ZigBee大容量Mesh组网技术研究

ZigBee作为一种低速短距离无线通信技术，由于其网络可以便捷地进行无线数据传输功能，在物联网领域具有非常强的可应用性。但是目前各ZigBee芯片内部资源有限，实际的组网能力远远小于理论值，大规模组网的需要ZigBee网络能支持更多的路由和终端节点。以zstack为基础，分析了组网容量受限原因，并提出了提升的解决方案。

刘卿[1] 李祯祥[1] 王秋英[2] 孙超[2]/1. 国网天津电科院 2. 烟台东方瑞创达电子科技有限公司

刘卿／高级工程师

关键词/Keywords

ZigBee ·

zstack ·

Mesh组网 ·

ZigBee大容量组网 ·

1 标准协议网络容量的局限性

1.1 ZigBee大规模组网的应用场景

ZigBee是基于IEEE 802.15.4标准的低功耗局域网协议。有近距离、低复杂度、自组织、低功耗、低数据速率、低成本的特点。目前各芯片的ZigBee解决方案，多是面向智能家居控制的应用，这样的网络通常网络规模较小，另外，受限于ZigBee无线芯片片上资源的限制，ZigBee实际的组网能力要远远小于它的理论值。但是现在越来越多的场合需要能支持ZigBee大规模组网的应用场景，需要的终端节点或者路由节点数目很多，远远超过了几百上千的规模。

1.2 ZigBee组网容量受限原因

按照ZigBee网络层协议的标准，网络内的各个节点的网络地址用一个2字节的数据来表示，即整个网络内的节点数量可以达到65 500个以上，但实际情况却并非如此。以TI的ZigBee无线芯片CC2530为例，CC2530片内的RAM空间只有4 K大小，除去os，ZigBee协议栈，以及应用程序占用的RAM空间，留给存放路由表和邻居表的空间已经所剩无几。在CC2530对应的ZigBee协议栈中，定义的NWK_MAX_DEVICE_LIST值为20，NWK_MAX_ROUTERS值为6，即一台路由设备只能带最多20个子设备，而且这20个子设备中最多只能有6个是路由设备。如此推算，用CC2530 搭建一个ZigBee网络，所支持的路由节点数量不过几十个，标签也不过几百个，这在智能家居控制的场合或许还能适用，但在需要支持上万个网络节点的工业级网络中就不再适用。

现在市面上上推出的高性能的ZigBee无线芯片，虽然在片上资源（如RAM容量等）有所提升，但也不是解决问题的根本办法。

下面以TI的标准ZigBee Pro协议栈ZStack-CC2530-2.5.1a为例说明改进方法。

2 终端节点容量扩展方法

2.1 标准协议中对终端节点的处理

（1）终端节点如何加入网络

对于终端节点，上电的时候，会发送一个beacon request的数据包，来探测周围的ZigBee网络，如图1所示。

如果存在ZigBee网络，则会由网络

P.nbr.	Time (us)	Length	Frame control field					Sequence number	Dest. PAN	Dest. Address	Beacon request	LQI	FCS
			Type	Sec	Pnd	Ack.req	PAN_compr						
RX	+1017614		CMD	0	0	0	0						
4	=7023375	10						0x5F	0xFFFF	0xFFFF		216	OK

图1 beacon request数据色

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

中的路由设备负责跟终端节点交换MAC地址并分配网络短地址给终端节点。此时终端节点加入了ZigBee网络。

终端节点加入网络后，会定时发送一个data request的数据包来询问自己的父设备，是否有发给自己的数据，这里要注意的是，由于终端节点是要求低功耗设计的，所以其大多数时间处于休眠状态，所以发送给终端节点的数据不能由其父设备实时地发送出去，要等到终端节点唤醒后，主动向父设备索取。data request数据包如图2所示。

data request数据包是需要ACK应答帧的，

P.nbr.	Time (us)	Length	Frame control field					Sequence number	Dest. PAN	Dest. Address	Source Address	Data request	LQI	FCS
			Type	Sec	Pnd	Ack.req	PAN_compr							
RX	+1004739		CMD	0	0	1	1	0x59	0x0000	0x0000	0x6210		216	OK
15	=6034068	12												

P.nbr.	Time (us)	Length	Frame control field					Sequence number	LQI	FCS
			Type	Sec	Pnd	Ack.req	PAN_compr			
RX	+768		ACK	0	0	0	0	0x59	228	OK
16	=6034836	5								

图2　data request数据色

标签以此判断自己是否丢失了父设备，如果data request数据包连续2次没有得到父设备的应答，则标签认为自己丢失了父设备，继续发送beacon request数据包来寻找父设备。

