· 电网技术 ·

一种基于 ZigBee 无线传感网络的智能抄表系统

金 萍[1], 田正其[1],彭宇菲[2]
(1.国网江苏省电力公司电力科学研究院,江苏 南京 211103;2.南京师范大学,江苏 南京 210023)

摘 要:目前解决电力公司能源供应和需求平衡的方案,以此控制电能的消耗都是基于经验。因为缺乏详细的用户消费记录,从而无法根据历史需求来预测控制电网将来的消费。基于无线传感器网络的智能抄表系统,整个网络是无线通信完成的,近距离短通过 ZigBee 网络,数据安全,用户节点扩展性强。实例模型表明,合理的容量规划,能实现远程对用户电表的自动、实时监测。这样准确记录和备份实时相关数据,减少纸质单据材料消耗,统计分析住户耗电数据,提高管理效率,为电网电能传输和能源节约提供依据。

关键词:无线传感网络;ZigBee;智能抄表;扩展性;远程监测
中图分类号:TM925 **文献标志码**:A **文章编号**:1009-0665(2016)04-0036-04

最早传统住宅仪表读数的方法,需要公司员工每一、两个月在用户面前直观地读取相应数据,来为用户或客户进行服务。一个足够大的系统阅读数量可以达到成千上万甚至上百万。近来,虽然许多通过使用无线设备抄表,解决了人工读数的弊端,但这些都是一天或者更长时间传送一次数据[1],并不能根据一天中凹凸不平的用户消费曲线,来调整供电方案[2,3]。这样供应和需求之间差异,增加了运营成本和电网管理的复杂性。

近年来随着技术更新, 新的通信系统进入市场。无线网络也不例外,并且这些技术将更多地出现在人们现实生活中。本文提供了一个执行远程电表读数平台,大大提高自动化水平,减少物业管理人员,降低运营支出。抄表平台运用无线网络进行访问时,不需要在用户周围部署昂贵的有线基础设施,大大降低资源消耗,无线传感器网络(WSN)作为无线网络的一种,对于长距离路径通信时具有很好的优势,相对于其他无线网络(GPRS,WiMAX,ADSL)将会更合适[4,5]。

1 平台的构建

基于人工完成读数,公司可以负责测量用户在一段时间内的能源消耗量,但是这种方法需要很大的人力,要求员工多次执行任务。自动抄表 (AMR)技术就是使电气公司执行远程抄表,不需要派遣员工到用户家中。

通过引入的 WSN,开发一个分布式和自动化流程执行读数。可以极大地改进电气公司和最终用户相关成本。具有一定优势:(1) 在低需求期鼓励用户使用电能;(2) 不再需要发送数量巨大的员工在客户处进行读数, 减少运营支出;(3) 公司能够给客户基于平台在线提供新的服务。

收稿日期:2016-03-14;修回日期:2016-04-29

1.1 特点和要求

基于无线传感器网络应用技术以及组网一系列相关具体特点与优势,实现不同情况下相应功能,从而满足用户和电力公司的需要。

1.1.1 应用要求

(1) 节点识别。必须正确识别网络中端点,并关联到一个特定的用户。

(2) 节点移动。这是一般无线传感器网络的一个非常重要的特征。此情况下一般是不相关的,实际案例中大多数是端点不动情形。

(3) 能源消耗和电池寿命。这是对无线传感器网络的能源供给要求,特别是单元电池的供电寿命。

(4) 可扩展性。在未来,随着用户数目的增加,很可能有新的端点将加入网络。因此应考虑在不需要执行特定技术改变设计的情况下,自动地扩大网络、优化网络。

(5) 可靠性。这是 AMR 平台的主要特征。当网络受到攻击或意外掉网, 必须保证数据信息不会丢失或篡改。

1.1.2 技术要求

(1) 识别设备。基于 ZigBee 技术的无线终端,有 2 种可能的设备地址:64 位 MAC 预编码地址和 16 位网络地址。其中第一个是惟一的,通常当作一个设备加入 ZigBee 网络。第二个是一个很短的地址,用来进行网络路由。

(2) 网络规模。ZigBee 网络的大小,理论上是有确定的 16 位地址限制。然而, 由于物理限制, 该网络(ZigBee)设备最大数量是 100,是一个小得多的量。

