

DOI:10.3969/j.issn.1673-4785.201107001

网络出版地址: <http://www.cnki.net/kcms/detail/23.1538.TP.20120210.1640.001.html>

## ZigBee 簇状网的 OMNeT ++ 仿真模型

牟杰, 蔡自兴, 刘丽珏

(中南大学 信息科学与工程学院, 湖南 长沙 410083)

**摘要:** 最新版的 ZigBee 2007 协议规范允许在一个网络中部署 64 000 个节点以上, 但目前市场和技术尚未完全成熟, 国内仍无大规模节点部署的实例. 为了给大规模部署 ZigBee 节点的研究提供参考模型, 通过 OMNeT ++ 仿真环境, 围绕 ZigBee 2007 协议中定义的网络结构及 AODV 路由算法进行了大规模节点的组网和路由仿真. 仿真实验表明, 该模型具有 ZigBee 2007 网络层和介质访问控制层的组网和路由功能, 成功实现了大规模节点的自组网和数据传输, 可用于大规模部署 ZigBee 节点的可行性研究.

**关键词:** ZigBee; OMNeT ++ ; AODV; 大规模节点网络; 仿真模型

**中图分类号:** TP393 **文献标志码:** A **文章编号:** 1673-4785(2012)01-0056-05

## A simulation of the ZigBee cluster-tree network in OMNeT ++

MOU Jie, CAI Zixing, LIU Lijue

(Institute of Information Science and Engineering, Central South University, Changsha 410083, China)

**Abstract:** ZigBee 2007 offers full wireless mesh networking capable of supporting more than 64,000 devices on a single wireless sensor network. Due to immature markets and technology, a deployment with hundreds of thousands of nodes does not exist at present. By using the OMNeT ++ simulation IDE, a simulation model of a large-scale network according to the ZigBee 2007 protocol was created which aimed at providing a reference model for deploying a large-scale sensor network. The model implemented the networking and routing functions of the network layer and medium access control layer according to the ZigBee 2007 protocol, and successfully established an ad-hoc network while transmitting data internally. For these reasons, it can be used for the study of deploying a large-scale ZigBee network.

**Keywords:** ZigBee; OMNeT ++ ; AODV; large-scale network; simulation model

无线传感器网络, 尤其是成百上千个节点的网络研究必须依赖于仿真模型. 通常, 仿真模型要尽可能接近实际情况, 同时易于修改和扩展. 文献[1]针对少数节点的星型无线传感器网络进行了仿真建模, 文献[2]建立的模型使用全局拓扑结构控制和 GEAR 路由. 前者不符合大规模网络的要求, 后者不符合外设资源有限的无线传感器节点网络的实际情况. 文献[3]基于 Worldsens 的一部分 WSN 建立了大规模节点模型 XS-WSN, 但是 Worldsens 扩展性能不理想. 文献[4]基于 TinyOS 的仿真组件 TOSSIM

建立了一个具有能量约束的分布式仿真模型, 根据文献[5]对仿真工具的对比分析, TOSSIM 的使用比较复杂并且仅适用于 MICA 节点平台, 不利于后续的开发. 文献[5-6]均指出 OMNeT ++ 是一款流行的、扩展性能极好且运行效率高的网络仿真工具. 故基于文献[5-6]的分析, 本文使用 OMNeT ++ 仿真工具, 根据最新的无线传感器网络协议 ZigBee 2007 建立一个大规模节点网络的仿真模型, 该模型具有自组网和点对点路由功能, 基于模块和面向对象的设计便于后续开发者使用, 为研究现实中部署大规模传感器节点, 如土地监测等应用, 提供可靠的参考模型.

收稿日期: 2011-07-03. 网络出版时间: 2012-02-10.

基金项目: 国家自然科学基金资助项目(90820302, 61175064).

通信作者: 牟杰. E-mail: JoeccMou@csu.edu.cn.

