天猫精灵蓝牙mesh软件基础规范

版本号	发布/更新日期	更新人员（部门/职位）	重要变更内容
V1.0	2018年3月16日	胡俊锋（崮德） 人工智能实验室- W实验室	初始版本
V1.1	2018年4月11日	胡俊锋（崮德） 人工智能实验室- W实验室	修改广播包时序
V1.2	2018年4月19日	胡俊锋（崮德） 人工智能实验室- W实验室	增加支持Publication和 Subscription， 修改Vendor Message的参数
V1.3	2018年4月23日	胡俊锋（崮德） 人工智能实验室- W实验室	增加NetKey、 AppKey等数量要求

V1.4	2018年6月10日	胡俊锋（崮德） 人工智能实验室- W实验室	删除Vendor Model&Message定义， 蓝牙Mesh模块串口透传部分
V1.5	2018年06月11日	童武胜（风裁） 人工智能实验室- W实验室	增加AuthValue使用SHA256的计算示例
V1.6	2018年06月13日	王森（载远） 人工智能实验室- W实验室	增加OTA章节
V1.7	2018年06月27日	童武胜（风裁） 人工智能实验室- W实验室	修改三元组计算AuthValue的描述
V1.8	2018年8月8日	人工智能实验室- W实验室- IOT技术研发中心	增加名词解释 增加场景定义 增加配网时随机数产生描述 修改语言描述 修改场景定义

1、目的

定义BLE Mesh通用模块的软件规范，指导模块厂家软件设计并接入天猫精灵。

2、BLE Mesh通用模块基本需求

使用场景：家庭，办公室，商铺，其中家庭会有3-4层别墅的情况，办公室和商铺前期考虑1000平米的环境。

使用Node数量：100个。

Feature：Relay，Proxy，Friend和Low Power。

Provisioner：天猫精灵

Server Model：Generic OnOff Server Model（开关）； Light LightnessServer Model（亮度），Light CTL Server Model（色温和亮度），Light HSL Server Model（色调、饱和度和亮度），Vendor Model，Firmware Update Server（固件升级），Object Transfer Server（对象传输）。

需要支持根据状态（开关变化、亮度变化，色温变化，色调、饱和度变化）Publication

需要支持Subscription
需要支持OTA overMesh。
支持2个NetKey，总计10个AppKey
支持Friend feature的节点支持10个Low Power节点，其中每个节点最少需要能缓存2个包的数据。

3、BLE Mesh通用模块软件规范

3.1 名词解释

三元组	阿里巴巴颁发的一组数据，包括MAC地址，Product ID，Secret，用于设备鉴权。 开发者可在天猫精灵开发者网站申请
CID	Company Identifier，公司标识符。 阿里巴巴的标识符为0x01A8

3.2 广播包

设备通过Mesh Beacon来广播信息，MeshBeacon包含两种类型：Unprovisioned Device beacon和Secure Networkbeacon，其中Unprovisioned Device Beacon是用来被Provisioner发现设备用的，包结构如下图所示。设备上电后，Unprovisioned Device Beacon每次广播时长是40ms，广播间隔是100ms，10分钟后停止广播直到下次上电后重复这个过程。

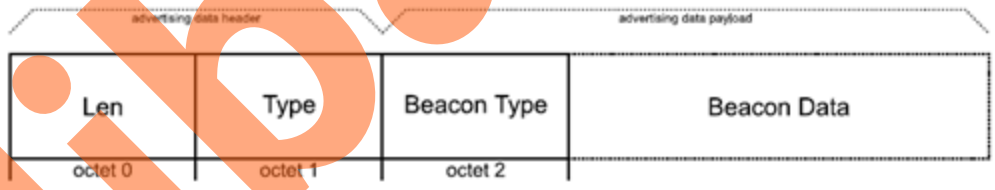

图1 Mesh Beacon广播包格式

具体字段含义如下表所示：

表1 Mesh Beacon广播包各个字段含义

Field	Size（Octets）	Notes
Len	1	长度
Type	1	0x2B
Beacon Type	1	0x00
Device UUID	16	设备UUID

