
- (2) $freq1(X) = (X2) \bmod N$, $N = 64$;
- (3) 用 $freq1(X)$ 作为索引查表A.2所示工作频点表, 得到工作频点。

计算示例:

假设数据串 X : 0x30||0x39||0x23||0xa5, 其中“||”表示“拼接”。

则 $X2 = 0x30||0x39 = 12345$

$freq1(X) = (X2) \bmod N = (12345) \bmod 64 = 57$, 根据余数与频点对应关系, 余数57对应频点 Ch_{58} , 查表A.2, Ch_{58} 频率值为2458MHz。

freq2 算法描述:

用途: 用于计算冲突响应 (CHECK_RSP) 频点。

计算方法:

1. X 为不小于2字节的数据串, 取 X 前2字节, 记为 $X2$;
2. $freq2(X) = (X2) \bmod N$, $N = 4$;
3. 用 $freq2(X)$ 作为索引查表A.3所示冲突响应频点表, 得到冲突响应频点。

计算示例:

假设数据串 X : 0x30||0x39||0x23||0xa5, 其中“||”表示“拼接”。

则 $X2 = 0x30||0x39 = 12345$

$freq2=(X) \bmod N = (12345) \bmod 4 = 1$ ，根据余数与频点对应关系，余数 1 对应频点 Ch_2 ，查表 A.3， Ch_2 频率值为 2466MHz。

A.2 RF通信地址计算方法

addr1 算法描述：

用途：用于计算激活响应（ATI）和冲突响应（CHECK_RSP）RF 通信地址。

计算方法：

$addr1(X) = X[0] \parallel X[1] \parallel \overline{X[0]} \parallel \overline{X[1]} \parallel 0x00$ ，其中“ \parallel ”表示“拼接”。

其中 X 为 2 字节数据串。

说明：按照下列顺序将各字节组合成一个 5 字节的 RF 地址： X 第 1 字节、 X 第 2 字节、 X 第 1 字节的按位取反、 X 第 2 字节的按位取反、最后一个字节补 0。

通信 *addr2* 算法描述：

用途：用于计算（除了 ATI 地址和 CHECK_RSP 地址之外的）其他所有 RF 通信地址。

计算方法：

$addr2(X) = X[0] \parallel X[1] \parallel X[2] \parallel X[3] \parallel X[4]$ ，其中“ \parallel ”表示“拼接”。

其中 X 为 5 字节数据串。

说明：按照下列顺序将 X 各字节组合成一个 5 字节的 RF 地址： X 第 1 字节、 X 第 2 字节、 X 第 3 字节、 X 第 4 字节、 X 第 5 字节。

A.3 AID计算方法

对于长度为 n ($2 \leq n \leq 14$) 字节的 ID_m，经过如下方式计算得到 AID：

a) 若 $n \leq 8$ ，则在 ID_m 后补 0x00 ($n=8$ 时不用补 0x00)，补齐 8 字节，作为 Ka ， $K=Ka \parallel \overline{Ka}$ （其中 \overline{Ka} 表示对 Ka 的按位取反）；若 $8 < n \leq 14$ ，则直接在 ID_m 后补 0x00，补齐 16 字节，作为 K 。

b) 计算 3DES[K , ID_m]（若 $n < 8$ ，则在 ID_m 后补 0x00，补齐 8 字节作为被加密明文；若 ID_m 长度 $n \geq 8$ ，则取 ID_m 前 8 字节作为被加密明文），得到 8 字节密文数据。