## 1 OMNeT++ 简介

OMNeT++ 是一个优秀的网络仿真 IDE (integrated development environment), 其开发界面类似于开发 JAVA 常用的 ECLIPSE, 平台使用 C++ 和 NED (network description) 作为开发语言. NED 语言用于定义一个模块, 通过几个简单的向导例子就能轻松掌握. 模块分为简单模块和组合模块, 简单模块的功能由用户的 C++ 代码实现, 组合模块由简单模块组合而成.

OMNeT++ 是基于离散事件驱动的, 一个事件即一个消息, 仿真中的节点在接收到消息后进行相关操作, 当整个网络中不再有消息传递时仿真停止运行. OMNeT++ 中的图形接口称为 Tkenv, 它可以出色地显示网络连接的各种事件和状态 (比如收发消息、节点之间的连接状态等), 并能对事件及数据进行记录和统计.

## 2 通信协议简介

IEEE 802.15.4-2003 协议<sup>[7]</sup>将设备分为全功能设备 (full-function device, FFD) 和简单功能设备 (reduced-function device, RFD), 全功能设备根据在网络中的角色又可分为网络协调器 (personal area network coordinator, PAN coordinator) 和协调器 (coordinator). 在 IEEE 802.15.4-2003 标准中, 簇状网是一个多子网 (cluster, 也称为簇) 构成的网络, 如图 1 所示. 图 1 中的连线表示父设备与子设备的关系, 不表示信息流. 每个子网呈树形展开, 由一个簇头 (cluster head) 负责与其他子网通信和维护本子网通信. 簇头在子网内的 16 bit 短地址 (short address) 为 0, 在子网内的其他设备的短地址由簇头分配.

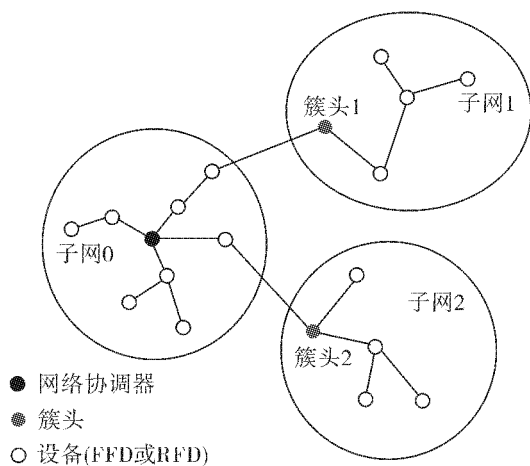


图1 IEEE 802.15.4-2003 定义的簇状网

Fig.1 Cluster-tree network defined by IEEE 802.15.4-2003

ZigBee 协议<sup>[8]</sup>是 ZigBee 联盟根据 IEEE 802.15.4-2003 标准制订的低速率、低功耗、全双工的无线通信协议, 最新的 ZigBee 2007 (下文均称为 ZigBee Specification) 是目前惟一获得 ZigBee 联盟董事会许可的版本.

ZigBee Specification 将设备分为协调器 (ZigBee coordinator)、路由器 (ZigBee router) 和终端设备 (ZigBee enddevice). ZigBee 协调器即 IEEE 802.15.4-2003 的网络协调器, ZigBee 路由器即 IEEE 802.15.4-2003 的路由器, ZigBee 协调器和 ZigBee 路由器都是全功能设备, 两者的角色是可以互相转换的. ZigBee 终端设备即 IEEE 802.15.4-2003 的简单功能设备, 简单功能设备之间不能直接进行通信, 要通过其父节点 (全功能设备) 进行通信. ZigBee Specification 描述的通信过程不涉及网间通信, 即 ZigBee 网络仅仅描述图 1 中网络协调器所在的子网而不涉及其他子网.

在本文中, ZigBee 簇状网指 ZigBee Specification 中的对等网络 (mesh network), 把每个路由器及其子设备看成一个簇, 如图 2 所示.