（2）路由节点如何管理其下的终端节点

网络中的终端节点只能通过其父设备来与网络中的其他节点通信，终端节点的父设备只能是路由节点，路由节点中通过关联表和邻居表来存放子节点的信息：

具体到ZigBee协议栈中关联表定义如下：

```
typedef struct
{
 UINT16 shortAddr;
 uint16 addrIdx;
 byte nodeRelation;
 byte devStatus;
 byte assocCnt;
 byte age;
 linkInfo_t linkInfo;
} associated_devices_t;
```

邻居表定义如下：

```
typedef struct
{
 uint16  neighborAddress;
 uint8   neighborExtAddr[Z_EXTADDR_LEN];
 uint16  panId;
 uint8   age;
 linkInfo_t linkInfo;
} neighborEntry_t;
```

路由节点的关联表和邻居表中会记录其下终端节点的长短地址信息和其他网络参数信息。并通过这两个表来动态维护挂在它下面的子节点。

2.2 几种终端节点容量扩展方法

受限于处理器内部RAM空间所限，CC2530实际的组网能力要远小于理论值。几种终端节点容量扩展方法为：

1）通过扩展CC2530的内存容量来扩展网络容量。这种方法很难操作，因为CC2530并没有将内部的系统总线引脚引出。

2）将协议栈中耗内存较大的各种关联表和邻居表存放到flash中，以达到节省RAM空间的方法。理论上可行，但是目前商用ZigBee协议栈大都不开源，修改难度较大。

3）本文的方法，不需要硬件做改动，只需要在深入理解zstack的基础上，对协议栈进行改进就能使支持的节点数量达到理论值。

2.3 协议栈改进对大容量终端节点的支持

（1）终端节点上行数据通信链路改进

终端节点只存放自己父设备节点的网络信息，终端节点在向其他网络节点发送信息的时候，它先发送到他的父设备，然后父设备转发。

终端节点的父设备，由于RAM空间的限制，其关联表和邻居表的容量有限，如果只是终端节点上传数据，并不会用到关联表和邻居表的路由信息，所以针对终端节点上行数据的情况，路由节点只要在邻居表中去掉终端节点的路由信息就可以了，即路由节点内并不保存终端节点的路由信息。

在路由节点收到终端节点的数据包后，要执

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

行TagNeighborClear_Progress来将邻居表中关于此终端节点的路由信息删除。

（2）终端节点下行数据通信链路改进

由于上面在路由节点中将子节点的路由信息删除了，所以其他节点的信息如果想发送到该子节点，就会因为找不到该子节点的路由信息而导致发送失败。

1）bitMap表。本文采用一种bitMap的方法，在每个路由节点中存放一张bitMap表，表中每一个bit代表一个终端节点的地址。其他节点在向某个终端节点发送数据的时候，先要遍历一遍所有路由节点的bitMap表，以此来确定目的终端节点的父设备是哪个路由节点。

这样只要把要发送的信息发送给这个路由节点，在目标终端节点唤醒的时候，就会发送data request包从该路由节点把数据取走。

2）bitMap表的生成。为了节省RAM空间，bitMap存放在CC2530的内部flash中，假设网络中有10 000个终端节点，这样就需要（10 000/8 = 1 250）个字节，共分成10组，每组125个字节，这样终端节点的网络地址按照顺序分配地址，与bitMap中的bit位一一对应，其他节点在遍历各个路由节点的bitMap表的时候，可以根据终端节点的网络地址取bitMap表中的一段，不必10段地址都遍历一遍，节省无线带宽资源。

3 路由节点容量扩展方法

3.1 标准协议中对路由节点的处理

在每个路由加入网络之前，寻址方案需要知道和配置一些参数。这些参数是MAX_DEPTH，MAX_ROUTERS和MAX_CHILDREN。这些参数是栈配置的一部分。MAX_DEPTH决定了网络的最大深度。协调器(Coordinator)位于深度0，其子节点深度1，孙节点深度2，以此类推。MAX_DEPTH参数限制了网络在物理上的长度。MAX_CHILDREN决定了一个路由(Router)或者一个协调器节点可以处理的子节点的最大个数。MAX_ROUTER决定了一个路由(Router)或者一个协调器(Coordinator)节点可以处理的具有路由功能的子节点的最大个数。这个参数是MAX_CHILDREN的一个子集。

路由通过请求/响应信息包被发现。一个源设备要寻找一个目的地址，通过发送一个广播路由请求（RREQ）信息到它的邻设备请求一个路由。当一个节点接收到一个RREQ信息时，它将依次转播这个RREQ信息。但是在进行之前，它更新RREQ信息的消耗域，并附加上自己所在的链接消耗。这样，RREQ信息将携带向前传输的所有的连接消耗。这个重复过程直到RREQ到达目的设备。在这个寻找路由的过程中会有其他RREQ信息经过不同的路径重复到达目的设备。该目的设备选择最好的RREQ信息并发送一个路由答复（RREP）返回到源设备。