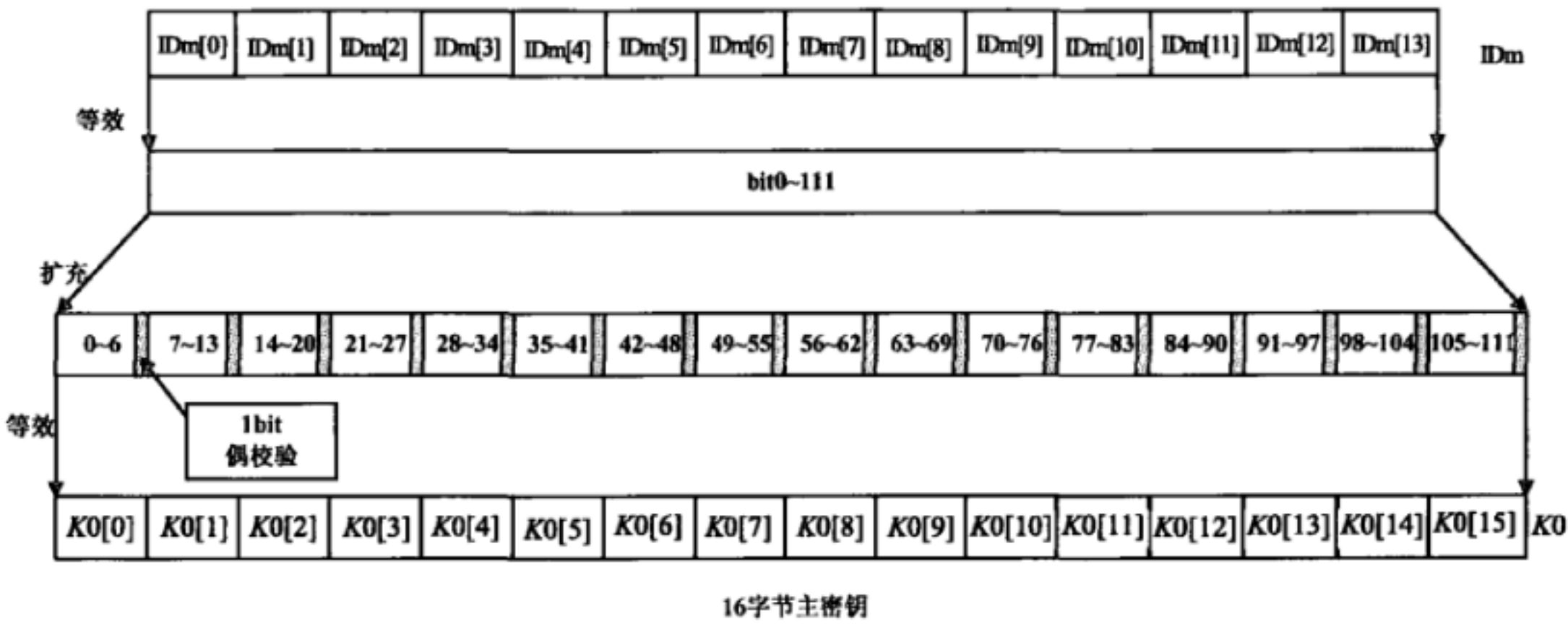
c) 取 8 字节密文数据前 2 字节，作为“AID”。

附录 B
(规范性附录)
密码相关算法定义

B.1 会话密钥产生方法

SKG0 会话密钥产生的方法如下。

第一步：计算主密钥 K ：如果使用预置根密钥（即 CONNECT_RSP 中确认的 RootKeyIndex 值不为“0”），则 16 字节主密钥 $K=K0 \oplus Ki$ ，（ $i \neq 0$ ）；如果不使用预置根密钥（即 CONNECT_RSP 中确认的 RootKeyIndex 值为“0”），则 16 字节主密钥 $K=K0$ ；其中，16 字节 $K0$ 由 14 字节 IDm（随机数）通过如图 B.1 所示方式扩展生成。



