armsky™
斯凯科技
http://www.armsky.net

IEEE 802.15.4 标准
ZigBee 协议规范

首字母缩略词及定义

ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	高级加密标准
AF	Application Framework	应用框架
AIB	APS Information Base	APS 信息库
APDU	APS sub-layer PDU	应用支持子层协议数据单元
API	Application Programming Interface	应用编程接口
APL	Application Layer	应用层
APS	Application Support Sub-Layer	应用支持子层
APSDE	APS Data Entity	APS 数据实体
APSDE-SAP	APS Data Entity - Service Access Point	APS 数据实体-服务访问点
APSME	APS Management Entity	APS 管理实体
APSME-SAP	APS Management Entity - Service Access Point	APS 管理实体-服务访问点
ASDU	APS Service Datagram Unit	APS 服务数据单元
BE	Backoff Exponent	回退指数
BI	Beacon Interval	信标间隔
BO	Beacon Order	信标阶数
BPSK	Binary Phase Shift Keying	二进制相移键控
BSN	Beacon Sequence Number	信标序号
BTR	Broadcast Transaction Record	广播事务记录
BTT	Broadcast Transaction Table	广播事务表
CAP	Contention Access Period	竞争访问周期
CBC	Cipher Block Chaining	密码防护链
CBC-MAC	Cipher Block Chaining Message Authentication Code	密码防护链消息验证代码
CCA	Clear Channel Assessment	空闲信道评估
CCM	Encryption using CTR with CBC-MAC	计数器模式和密码防护链消息验证代码
CD	Carrier Detect	载波检测
CFP	Contention-Free Period	无竞争周期
CID	Cluster Identifier	簇标识
CLH	Cluster Head	簇头
Coordinator	A full function device that accepts associations and transmits beacons	一个接受关联并传输信标的全功能设备
CRC	Cyclic Redundancy Check	循环冗余校验
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance	避免冲突的载波侦听多路存取
CW	Contention Window	竞争窗口（长度）
DSN	Data Sequence Number	数据序号
DSSS	Direct Sequence Spread Spectrum	直接序列扩频

ED	Energy Detection	能量检测
FCF	Frame Control Field	帧控制域
FCS	Frame Check Squence	帧校验序列
FFD	Full Function Device	全功能设备
FH	Frequency Hopping	跳频
FHSS	Frenquency Hopping Spread Spectrum	跳频扩展频谱
FIFO	First In First Out	先进先出
FLI	Frame Length Indicator	帧长度指示器
GTS	Guaranteed Time Slot	确保时隙
HCL	Home Control Lighting	家庭控制照明
IEEE	Institute of Electrical and Electronics Engineers	电气和电子工程学会
IF	Intermediate Frequency	中频
IFS	InterFrame Spacing	帧间隔
IB	Information Base	信息库
ISM	Industrial，Scientific and Medical	工业、科学和医学
KVP	Key-Value Pair	键值对
LIFS	Long Interframe Spacing	长帧间隔
LLC	Logical Link Control	逻辑链路控制
LPDU	LLC Protocol Data Unit	LLC 协议数据单元
LQ	Link Quality	链路质量
LQI	Link Quality Indication	链路质量指示
LR-WPAN	Low-Rate Wireless Personal Area Network	低速无线个域网
LSB	Least Significant Bit/Byte	最低有效位/字节
MAC	Medium Access Control	媒体存取控制
MCPS	MAC Common Part Sublayer	MAC 公共部分子层
MCPS-SAP	MAC Common Part Sublayer - Service Access Point	MAC 公共部分子层-服务访问点
MFR	MAC Footer	MAC 帧尾
MHR	MAC Header	MAC 帧头
MIC	Message integrity code	消息完整性检测码
MLME	MAC Sublayer Management Entity(management interface)	MAC 子层管理实体（管理接口）
MLME-SAP	MAC Sublayer Management Entity - Service Access Point	MAC 子层管理实体-服务访问点
MPDU	MAC Protocol Data Unit	MAC 协议数据单元
MSG	Message Service Type	消息服务类型
MSB	Most Significant Bit/Byte	最高有效位/字节
MSDU	MAC Service Data Unit	MAC 服务数据单元
NB	Number of Backoff(periods)	退避（周期）数
NBDT	Network Broadcast Delivery Time	网络广播发送时间
NHLE	Next Higher Layer Entity	下一个更高层实体
NIB	Network layer Information Base	网络层信息库
NLDE	Network Layer Data Entity	网络层数据实体