(3) 传感器。传感器通过串行接口与电表连接,无线设备内置于电表表内,从而减少装置的所占空间。

(4) 协调器限制。设计中一个集线器最多只能与四个协调器直接连接。

1.2 构架

众多高楼和房屋的城市密集建筑区，相邻的 2 个建筑都是不同的,每个房子都有一个电表读取电度数。仪表的位置取决于房子装饰类型，大部分安装于房子的外面。通过无线接口连接到一个叫集线器的专用设备,然后集线器将用户电表信息传给电力公司服务器。如图 1 所示,将整个路径分为两段,从端点到集线器作为短距离段,从集线器到管理服务器作为长距离段,整个网络包括 4 个部分,每个部分彼此间相互联系,分别扮演着不同的角色,组合完成自动抄表整个过程。

(1) 端点。作为网络基础成员,实现了用户定点的物理逻辑转换,从而与用户电表进行数据的现场交互。

(2) 协调器。负责 ZigBee 网络协调,给结点成员按照一定规则分配网络地址，负责创建并维护一个局域网并实现路由功能。

(3) 集线器。负责收集和汇总几个 ZigBee 网络内所有端点信息。为端点和服务器平台的通讯,提供逻辑接口。

(4) 管理服务器。作为服务器平台,负责储存结点电表数据,进行历史数据查询,报表和曲线分析,电力公司实现智能化管理的数据平台。

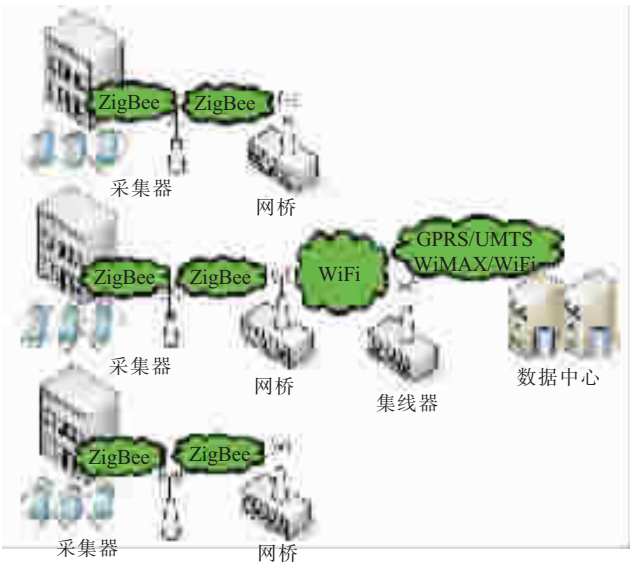

图 1 智能抄表系统平台

短距离段通常对应于一个或多个 ZigBee 网络,通过串行或通过 WiFi 直接连接到一个集线器。集线器收集所有区域内电表数据，再通过长距离段将数据反馈给服务器。ZigBee 是一种低成本、低功耗的无线技术,在定位和流量使用上非常适合这个网络要求。若集线器距离 ZigBee 网络终端较远时，可以用 WiFi 来实现集线器与 ZigBee 网络终端间的数据传递。

长距离段是集线器与服务器之间数据桥梁，一般可由 GPRS ,UMTS, WiFi,WiMAX 通信技术组成。它将所有电表信息汇总,传给管理服务器。

当然目前还有一些其他的通信方式来实现上述数据的传递[7],比如在短距离段用 PLC(线载通信)代替 ZigBee,或使用 GPRS 直接连接到每个电表端点。直接使用 GPRS 连接每一电表端点，特别是规模宏大的电表用户时成本比较高[8]。PLC 具有一定带宽的限制使用不够灵活[9]。同时还需要有线来支持,材料使用和改造及其不方便。本智能抄表系统平台使用灵活,只要接口统一,管理软件适应,不仅能够完成电表的远程自动抄表,还可以用于其他公用事业,如暖、气、水表的自动抄表等。

2 组网关键

要能够成功地获得所有的电表读数，并能使系统的成本、可靠性、可扩展性和其他都具有相对的优越性。关键主要集中在 3 个方面:

(1) 传感器的识别是否正确。让管理服务器能正确识别到每一个网络节点。

(2) 网络是否安全。建立一定的认证机制,确保数据保密、完整、可利用。

(3) 容量规划是否合理，根据网络规模设计一定数量的集线器、协调器、传感器等。

2.1 传感器的识别和寻址及命名

大规模的抄表系统，面对的是几十万或者是百万用户电表,因此必须要建立一个对应关系。使得用户电表与数据储存地址一一对应。16 位寻址的 ZigBee 技术空间上还是不够的,为了解决上述问题。ZigBee 协调器通过动态分配网络地址给设备，使用长 64 位的 MAC 地址来标识每一个结点。当对每一个传感器结点进行访问时,ZigBee 通过搜索所有路径，分析它们的位置关系以及远近，然后选择其中的一条路径与该传感器结点进行数据传输。当一条路径发生拥挤或者是断开时,立刻分析下一条路径,直到搜索到相应的传感器结点。