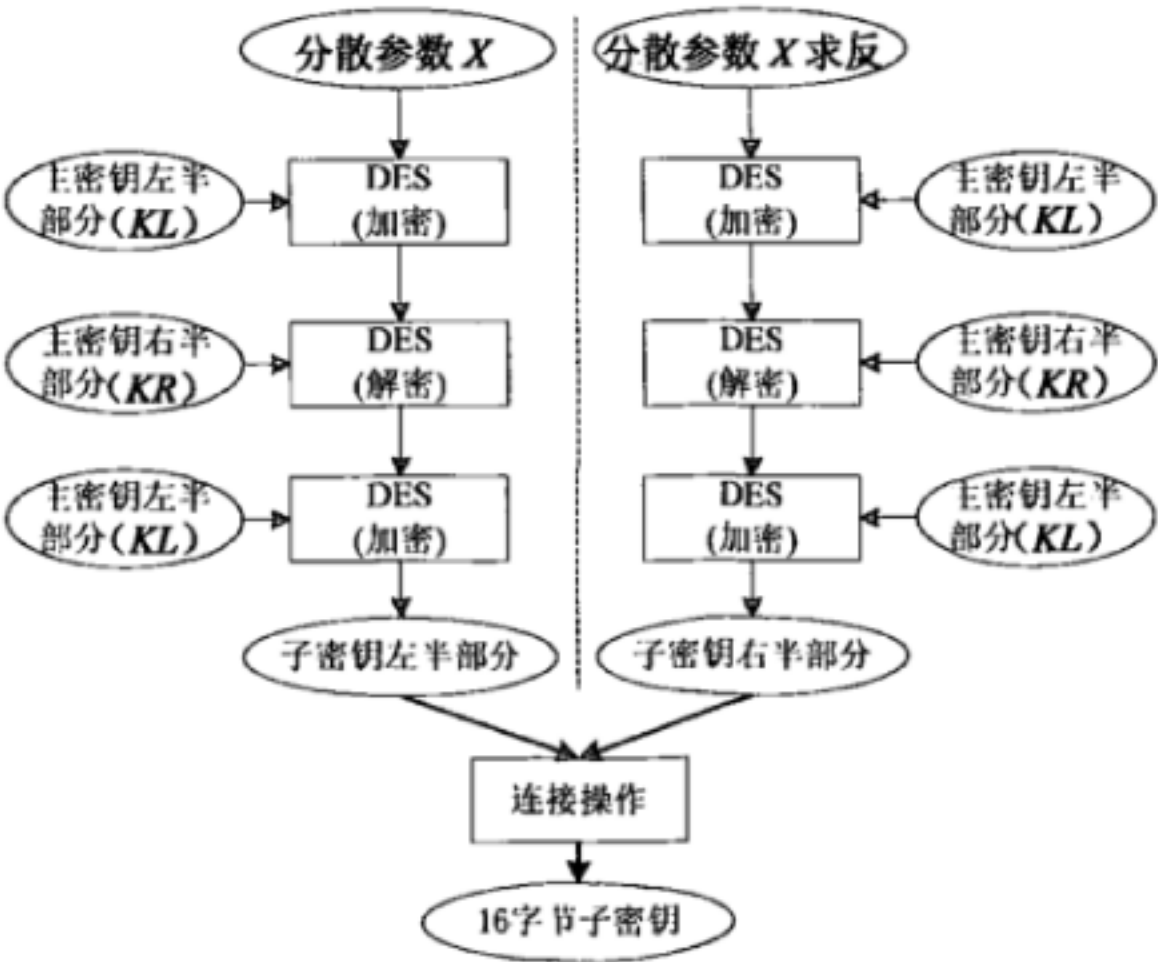
图B.1 IDm 扩展生成 K0 的方式

第二步：以响应方产生的 8 字节随机数 SDRand 为分散参数 X ，按照本标准附录 B.2 所定义的“子密钥分散算法”对第一步中计算得到的主密钥 K 进行密钥分散，得到 16 字节子密钥 Ks 。

第三步：使用 Ks 作为会话密钥。

B.2 子密钥分散算法

子密钥分散算法如图B.2所示。



图B.2 子密钥分散算法

分散参数 X 不足8字节, 则先右补0x80, 如不足8字节则补0x00至8字节。

分散参数 X 超过8字节, 则取最右8字节。

B.3 3DES加解密算法

3DES 加解密算法定义如下:

密钥长度为 16 字节 ($K = (KL||KR)$), 数据分组长度为 8 字节。

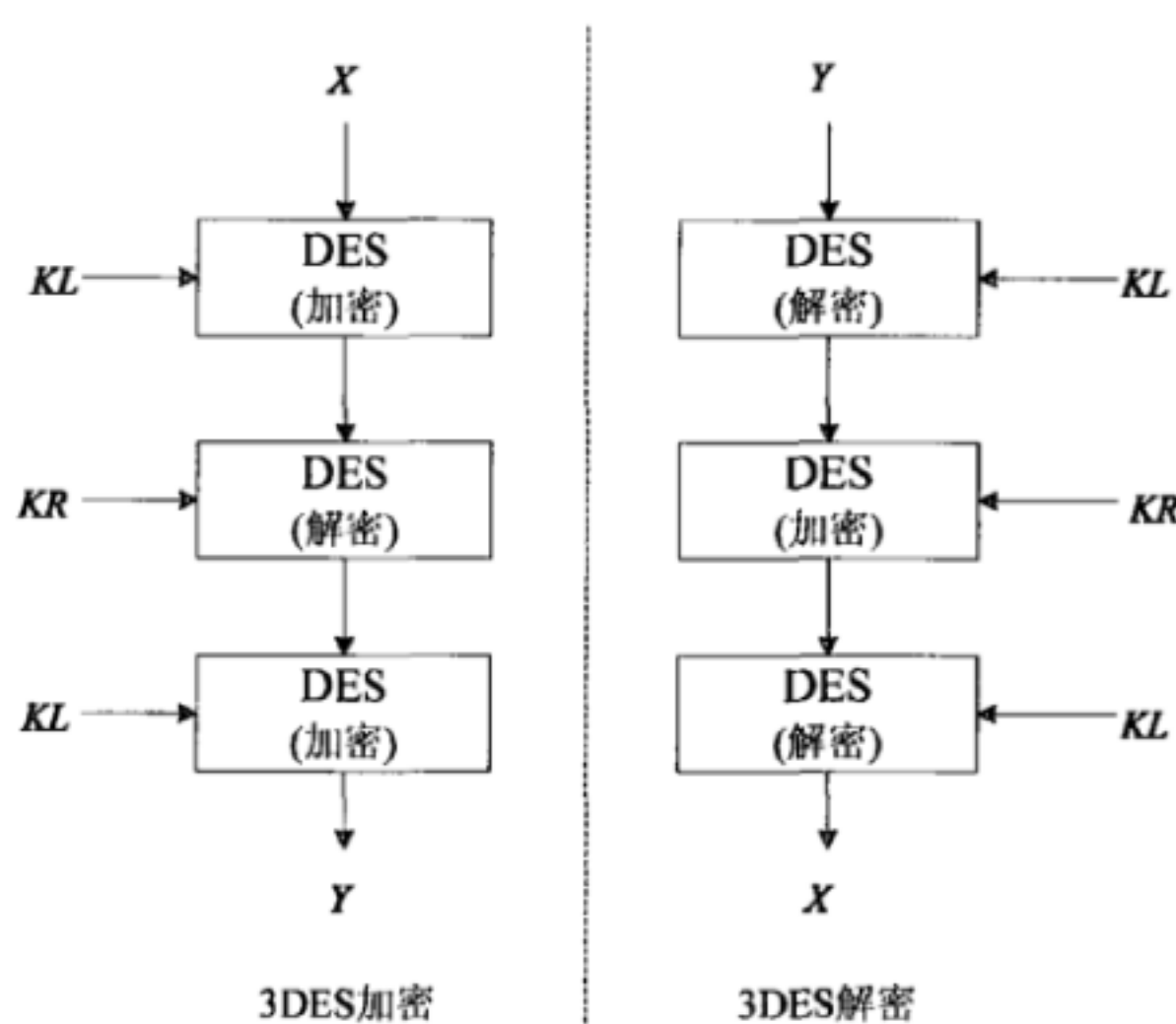
对于每个数据分组的加密算法如下:

$$Y = 3DES[K, X] = DES(KL)[DES^{-1}(KR)[DES(KL)[X]]]$$

解密算法如下:

$$Y = 3DES^{-1}[K, X] = DES^{-1}(KL)[DES(KR)[DES^{-1}(KL)[X]]]$$

每个分组的加解密过程如图 B.3 所示。



图B.3 3DES 加解密过程

对于多个分组的加/解密过程, 只需要将所有加/解密后的数据块依照原顺序连接在一起。

B.4 数据报文加解密方法

ALG0 数据加密方法如下。

对应用层数据报文 Payload 采用 ECB 模式的对称密码算法进行加解密。

按照如下步骤对数据报文进行加密。

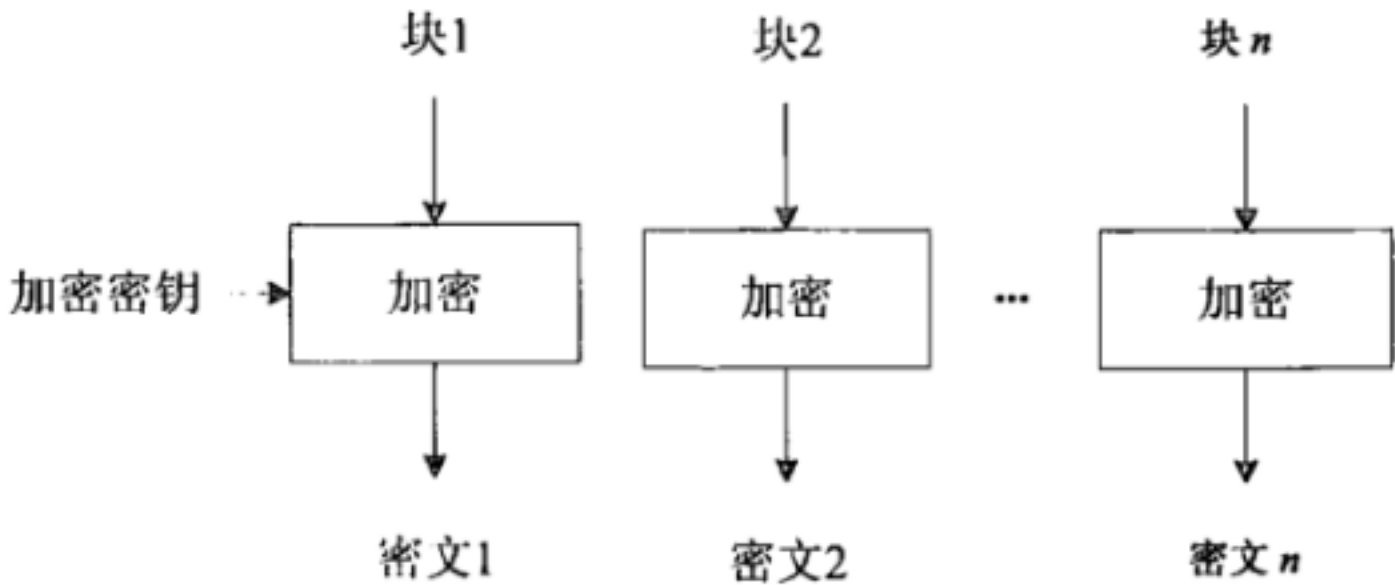
第一步: 用 PLen (2 字节) 表示明文数据的字节长度, 在明文数据前加上 PLen, 产生新的数据块。

第二步: 将该数据块分成以分组长度 8 字节为单位的数据块, 表示为块 1、块 2……块 n 。

第三步: 如果最后 (或唯一) 的数据块的长度是分组长度, 转到第四步; 如果不足分组长度, 则在其后加入 16 进制数 “80”, 如果达到分组长度, 则转到第四步, 否则在其后加入 16 进制数 “00” 直到长度达到分组长度。