NLDE-SAP	Network Layer Data Entity - Service Access Point	网络层数据实体-服务访问点
NLME	Network Layer Management Entity	网络层管理实体
NLME-SAP	Network Layer Management Entity - Service Access Point	网络层管理实体-服务访问点
NPDU	Network Layer Protocol Data Unit	网络层协议数据单元
NSDU	Network Layer Service Data Unit	网络层服务数据单元
NWK	Network	网络
OFB	Output Feedback(encryption)	输出反馈（加密）
O-QPSK	Offset-Quadrature Phase Shift Keying	偏移正交相移键控
OSI	Open Systems Interconnection	开放系统互连
PAN	Personal Area Network	个域网
PD-SAP	PHY layer Data - Service Access Point	物理层数据-服务访问点
PDU	Protocol Data Unit	协议数据单元
PER	Packet Error Rate	包差错率/误帧率
PAN Coordinator	A coordinator that is the principal coordinator of a PAN	一个协调器，它是一个 PAN 的主要协调器
PHY	Physical layer	物理层
PIB	PAN Information Base	PAN 信息库
PLME	Physical layer Management Entity	物理层管理实体
PLME-SAP	Physical layer Management Entity - Service Access Point	物理层管理实体-服务访问点
POS	Personal Operating Space	个人工作空间
PPDU	PHY Protocol Data Unit	物理层协议数据单元
PSDU	PHY Service Data Unit	物理层服务数据单元
PSK	Phase Shift Keying	相位键控
PTI	Packet Trace Interface	包跟踪接口
QoS	Quality of Service	服务质量
RF	Radio Frequency	无线射频
RFD	Reduced Function Device	简化功能设备
RN	Routing Node	路由节点
RREP	Route Reply	路由应答
RREQ	Route Request	路由请求
RSSI	Received Signal Strength Indicator	接收信号强度指示
SAP	Service Access Point	服务访问点
SD	Superframe Duration	超帧周期
SDU	Service Data Unit	服务数据单元
SFD	Start of Frame Delimiter	帧开始定界符
SHR	Synchronization Header	同步头
SFS	Short InterFrame Spacing	短帧间隔
SKG	Secret Key Generation	密钥产生
SKKE	Symmetrck-Key Key Establishment	对称密钥建立
SO	Superframe Order	超帧阶数
SPDU	SSCS Protocol Data Unit	SSCS 协议数据单元

SSCS	Service Specific Convergence Sublayer	特定服务汇聚子层
SSS	Security Services Specification	安全服务规范
WLAN	Wireless Local Area Network	无线局域网
WPAN	Wireless Personal Area Network	无线个域网
ZDO	ZigBee Device Object	ZigBee 设备对象

目 录

首字母缩略词及定义.....2
第一部分 IEEE802.15.4 标准.....12
1.概述.....12
2.物理层规范.....12
2.1 物理层概述.....12
2.2 物理层服务规范.....13
2.2.1 物理层数据服务.....13
2.2.2 物理层管理服务.....14
2.3 物理层数据格式.....16
2.4 物理层的常量和属性.....16
2.52.4GHz 频段的物理层技术.....17
2.6868/915MHz 频段的物理层技术.....18
2.7 通用射频规范.....19
3.MAC 层规范.....20
3.1MAC 层服务规范.....20
3.1.1MAC 层数据服务.....20
3.1.2MAC 层管理服务.....23
3.1.2.1 关联原语 MLME-ASSOCIATE.....23
3.1.2.2 解关联原语 MLME-DISASSOCIATE.....25
3.1.2.3 信标通知原语 MLME-BEACON-NOTIFY.....27
3.1.2.4 读取属性原语 MLME-GET.....27
3.1.2.5GTS 管理原语 MLME-GTS.....28
3.1.2.6 孤立通知原语 MLME-ORPHAN.....30
3.1.2.7 复位原语 MLME-RESET.....31
3.1.2.8 接收机状态原语 MLME-RX-ENABLE.....31
3.1.2.9 信道扫描原语 MLME-SCAN.....33
3.1.2.10 通信状态原语 MLME-COMM-STATUS.....35
3.1.2.11 设置属性原语 MLME-SET.....35
3.1.2.12 更新超帧配置原语 MLME-START.....36
3.1.2.13 同步原语 MLME-SYNC.....37
3.1.2.14 失步原语 MLME-SYNC-LOSS.....37
3.1.2.15 轮询原语 MLME-POLL.....38
3.2MAC 层帧格式.....40
3.2.1MAC 帧一般格式.....40
3.2.2 特定 MAC 帧格式.....42
3.2.2.1 信标帧格式.....42
3.2.2.2 数据帧格式.....45
3.2.2.3 确认帧格式.....45
3.2.2.4 命令帧格式.....46
3.3MAC 层命令帧.....46