OOB Information	2	bit0 Other bit1 Electronic / URI bit2 2D machine-readable code bit3 Bar code bit4 Near Field Communication (NFC) bit5 Number bit6 String bit7 Reserved for Future Use bit8 Reserved for Future Use bit9 Reserved for Future Use bit10 Reserved for Future Use bit11 On box bit12 Inside box bit13 On piece of paper bit14 Inside manual bit15 On device Default:0x0000
URI Hash	4	网址（Optional）

广播包中的关键信息是Device UUID，阿里巴巴对Device UUID的定义如下表所示，全部使用小端模式。

表2 Device UUID格式

Field	Size（Octets）	Notes
CID	2	公司ID，设置为0x01A8：Taobao

PID	1	Bit0-3蓝牙广播包版本号， 目前是0x01 bit4　　0：一型一密 　　1：一机一密， 默认是一机一密 bit5　　是否支持OTA， 默认是支持 bit6-7　　00 BLE4.0 　　01 BLE4.2 　　10 BLE5.0 　　11 BLE5.0以上 　　默认是01
ProductID	4	阿里巴巴平台颁发，一型一号
MAC地址	6	阿里巴巴平台颁发，一机一号
RFU	3	Reserved for future use

不支持PB-ADV的设备，如蓝牙4.0手机，则需要通过和节点建立GATT连接，并通过Mesh Provisioning Service通信。因此建立GATT连接之前，节点需要广播PB-GATT的广播包。综上所述，节点需要交叉广播Unprovisioned Device Beacon广播包和PB-GATT的广播包。设备上电后，PB-GATT的广播包每次广播时长是40ms，广播间隔是1s。

PB-GATT广播包结构如下图所示：

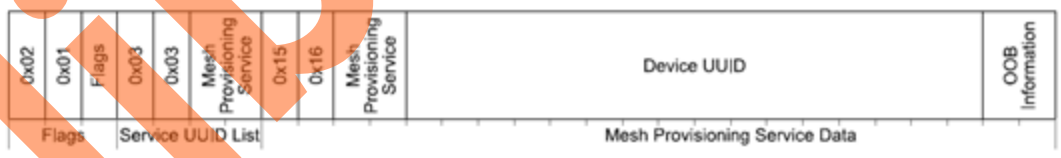

图2 PB-GATT的广播包格式

具体字段含义如下表所示：

表3 Mesh Beacon广播包各个字段含义

Field	Size（Octets）	Notes
Flags	1	长度， 0x02表示后面还有2个字节

	1	类型， 0x01表示类型是Flags（Assigned Number）
	1	Flags的值，0x02表示LE General Discoverable Mode
Service UUID List	1	长度，0x03表示后面还有3字节
	1	类型，0x03表示Complete List of 16-bit Service Class UUIDs
	2	Mesh Provisioning Service，0x1827
	1	长度， 0x15表示后面还有21字节
	1	类型，0x16表示Service Data - 16-bit UUID
	2	Mesh Provisioning Service，0x1827
Device UUID	16	设备UUID， 参考上述Unprovisioned Device beacon的广播包中的UUID字段

OOB Information	2	bit0 Other bit1 Electronic / URI bit2 2D machine-readable code bit3 Bar code bit4 Near Field Communication (NFC) bit5 Number bit6 String bit7 Reserved for Future Use bit8 Reserved for Future Use bit9 Reserved for Future Use bit10 Reserved for Future Use bit11 On box bit12 Inside box bit13 On piece of paper bit14 Inside manual bit15 On device Default：0x0000