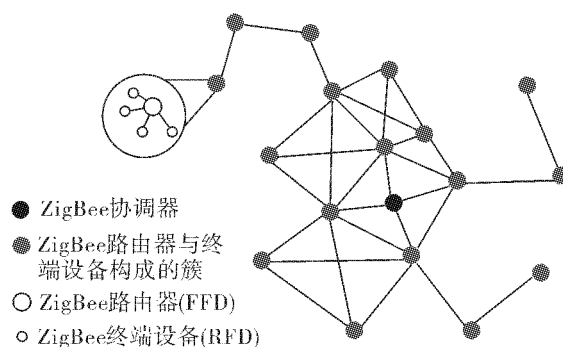


图2 ZigBee Specification 定义的对等网络

Fig.2 Mesh network defined by ZigBee Specification

## 3 ZigBee 簇状网的仿真模型设计

本模型设计的主要目的是实现大规模 ZigBee 节点的自组网和点对点路由, 为研究 ZigBee 节点部署提供参考依据, 故模型包含了介质访问控制层和网络层的组网和点对点路由功能, 如图 3 所示, 应用层仅用于产生净载荷.

通常, 建立模型前需要提出一些假设条件, 本模型做如下假设: 1) 信道是无损、无延迟的理想信道; 2) 鉴于 ZigBee 路由器与 ZigBee 协调器的角色可以相互转换, 认为所有 ZigBee 路由器都可作为潜在的 ZigBee 协调器, 模型中不单独设计 ZigBee 协调器; 3) 网内通信使用 16 bit 短地址, 且短地址为静态分配, 使用 OMNeT++ 给模块分配的 ID 号作为短地

址;4)广播消息不设置重发.在以上假设条件下,仿真模型设计如下.

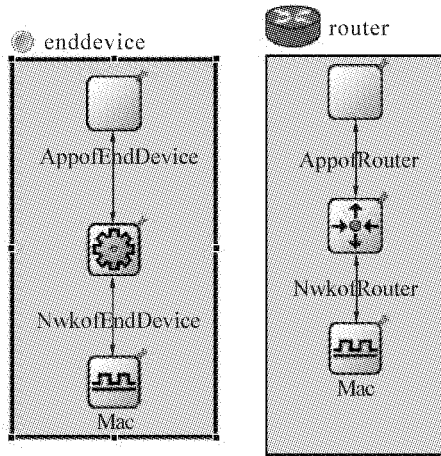


图3 ZigBee 节点模型

Fig.3 Node model of ZigBee

### 3.1 参数

网络节点个数可以选取任意值,出于仿真时间成本的考虑,总共使用500个节点,具体网络参数见表1.

表1 网络关键参数

Table 1 Parameters of the network

参数名	值
数据传输速率/(Kbit · s <sup>-1</sup> )	250
MAC 应答等待时间/ms	4.08
路由发现等待时间/s	10
应用层发送数据间隔/s	10
节点通信半径 <sup>[9]</sup> /m	100
ZigBee 路由器的个数	100
ZigBee 终端设备的个数	400

### 3.2 帧格式

关于帧格式的细节请查阅文献[8-9],本文对帧格式做了适当简化:数据包(packet)包括MAC层帧头(如表2所示)和网络层消息.网络层消息有4种,包括连接请求消息、连接确认消息、路由请求消息和路由应答消息,网络层消息由网络层帧头和网络层载荷组成,如表3~7所示.