3.3.1 关联和解关联命令.....47
3.3.1.1 关联请求.....47
3.3.1.2 关联响应.....48
3.3.1.3 解关联通知.....48
3.3.2 协调器交互命令.....49
3.3.2.1 数据请求.....49
3.3.2.2PANID 冲突通知.....49
3.3.2.3 孤立通知.....50
3.3.2.4 信标请求.....50
3.3.2.5 协调器重排列.....50
3.3.3GTS 管理命令.....51
3.4MAC 层功能描述.....52
3.4.1 信道访问机制.....52
3.4.1.1 超帧结构.....52
3.4.1.2 帧间隔（IFS）.....53
3.4.1.3CSMA-CA 算法.....53
3.4.2PAN 的建立和运行机制.....56
3.4.2.1 信道扫描.....56
3.4.2.2PAN 标识冲突处理.....58
3.4.2.3PAN 建立.....58
3.4.2.4 信标产生.....58
3.4.2.5 设备发现.....59
3.4.3 关联和解关联.....59
3.4.3.1 关联.....59
3.4.3.2 解关联.....60
3.4.4PAN 同步机制.....61
3.4.4.1 支持信标的 PAN 同步.....61
3.4.4.2 不支持信标的 PAN 同步.....61
3.4.4.3 孤立设备重排列.....62
3.4.5 事务处理.....62
3.4.6 帧的传输.....63
3.4.6.1 发送.....63
3.4.6.2 接收和拒绝.....63
3.4.6.3 从协调器提取数据.....64
3.4.6.4 确认.....65
3.4.6.5 重传.....66
3.4.6.6 混杂模式.....66
3.4.6.7 传输可靠性情景.....66
3.4.7GTS 分配和管理.....68
3.4.7.1CAP 维护.....68
3.4.7.2GTS 分配.....68
3.4.7.3GTS 使用.....69
3.4.7.4GTS 撤销.....70

3.4.7.5GTS 重分配 70
3.4.7.6GTS 空闲判断 71
3.4.8MAC 帧的安全处理 72
3.4.8.1ACL 入口 72
3.4.8.2 不安全模式 72
3.4.8.3ACL 模式 73
3.4.8.4 安全模式 73
3.5MAC 层安全规范 75
3.5.1 安全套件构造模块 76
3.5.1.1CTR 加密模式 76
3.5.1.2CBC-MAC 认证模式 77
3.5.1.3CCM 联合加密和认证模式 78
3.5.1.4AES 加密算法 80
3.5.1.5PIB 安全材料 81
3.5.2AES-CTR 安全套件 81
3.5.2.1 数据格式 81
3.5.2.2 安全参数 82
3.5.2.3 安全操作 82
3.5.3AES-CCM 安全套件 83
3.5.3.1 数据格式 83
3.5.3.2 安全参数 83
3.5.3.3 安全操作 84
3.5.4AES-CBC-MAC 安全套件 84
3.5.4.1 数据格式 84
3.5.4.2 安全参数 85
3.5.4.3 安全操作 85
3.6MAC-PHY 信息交互流程 85
第二部分 ZigBee 协议规范 93
1.应用层规范 93
1.1 应用层规范概述 93
1.2ZigBee 应用支持子层（APS） 97
1.2.1APS 概述 97
1.2.2 服务规范 97
1.2.2.1APS 数据服务 98
1.2.2.2APS 管理服务 100
1.2.3 帧格式 102
1.2.4 常量和 PIB 属性 104
1.2.5 功能描述 104
1.2.5.1 绑定 104
1.2.5.2 发送、接收和确认 105
1.3ZigBee 应用框架 107
1.3.1 创建 ZigBee 配置文件 107
1.3.2 标准数据类型 108