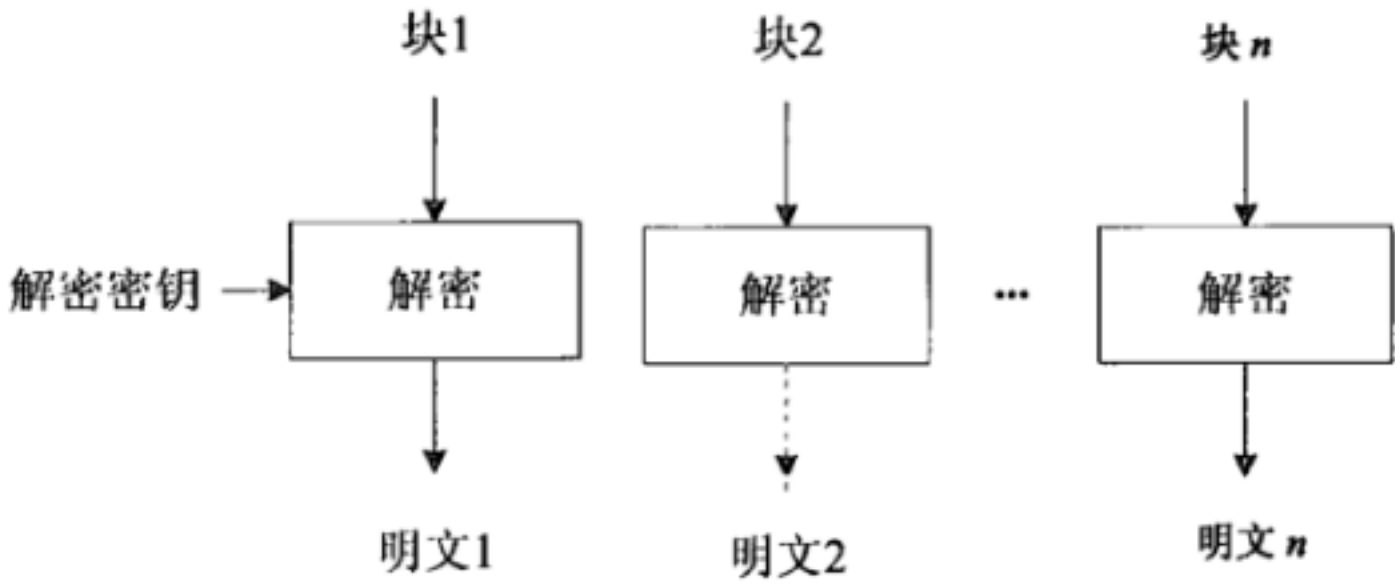
第四步: 按照图 B.4 所述的算法使用加密密钥对每一个数据块进行加密。

第五步: 计算结束后, 所有加密后的数据块依照原顺序连接在一起。



图B.4 分组加密

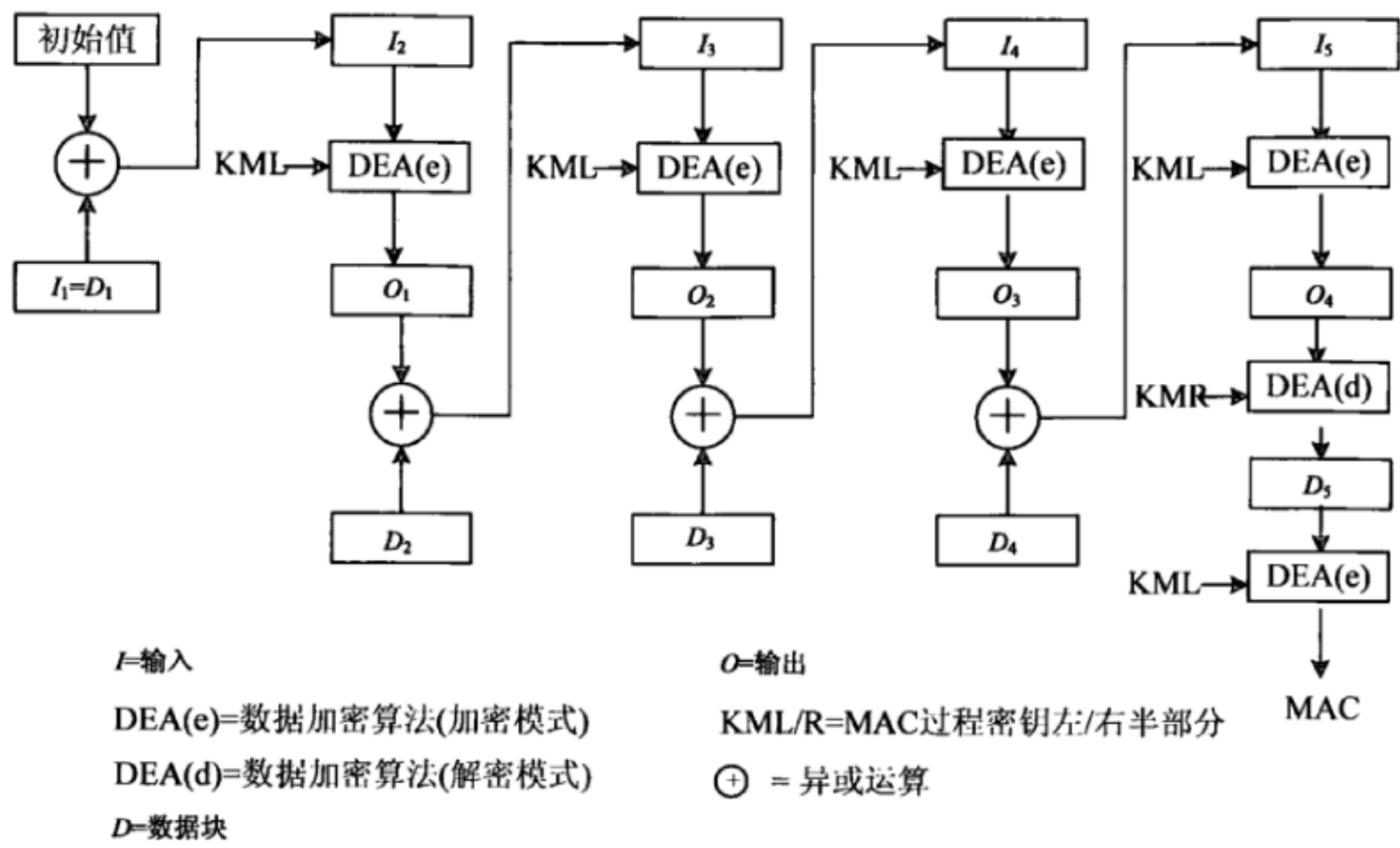
- 按照如下步骤对数据进行解密：
- 第一步：将该数据块分成以分组长度 8 字节为单位的数据块，表示为块 1、块 2……块 n 。
 - 第二步：按照图 B.5 所述的算法使用解密密钥对每一个数据块进行解密。
 - 第三步：计算结束后，所有解密后的数据块依照原顺序连接在一起。
 - 第四步：前 2 个字节为 PLen，从第 3 字节起，取前 PLen 字节数据作为明文输出。