3.2 标准协议中路由节点数量受限原因

依然是受限于CC2530内部RAM空间的限制，存不了过多数量的路由表。当路由节点内部的路由条目使用完之后，网络外的其他路由将不能成功加入到网络中去。

3.3 协议栈改进对大容量路由节点的支持

（1）AODV路由算法

ZigBee执行的路由协议是基于AODV（Ad hoc On demand Distance Vector）的路由协议。作为一个简单的应用——传感器网络，AODV支持环境中的移动节点、连接失败和丢包功能。

AODV路由算法依靠路由路径上的所有路由节点建立和维护的动态路由表，AODV是一种按需路由协议，那些不在路径内的路由节点并不保存路由信息，也不参与维护动态路由表。路由发现主要由正向路由表建立和反向路由表建立两部分组成。

但是由于资源有限，路由节点中存放的路由表条目有限，若网络中路由节点数目过多，会导致发起寻找路由失败。

（2）改进的AODV路由算法

为了支持更大容量的路由节点，在网络层自己实现组网协议，即自己实现AODV路由算法，并根据实际的应用需求进行适当改进，改进主要在如下几个方面：

1）采用改进的静态路由模式，自组网协议不再自动维护路由表（当某个路由节点丢失链接的

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

时候，不再通知其他路由删除无效的路由条目，也不会重新建立新的路由条目），取而代之的是在发送数据的时候，实时产生新的路由表（因为250 KB/s的带宽足以应对大多数的组网需求，并不会产生不可接受的网络延迟）。

2）路由节点内的路由条目采用分时复用的策略，当路由节点内的路由表条目满的时候，再有新的寻找路由出现的时候，按照先进先出的原则删除路由表内老的路由条目并重新执行发现路由命令，将新的路由信息填入路由表。

4 结束语

本文针对路由节点数目大、终端多的场景。常见的解决方案多是基于WIFI的，但成本较高；ZigBee的成本低，但是单个组网容量有限，在很多应用中有很大的局限性。本文针对具体的项目需求，分别从支持的终端节点数量和路由节点数量两方面对ZigBee协议栈zstack进行了深入分析，并提供相应的改进措施实现ZigBee大容量组网。

参考文献

[1] 王中生，曹琦. 基于ZigBee技术的无线定位研究与实现[J]. 计算机技术与发展, 2010(12).

[2] 王玉柱，郑文岭，马文丽，等. 基于ZigBee的医院病人追踪定位系统设计[J]. 微计算机信息, 2010(2).

[3] 王立波，陈慈发. CC2431的室内定位系统设计[J]. 单片机与嵌入式系统应用, 2008(9).

[4] 金纯，蒋小宇，罗祖秋. ZigBee与蓝牙的分析与比较[J]. 信息技术与标准化, 2004(6).

[5] 江修波. ZigBee技术及其应用[J]. 低压电器, 2005(7).

作者简介

刘卿（1980-），男，高级工程师，主要从事电能计量专业技术管理工作。

（收稿日期：2015-12-10）EA

（编辑：鞠佳）

（上接第681页）

所有的场景展现与功能实施，都是基于一套完整的三维生产线模型。为了和真实现场相吻合，三维生产线模型的制作首先要与静态的真实生产线一致，同时涉及到的设备动作也要与真实情况相符。而且，仿真三维模型属于实时渲染场景，要求具有最少的多边形模型与最优化的细节效果，对三维制作提出更高的要求，如图8所示。

为了保证系统的高实时性、高可靠性，让系统始终处于合理的负荷状态是非常重要的。保证每个三维模型最精简、最优化是三维仿真实时渲染的流畅性、实时性最重要的前提。

5 结束语

在四线一库三维仿真系统中，制作了一个与四线一库实际运行环境完全一致的虚拟仿真环境，为四线一库运行监控提供了直观可靠的技术方案，便于监控人员掌握设备运行中的状态数据和需要关注的业务数据。

参考文献

[1] 张燕，黄金娟. 电能表智能化检定流水线系统的研究与应用[J]. 电测与仪表, 2009(12): 74-77.

[2] 陈宏敏，等. 基于实时测控数据驱动的航天可视化仿真系统[J]. 系统仿真学报, 2008(增刊1): 268-272.

[3] 王兴建，葛良全，刘思颂. 基于Virtools的高级交互式虚拟现实模型库的建立[J]. 2008, 34(6): 17-22.

[4] 张雪鹏，陈国华，等. 基于3D的虚拟运动仿真平台设计及Virtools功能实现[J]. 北京化工大学学报:自然科学版, 2009, 36(4): 93-95.

[5] 孙倩. 基于3DS+MAX的三维建模及其在Virtools环境中的应用[J]. 中国科技信息, 2008(12): 94-95.

作者简介

安泰（1981-），男，工程师，主要研究方向为电力自动化、用电信息采集、电力器具计量。

龙孔操（1984-），男，系统集成项目管理师，主要研究方向为计量用电、软件开发。

（收稿日期：2015-12-10）EA

（编辑：鞠佳）

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net