1.3.3ZigBee 描述符.....110
1.3.3.1 节点描述符.....110
1.3.3.2 节点电源描述符.....111
1.3.3.3 简单描述符.....112
1.3.3.4 复杂描述符.....113
1.3.3.5 用户描述符.....113
1.3.4AF 帧格式.....114
1.3.5KVP 命令帧.....116
1.3.6AF 功能描述.....118
1.4ZigBee 设备配置文件.....118
1.4.1 设备配置文件概述.....118
1.4.2 客户端服务.....120
1.4.2.1 设备和服务发现客户端服务.....120
1.4.2.2 绑定和解绑定客户端服务.....123
1.4.2.3 网络管理客户端服务.....124
1.4.3 服务器服务.....126
1.4.3.1 设备和服务发现服务器服务.....127
1.4.3.2 绑定和解绑定服务器服务.....130
1.4.3.3 网络管理服务器服务.....131
1.5ZigBee 设备对象（ZDO）.....134
1.5.1 设备对象描述.....134
1.5.2 层接口描述.....136
1.5.3 对象定义和行为.....136
1.5.3.1 对象概述.....136
1.5.3.2 状态机功能描述.....136
1.5.3.3 设备和服务发现.....139
1.5.3.4 安全管理器.....139
1.5.3.5 绑定管理器.....140
1.5.3.6 网络管理器.....141
1.5.3.7 节点管理.....141
1.5.4 配置属性.....142
2.网络层规范.....143
2.1 网络层规范概述.....143
2.2 网络层服务规范.....144
2.2.1 网络层数据服务.....144
2.2.2 网络层管理服务.....146
2.2.2.1 网络发现.....146
2.2.2.2 网络构建.....146
2.2.2.3 允许设备入网.....148
2.2.2.4 配置 ZigBee 路由器.....148
2.2.2.5 设备入网.....149
2.2.2.6 离开网络.....151
2.2.2.7 设备复位.....152

2.2.2.8 接收机同步.....153
2.2.2.9NIB 维护.....155
2.3 网络层帧格式.....156
2.3.1NWK 帧的一般格式.....156
2.3.2 特定 NWK 帧的格式.....156
2.4 网络层命令帧.....157
2.5 网络层功能详述.....159
2.5.1 网络和设备维护.....159
2.5.1.1 创建新网络.....160
2.5.1.2 允许设备加入网络.....161
2.5.1.3 设备入网.....162
2.5.1.4 分布式地址分配机制.....168
2.5.1.5 上层地址分配机制.....169
2.5.1.6 设备离网.....170
2.5.1.7 变更 ZigBee 协调器配置.....174
2.5.1.8 设备复位.....174
2.5.2 发送和接收.....174
2.5.3 路由功能.....175
2.5.3.1 路由成本.....175
2.5.3.2 路由表.....176
2.5.3.3 基本路由算法.....177
2.5.3.4 路由发现.....179
2.5.3.5 路由维护.....183
2.5.4 信标发送时序.....184
2.5.5 广播通信.....186
2.5.6MAC 信标中的 NWK 信息.....187
3.安全服务规范.....188
3.1 安全服务规范概述.....188
3.2MAC 层安全服务.....191
3.2.1 流出 MAC 帧的安全处理.....191
3.2.2 流入 MAC 帧的安全处理.....192
3.2.3 与安全有关的 MACPIB 属性.....193
3.3NWK 层安全服务.....193
3.3.1 流出 NWK 帧的安全处理.....193
3.3.2 流入 NWK 帧的安全处理.....194
3.3.3 与安全有关的 NIB 属性.....195
3.4APS 层安全服务.....195
3.4.1 流出 APS 帧的安全处理.....195
3.4.2 流入 APS 帧的安全处理.....196
3.4.3 建立密钥服务.....197
3.4.4 传递密钥服务.....199
3.4.5 设备更新服务.....200
3.4.6 删除设备服务.....201

3.4.7 请求密钥服务.....201
3.4.8 切换密钥服务.....202
3.4.9APS 安全命令帧.....202
3.5 安全处理公共基础.....204
3.6 安全服务功能详述.....205
3.6.1 加入安全网络.....205
3.6.2 认证新入网的设备.....207
3.6.3 更新网络密钥.....210
3.6.4 恢复网络密钥.....211
3.6.5 创建端到端应用密钥.....212
3.6.6 离开网络.....214
参考文献.....216