表2 MAC层帧头

Table 2 MAC header

数据类型	域名	含义
uint8	frameType	帧类型
bool	ackRequest	是否需要应答
uint8	sequenceNumber	帧序号
uint16	sourceAddress	MAC 源地址
uint16	destinationAddress	MAC 目的地址

表3 网络层帧头

Table 3 NWK header

数据类型	域名	含义
uint8	frameType	帧类型
uint8	sequenceNumber	帧序号
uint16	sourceAddress	NWK 源地址
uint16	destinationAddress	NWK 目的地址

表4 连接请求消息的网络层载荷

Table 4 Payload field of the connection request command

数据类型	域名	含义
uint8	commandFrameID	命令 ID
uint8	deviceType	设备类型

表5 连接确认消息的网络层载荷

Table 5 Payload field of the connection confirm command

数据类型	域名	含义
uint8	commandFrameID	命令 ID
bool	isSuccess	是否成功连接

表6 路由请求消息的网络层载荷

Table 6 Payload field of the routing request command

数据类型	域名	含义
uint8	commandFrameID	命令 ID
uint8	routeRequestID	路由请求 ID
uint16	destAddress	请求的目的地址
uint8	pathcost	代价

表7 路由应答消息的网络层载荷

Table 7 Payload field of the routing reply command

数据类型	域名	含义
uint8	commandFrameID	命令 ID
uint8	routeRequestID	路由请求 ID
uint16	originatorAddress	请求的源地址
uint16	responderAddress	应答地址
uint8	pathCost	代价

### 3.3 自组网

由文献[8]得知2.4GHz ZigBee 模块 CC2430 的传输距离约为100 m.组网过程中,ZigBee 终端设备向其通信半径内最近的 ZigBee 路由器发出连接请求,ZigBee 路由器之间也互相发送连接请求,请求成功后相互将对方添加到自己的邻居表中.网络节点随机均匀分布在750 m × 750 m 的区域内,连接过程可用伪代码表示为:

```

if Router(1) 与 Router(2) 的距离 < 通信距离,
    Router(1) < - - > Router(2) (同级, sibling);
if (EndDevice(1) 与 Router(1) 的距离 < 通信距离
    && Router(1) 的邻居表未满),
    EndDevice(1) < - - > Router(1) (Router(1)
    是 EndDevice(1) 的父节点).
  
```

这里需要说明的是,“< - - >”在 NED 语言中表示 2 个门(gates)之间互连,门即消息传递的接口。

3.4 路由算法

ZigBee 协议规范使用的路由算法是经典的 AODV(Ad hoc on-demand distance vector)算法<sup>[10]</sup>,该算法依赖于 2 个表——路由发现表(route discovery table)和路由表(route table),分别如表 8~9 所示。

表 8 路由发现表

Table 8 Route discovery table

数据类型	域名
uint8	routeRequestID
uint16	sourceAddress
uint16	senderAddress
uint16	forwardCost
uint16	residualCost
double	expiredTime

表 9 路由表

Table 9 Route table

数据类型	域名
uint8	status
uint16	nextHopAddress
uint16	destAddress

启动路由发现后,ZigBee 路由器向通信距离内的其他路由器广播路由请求,发起或转播路由请求的 ZigBee 路由器均建立以上 2 个表.其中路由发现表记录了路由请求 ID、发起路由的源地址、转发路由请求节点的地址、前向代价(路由请求消息中的 pathCost)、后向代价(路由应答消息中的 pathCost)以及路由发现超时时间.路由表中记录了路由请求的目的地址、路由的下一跳地址和路由状态。

当先后抵达 ZigBee 路由器的 2 个路由请求的 routeRequestID 和 sourceAddress 均相同时,路由器只转播前向代价最小的请求,同时更新路由发现表.当多个路由请求均指向同一个目的地址时,路由器在其路由表中仅建立一个与目的地址相应的记录,同时在其路由发现表中建立几个不同的路由请求记录,如图 4 所示。

当目的节点接收到路由请求,它就给发送路由请求的邻居回发一个路由应答.在接收到路由应答后,ZigBee 路由器更新路由表的 nextHopAddress,使之成为最小后向代价的应答消息的发送者.最后,从路由表中的 nextHopAddress 可确定一条从路由源地址到目的地址的代价最小路径。