图B.5 分组解密

B.5 MAC算法

- MAC 的产生使用以下算法：
- 第一步：将一个 8 个字节长的初始值（Initial Vector）设定为 16 进制的“0x 00 00 00 00 00 00 00 00”。
 - 第二步：将所有的输入数据按指定顺序连接成一个数据块。
 - 第三步：将连接成的数据块分割为 8 字节长的数据块组，标识为 D1、 D2、 D3、 D4 等。分割到最后，余下的字节组成一个长度小于等于 8 字节的最后一块数据块。
 - 第四步：如果最后一个数据块长度为 8 字节，则在此数据块后附加一个 8 字节长的数据块，附加的数据块为：16 进制的“0x 80 00 00 00 00 00 00 00”。如果最后一个数据块长度小于 8 字节，则该数据块的最后填补一个值为 16 进制“0x80”的字节。如果填补之后的数据块长度等于 8 字节，则跳至第五步。如果填补之后的数据块长度仍小于 8 字节，则在数据块后填补 16 进制“0x00”的字节至数据块长度为 8 字节。
 - 第五步：MAC 的产生是通过上述方法产生的数据块组，由 K0 进行加密运算，加密算法 DEA 使用 DES。MAC 算法如图 B.6 所示。



图B.6 MAC 算法

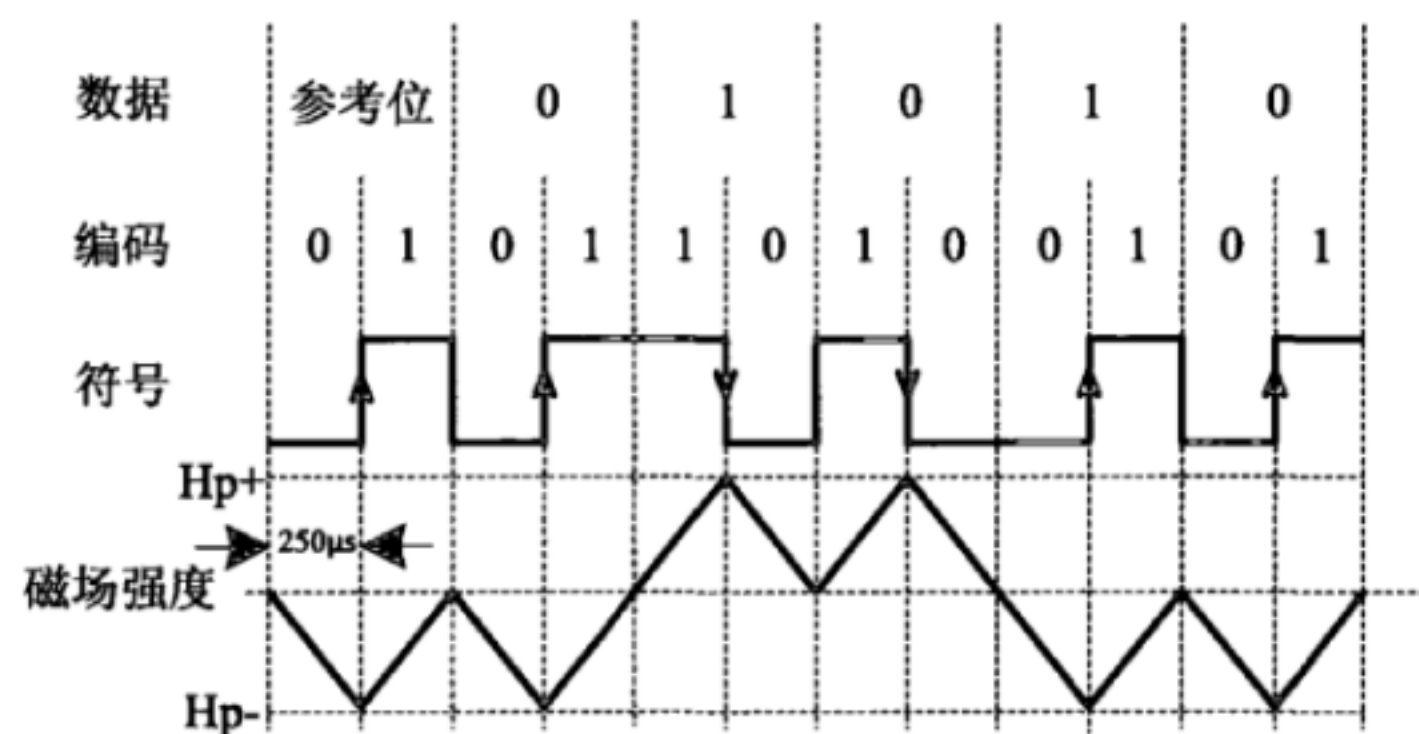
第六步：最终值的左4字节为MAC。

附录 C

(资料性附录)