为了支持Proxy特性，需要设置节点的Proxy Feature为Enable，那么节点会广播如下图所示广播包：

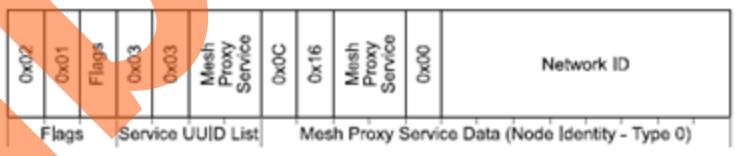

图3 Proxy的Network ID广播包

具体字段含义如下表所示：

表4 Proxy的Network ID广播包各个字段含义

Field	Size（Octets）	Notes
Flags	1	长度， 0x02表示后面还有2个字节

	1	类型， 0x01表示类型是Flags（Assigned Number）
	1	Flags的值，0x02表示LE General Discoverable Mode
Service UUID List	1	长度，0x03表示后面还有3字节
	1	类型，0x03表示Complete List of 16-bit Service Class UUIDs
	2	Mesh Proxy Service，0x1828
	1	长度， 0x0c表示后面还有12字节
	1	类型，0x16表示Service Data - 16-bit UUID
	2	Mesh Proxy Service，0x1828
Identification Type	1	实体类型，0x00表示Network ID类型
Network ID	8	参考蓝牙Mesh协议， Network ID = k3(NetKey)

如果节点属于多个网络，则需要交叉广播相应网络的Network ID包。Network ID包每次广播时长是40ms，广播间隔是1s。

为了支持Proxy特性，且节点的Proxy Feature设置为Enable，节点还会在以下两种情况下广播Node Identity包：

1、节点通过PB-GATT入网后立即开始广播，每次广播时长是40ms，广播间隔是2s。

2、节点在Configuration阶段设置Node Identity State是Enable的时候立即开始连续广播，60秒后停止广播。

Node Identity广播包如下图所示：

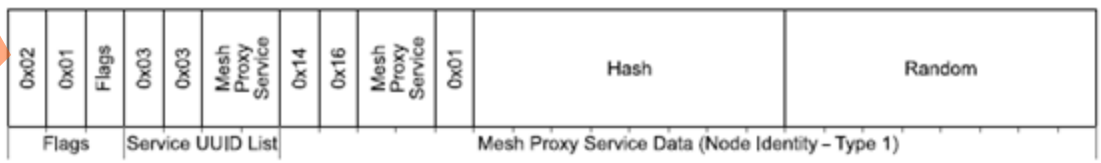

图4 Proxy的Node Identity广播包

具体字段含义如下表所示：

表5 Proxy的Node Identity广播包各个字段含义

Field	Size（Octets）	Notes
Flags	1	长度， 0x02表示后面还有2个字节
	1	类型， 0x01表示类型是Flags（Assigned Number）
	1	Flags的值，0x02表示LE General Discoverable Mode
Service UUID List	1	长度，0x03表示后面还有3字节
	1	类型，0x03表示Complete List of 16-bit Service Class UUIDs
	2	Mesh Proxy Service，0x1828
	1	长度， 0x14表示后面还有20字节
	1	类型，0x16表示Service Data - 16-bit UUID
	2	Mesh Proxy Service，0x1828
Identification Type	1	实体类型，0x01表示Node Identity类型
Hash	8	参考蓝牙Mesh协议， Hash =e(IdentityKey, Padding | Random | Address) mod 264
Random	8	随机数

3.3 蓝牙Mesh设备注册流程-Mesh1.0标准协议

Mesh设备注册流程遵循蓝牙Mesh标准的Provisioning流程，其中几个使用自定义数据的步骤描述如下：

1、Provisioning Capabilities阶段

Mesh设备在Provisioning Capabilities阶段提供OOB方式，选用Static OOB方式，其中的AuthValue= SHA256(Product ID，MAC，Secret)。即：将ProductID，MAC，Secret三元组通过字符串用英文逗号连接，然后进行SHA256摘要计算，取前16字节。其中的Secret使用一机一密的方式，需要阿里云端产生Product ID+MAC<->Secret对应表，并通过安全方式发送给模块生产工厂，由他们的生产工具读取后，把Product ID+MAC和Secret写入模块相应地址。