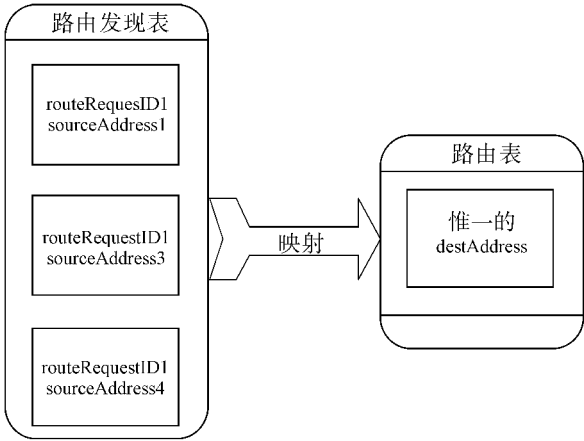


图 4 路由发现表与路由表的对应关系

Fig. 4 The relationship between route discovery table and route table

3.5 净载荷(goodput)

组网完成后,在终端设备上每 10 s 随机产生一个地址,若该地址与自己的地址相同,则终端设备生成一个数据包(data),并随机挑选一个 ZigBee 路由器作为目的节点。

4 仿真结果

ZigBee 簇状网的局部网络放大后如图 5 所示,图中连线表示 2 个设备成功连接,end 表示 enddevice,rte 表示 router。

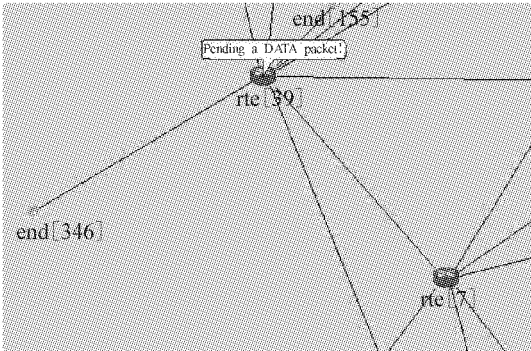


图 5 路由器将终端设备的数据包暂存

Fig. 5 The data packet temporary storage in routers

图 5 中,end[346]要给 rte[84]发送 1 个数据包,先将数据包发给其父节点 rte[39],由于 rte[39]不是数据包的目的节点,目的节点 rte[84]不是 rte[39]的邻居,并且 rte[39]没有 rte[84]的相应路由记录,所以 rte[39]只能将数据包暂存并为该数据包寻找路由。

当 rte[39]成功收到路由应答后,它先更新路由表,然后从数据队列中取出数据包,将数据包的目的地址与路由表中的目的地址比对,若相同且路由表状态为 ACTIVE,则将数据包发给路由表中 nextHopAddress 对应的邻居.邻居继续沿路由表中对应的 nextHopAddress 转发下去,最后 rte[84]成功接收到

end[346]发给它的数据包,如图6所示。

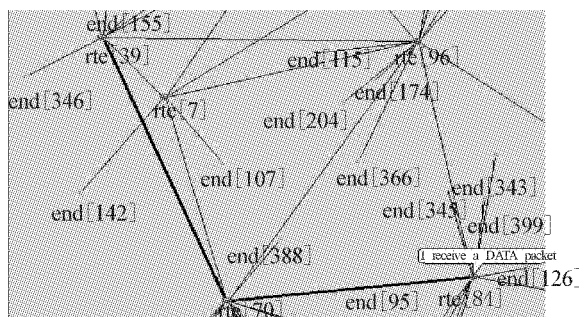


图6 数据包成功路由到目的地址

Fig.6 The data packet has been successfully routed to its destination

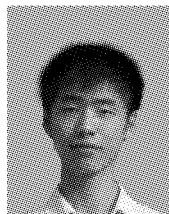
## 5 结束语

为研究大规模无线传感器网络的部署提供参考,通过分析 IEEE 802.15.4 和 ZigBee2007 协议,运用开源、构件化、面向对象设计的网络仿真工具 OM-NeT++ 建立了大规模 ZigBee 节点的网络仿真模型。仿真结果表明,该模型具有大规模节点的自组网和路由功能,为研究现实中部署 ZigBee 节点提供了可靠友好的仿真环境。后续的工作可以分3个方向:1)继续完善本模型,如增加节点移动性能,改进信道模型,增加传感模块和能量模块等,实现网络覆盖、能量效率、安全加密等功能,以满足部署 ZigBee 节点的研究需要;2)加入不同的无线传感器通信协议,比较不同协议之间的性能;3)基于不同的仿真工具开发仿真模型,比较各个模型的性能,为不同的应用场合提供量材定制的仿真环境。