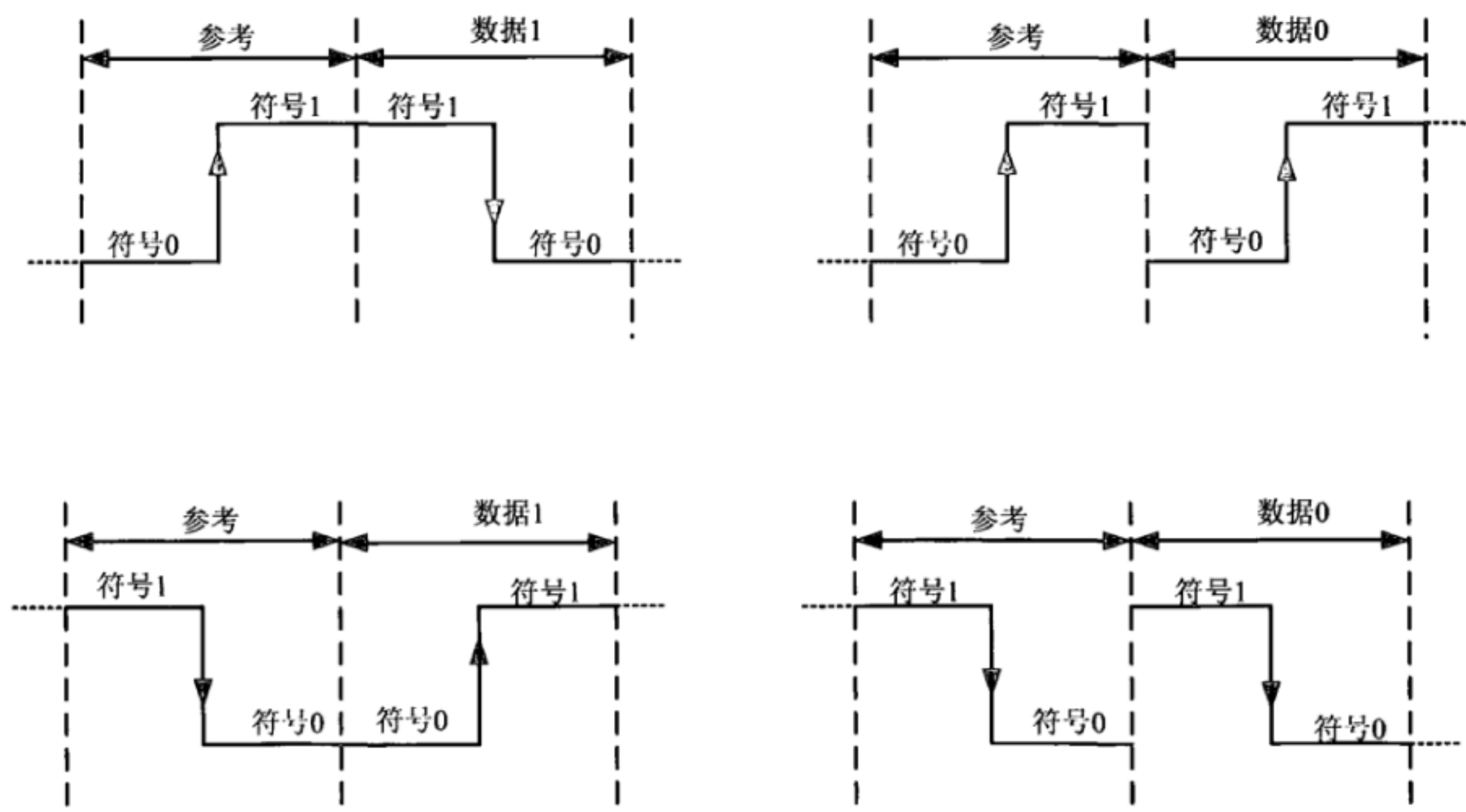
磁通道通信原理说明

磁场强度变化率调制如图C.1所示,符号“1”的场强变化率与符号“0”的场强变化率应为相反关系,且变化率大小相等并保持恒定。磁通道数据编码符号率为4kS/s,每个符号周期为250 μ s, H_p 为发起方磁场信号强度峰值。磁通道信号符号的极性只与磁场强度变化率的方向有关,而与磁场强度变化率的大小无关。磁场强度变化率的大小决定了磁场强度的峰值,磁场强度峰值的规范要求用于距离控制。



图C.1 磁场强度变化率调制

磁通道数据编码采用差分曼彻斯特编码 (DME), 如图C.2所示。每个数据位由2个符号组成的序列表示, 每个数据位的符号序列必须为“10”或“01”。数据位“1”的符号序列与前一个数据位的符号序列相反, 数据位“0”的符号序列与前一个数据位的符号序列相同。