表6 SHA256计算示例

数据字段	数据格式与示例	计算使用的输入字符串
Product ID	十进制数值：168930， 对应十六进制数值：0x293e2	”000293e2”
英文逗号	英文逗号：”,”	”,”
Mac Address	”AB:CD:F0:F1:F2:F3” (扫描到的蓝牙设备MAC地址)	”abcdf0f1f2f3”
英文逗号	英文逗号：”,”	”,”
Secret	”53daed805bc534a4a93c825ed20a7063”	”53daed805bc534a4a93c825ed20a7063”
连接后字符串形式	”000293e2,abcdf0f1f2f3,53daed805bc534a4a93c825ed20a7063”	
SHA256结果输出(HEX)	c1 c7 67 41 55 32 36 fb 7d a0 a5 86 e6 22 98 c2 31 da c2 88 5e 73 5f eb a6 b8 b441 7c 7d 9e 72	
SHA256结果前16字节(HEX)	c1 c7 67 41 55 32 36 fb 7d a0 a5 86 e6 22 98 c2	

2、Provisioning Confirmation

这个阶段，Provisioner和Mesh设备会使用之前提到的StaticOOB来做认证确认，如果Provisioner和Mesh设备两边计算得到的Confirmation值不相同，则认证失败，结束流程。**注意：SIG mesh协议在此阶段中有一个步骤是设备端生成一个随机数并发送给天猫精灵，天猫精灵会把这个随机数发送给云端鉴权，云端会保存设备端每次发送的随机数，如果设备端发送的随机数是之前使用过的，则云端将会拒绝该设备配网，所以务必保证每次生成的随机数都不重复。**

3、Provisioning Data阶段

天猫精灵在Provisioningdata阶段给设备配置NetKey（128bits）和Unicast address（16bits）等，如下图所示。其中NetKey目前每个天猫精灵账号一个NetKey，维护一张主网。后续扩展再考虑子网的NetKey。Unicast address可以本地维护一个从0x0002开始的局域地址。当然天猫精灵自己默认有一个Unicast address（0x0001）。

Field	Size (octets)	Notes
Network Key	16	NetKey
Key Index	2	Index of the NetKey
Flags	1	Flags bitmask
IV Index	4	Current value of the IV Index
Unicast Address	2	Unicast address of the primary element

图 5Provisioning data格式

蓝牙Mesh设备入网时，需要启用Attention Timer，设置该值为3秒，也就是设备（比如灯）会以1Hz的频率闪烁3下（0.8秒/次），每次闪烁需要发送信息给天猫精灵，需要定义一个Publish过程。

3.4 mesh数据发送和接收

为了保证天猫精灵能够收到设备端发送的mesh数据，非LPN节点设备在需要向天猫精灵端发送unsegment mesh数据包时，每个数据包需要持续发送10ms，然后开启scan窗口进行监听，如果收到天猫精灵的ack，则完成数据包发送动作，否则在400ms之后进行重发，一共发送6次，最后一次发送数据后的scan窗口为1s。

3.5 蓝牙mesh模块支持场景列表

蓝牙mesh模块需要支持scene model，天猫精灵可以通过设置Scene Number让设备端调用预存的配置状态来让设备快速进入特定状态，Scene Number是一个uint16的值，总共可以储存65535种状态。常用操作有Scene Store和Scene Recall。以下是阿里巴巴定义的scene number所代表的模式。

表6 Scene Index

Scene Number	模式名称	模式内容
0x0000	保留	
0x0001	默认模式	厂商默认状态
0x0002	自动模式	有自动模式设备设置为自动模式
0x0003	阅读模式	
0x0004	影院模式	
0x0005	温暖模式	
0x0006	夜灯模式	
0x0007	助眠模式	