## 参考文献:

- [1] FENG Chen, FALKO D. A simulation model of IEEE 802.15.4 in OMNeT++ [C]//Proceedings of the 6th GI/ITG KuVS Fachgesprach Drahtlose Sensornetze. Aachen, Germany, 2007: 35-38.
- [2] CHEN Jiming, ZHANG Jianhui, XU Weiqiang, et al. The development of a realistic simulation framework with OMNeT++ [C]//Second International Conference on Future Generation Communication and Networking. Sanya, China, 2008: 497-500.
- [3] ALI A, SEBASTIEN T. XS-WSNet: extreme scale wireless sensor network simulation [C]//2010 IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks. Montreal, Canada, 2010: 1-9.
- [4] MINA J, JAE C. SWARM-eTOSSIM: a simulator for distributed energy-constrained tiny devices [C]//2011 Tenth International Symposium on Autonomous Decentralized Systems. Kobe, Japan, 2011: 17-24.
- [5] MUHAMMAD Z, BOB A, FAYCAL B, et al. Limitations of simulation tools for large-scale wireless sensor networks [C]//2011 Workshops of International Conference on Advanced Information Networking and Applications. Singapore, 2011: 820-825.
- [6] EYANGELIA K, VASSILIOS V. Assessment of network simulators for real world WSNs in forest environments [C]//2011 International Conference on Networking, Sensing and Control. Delft, Netherlands, 2011: 427-432.
- [7] LAN/MAN Standards Committee of the IEEE Computer Society. SS95127 Part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANS) [S]. New York, USA: The Institute of Electrical and Electronics Engineers Inc, 2003: 29-160.
- [8] ZigBee-Alliance. ZigBee specification; document 053474r17 [S]. San Ramon, CA, USA: ZigBee-Alliance Inc, 2008: 259-418.
- [9] 郭宏福, 白丽娜, 郭志华. 2.4 GHz Zigbee 数传模块传输距离的估算方法[J]. 西安电子科技大学学报, 2009, 36(4): 691-695.  
GUO Hongfu, BAI Li'na, GUO Zhihua. Estimation method for the transmission distance for the 2.4 GHz Zigbee application[J]. Journal of Xidian University, 2009, 36(4): 691-695.
- [10] CHARLES E, ELIZABETH M. Ad-hoc on-demand distance vector routing [C]//Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications. New Orleans, USA, 1999: 90-100.

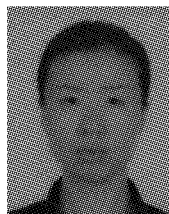
### 作者简介:



牟杰,男,1987年生,硕士研究生,主要研究方向为无线传感器网络。



蔡自兴,男,1938年生,教授,博士生导师,首届国家级教学名师奖、宝钢教育基金优秀教师特等奖和徐特立教育奖获得者,国际导航与运动控制科学院院士、纽约科学院院士,任中国人工智能学会第5届理事会副理事长及智能机器人专业委员会主任、中国自动化学会理事、中国计算机学会模式识别与人工智能专委会委员等。主要研究方向为智能系统、人工智能、智能控制、智能机器人等。主持并完成包括国家自然科学基金重点项目在内的科教研究项目30余项,其中获国际奖励2项、国家级奖励2项、省部级等奖励15项。发表学术论文660余篇,出版专著、教材32部。



刘丽珏,女,1973年生,副教授,主要研究方向为人工智能、智能计算、传感器网络、多机器人等。