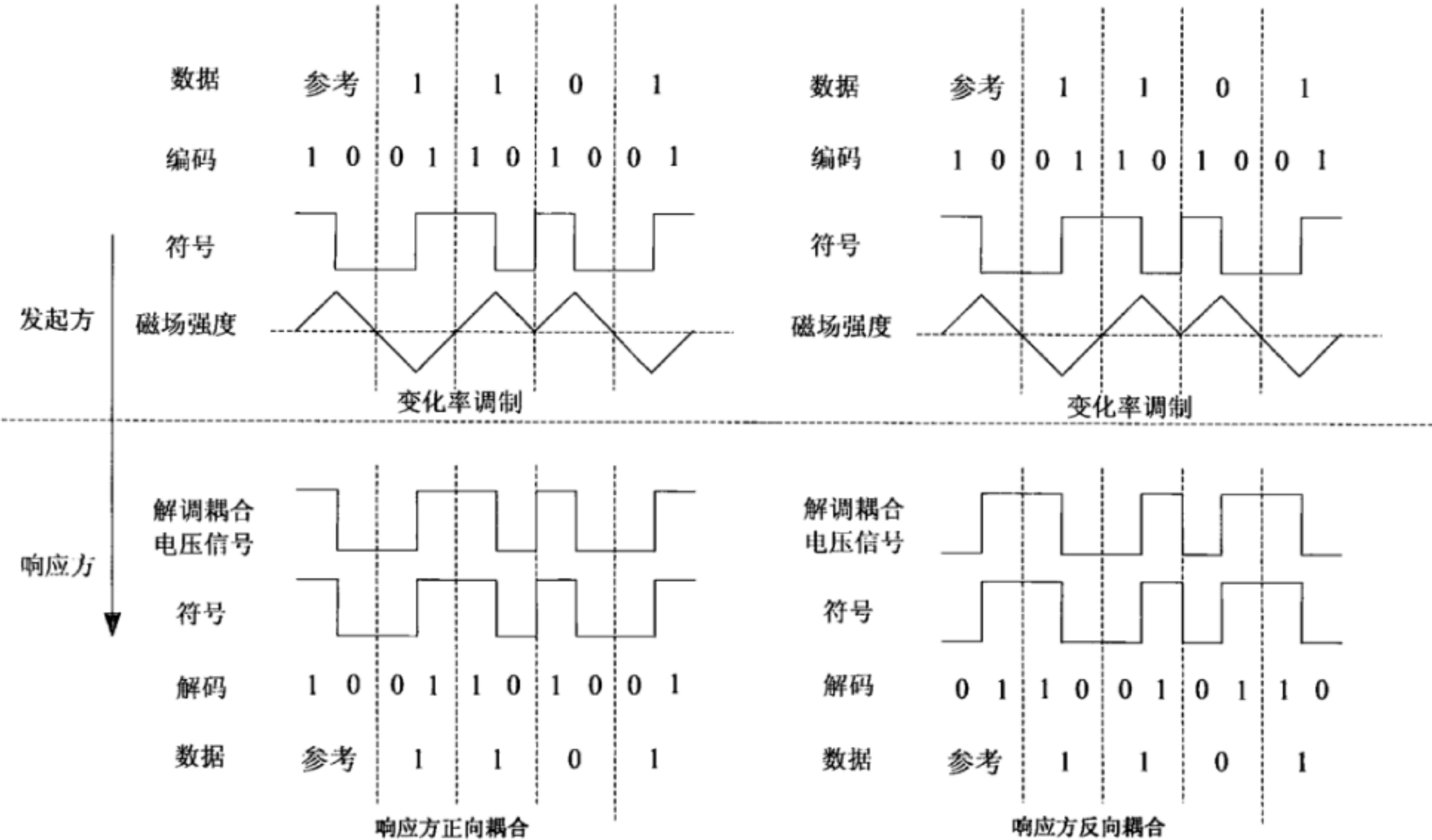
图C.2 差分曼彻斯特编码

磁通道调制解调及编解码原理如图C.3所示，发起方根据上述编码和调制原理，将磁通道数据转换为磁场强度变化率调制信号。响应方通过磁感应线圈感应得到解调耦合电压信号，电压信号与磁场信号的关系如下：

$$V = \frac{Nd\phi}{dt} = \frac{Nd(BS)}{dt} = \frac{NSdB}{dt} = \frac{NSd(\mu_0 H)}{dt} = \mu_0 NS \frac{dH}{dt}$$

式中：
 V 为响应方耦合电压；
 N 为响应方耦合线圈匝数；
 S 为响应方耦合线圈面积；
 $\frac{dH}{dt}$ 为磁场强度的变化率；
 μ_0 为空气中磁导率。

响应方从电压信号中得到磁通道信号符号序列，再根据差分曼彻斯特编码机制解码得到磁通道数据。从图C.3中所列的两种情况可以看出，无论响应方采用正向耦合方式或是反向耦合方式，最终都能得到正确的解码数据结果。



图C.3 磁通道调制解调及编解码原理

中华人民共和国
通信行业标准

手机支付

基于 2.45GHz RCC(限域通信)技术的非接触射频接口技术要求

YD/T 2772-2014

*

人民邮电出版社出版发行

北京市丰台区成寿寺路 11 号邮电出版大厦

邮政编码: 100164

北京康利胶印厂印刷

版权所有 不得翻印

*

开本: 880×1230 1/16

2015 年 12 月第 1 版

印张: 3.5

2015 年 12 月北京第 1 次印刷

字数: 93 千字

15115 • 603

定价: 35 元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492