0x0008	起床模式	
0x0009	制冷模式	
0x000A	制热模式	
0x000B	通风模式	
0x000C	送风模式	
0x000D	除湿模式	
0x000E	睡眠模式	
0x000F	生活模式	
0x0010	手动模式	
0x0011	静音模式	
0x0012	省电模式	
0x0013	正常风模式	
0x0014	自然风模式	
0x0015	睡眠风模式	
0x0016	静音风模式	
0x0017	舒适风模式	
0x0018	宝宝风模式	
0x0019	棉织物模式	
0x001A	化纤模式	
0x001B	羊毛模式	
0x001C	除菌模式	
0x001D	筒清洁模式	
0x001E	丝绸模式	
0x001F	假日模式	
0x0020	智能模式	

0x0021	音乐模式	
0x0022	零重力模式	
0x0023	止鼾模式	
0x0024	多人模式	
0x0025	摇摆模式	
0x0026	强效模式	
0x0027	普通模式	
0x0028	工作模式	
0x0029	速冷模式	
0x002A	速冻模式	
0x002B	微干模式	
0x002C	全干模式	
0x002D	超干模式	
0x002E	夏季模式	
0x002F	冬季模式	
0x0030	标准模式	
0x0031	快洗模式	
0x0032	婴童洗模式	
0x0033	单脱水模式	
0x0034	节能洗模式	
0x0035	智能光感模式	
0x0036	学习模式	
0x0037	睡前模式	
0x0038	护眼智能感光模式	
0x0039	护眼模式	

0x0040~0xFFFF	待定	

3.6 恢复出厂设置

当需要恢复模块出厂设置的时候（比如移除一个Node），可以通过Config Node Reset的软复位的方法来移除Node（天猫精灵在移除Node后需要做Key Refresh），也可以通过硬复位的方法实现，比如灯的恢复出厂设置步骤如下：

1、 上电，立刻断电(1.5秒内);
2、 上电，立刻断电(1.5秒内);
3、 上电，立刻断电(1.5秒内);
4、 上电，立刻断电(1.5秒内);
5、 上电，立刻断电(1.5秒内);
6、 上电，灯会以1Hz的频率闪烁3下，表示完成了硬复位，恢复出厂设置（驱动软件需要调用擦除Flash和SoftReset的API实现）。

3.7 OTA升级

模块在这个链路中扮演updating节点，负责接收天猫精灵的OTA升级请求,并完成版本的更新。模块只需要实现两个model，Firmware Update Server和Object Transfer Server。

1、协商流程

OTA升级时，天猫精灵首先会从模组端读取CID，Firmware ID，进行比较，确认是否进行OTA升级。它的结构如下：

表 7固件信息的消息格式

Field	Size (bytes)	Notes
Company ID	2	Company identifier
Firmware ID	1+N	Unique firmware identifier
Update URL	N	URL for update source (optional)

这里CID填0x01A8，FirmwareID为模组自定义，默认为4个字节，Update URL 填0。

天猫精灵需要获取模块的最大传输能力。模组需要回传自己的传输能力，每个block最大支持4096个字节，最大支持16个chunk,每个chunk包含256个字节。

2、传输流程

首先天猫精灵开启block传输，确认block状态。然后开启chunk传输，每个block传输后，会检查模组端block有没有完整的传输，重传丢失的chunk。

3、断点续传

模组端接受到的版本数据建议按页写入到flash中，不建议过多的缓存buffer中，防止模组意外掉电时保存的数据丢失，下次发起OTA升级时，相应的数据还要重传，加重网络负担。

4、更新检查

a、每个块传输完成后，模组需要计算校验CRC32，等待天猫精灵查看,如果连续固件更新检查请求均未收到反馈，则认为该模块已经掉电，不再对该模块进行OTA升级。

b、所有的固件传输完毕后，模组端需要生成校验和，等待天猫精灵校验。

5、静默升级

版本传输成功后，模块不允许自动切换版本，需要等待天猫精灵下发切换版本命令。

注意：如需了解OTA升级具体实现方式，请向蓝牙mesh芯片原厂或代理商索取该平台OTA升级标准文档。