这种搜索的方法存在一些潜在的问题，随着网络规模的增大,数据访问效率会降低。每次管理服务器要与客户结点建立联络时，它首先必须查阅数据库获取相应设备的 MAC 地址。这样当管理平台为了与某个电表建立联系,首先必须发送请求到每一个集线器,一旦一个集线器接收请求时，通过与相应协调器的接口建立连接获得 MAC 地址。相反，使用 MAC 地址在 ZigBee 网络中轮流搜索相应设备。这样增加了搜索过程的复杂性。

为解决上述问题，提出基于 IP 的虚拟网络地址,主要思想是建立一个完整的 IP 网络,通过不同的网段来有针对性地访问各个传感器的结点，从而节省搜索时间。

2.2 网络和数据的安全

该 AMR 平台主要是基于无线网络，这种网络与有线网络相比面临诸多漏洞[10]。比如只要范围内和知道传输频率的任何人都可以直接访问网络，从而形成攻击，常见的攻击类型有：(1) 拒绝服务造成干扰，利用在无线网络中特别是 ZigBee 和 WiFi 网络，CSMA/CA 协议(载波侦听多路访问/碰撞检测)的脆弱性[11]；(2) 攻击数据保密性；(3) 重复攻击；(4) 取代端点。

在自动抄表的背景下，取代的端点是最有可能发生的攻击，因此必须建立一定的认证机制，来确保数据的保密性、完整性、可利用性。

2.2.1 短距离段的认证

短距离段的通信一般是 ZigBee 或 WiFi 网络。ZigBee 技术在数据加密过程中，可以使用 3 种基本密钥，分别是主密钥、链接密钥和网络密钥[12]。主密钥是 2 个设备长期安全通信的基础，也可以作为一般的链接密钥使用。所以必须维护主密钥的保密性和正确性。当在网络传输过程中，采用主密钥可以阻止窃听[13]。在 CCM* (counter with cipher block chain-ing-message authentication code) 加密模式下执 AES-128 加密算法，保证了通信的安全。在这种模式下，所有的信息都是加密的，2 个点之间的握手，是建立在由一个主密钥生成的点对点之间。提供了加密、数据完整性检查和鉴权功能，有较高的安全性，同时避免了内部攻击[14]。

当使用 WiFi 时，可以利用目前被认为是安全的 WiFi 安全标准 802.11i(WPA/WPA2)与 802.1x 认证(EAP)[15]，为加强其安全性，还可以考虑多种机制。

(1) IPSec VPN：用以提供公用和专用网络的端对端加密和验证。

(2) MAC 地址过滤：只有经过授权的设备允许访问网络，有效控制用户上网权限。

(3) 隐藏：隐藏访问接入点。

2.2.2 长距离段的认证

这段通信主要考虑用 GPRS/UMTS 和 WiFi/WiMAX 单一或联合网络来实现。目前这段网络上的安全性基本上被认为是安全的。如 WiFi 网络认证可考虑以 802.11i(WPA2)和 802.1x(EAP)为标准认证，WiMAX 网络认证以 EAP 和 PKMv2 802.16g 为标准认证[16]。

2.3 网络容量规划

网络容量规划，根据网络实际的限制和约束，合理地规划设备数量、带宽、网段，使系统在最佳条件下工作，设计过程中主要考虑的参数有节点数、ZigBee 协调器数、集线器数、在每一个网络段的表数、每一个 ZigBee 网络节点的最大数量、电表数目、采样时间间隔等。在实际情况下，合理配置上述参数，对网络的稳定、有效性具有一定的意义。当然还要结合其他参数，如与建筑物间距离，地区通信条件和信号覆盖等环境条件限制情况等。

3 实例分析

根据本文第二章节分析，具体设计了一个例子，通过举例来合理配置相关参数，以求达到最优。如图 2 所示。5 栋住户电表中，其中 4 栋楼住户电表采用 WiFi 连接到一个集线器，第 5 栋楼住户假设距离其他楼宇较远，因此电表通过串口直接连接到另一个集线器。一个电表数据最多占有 60 个字节，包括标题和安全冗余部分。绘制成表格如表 1 所示。计算出端点、协调器、网桥、集线器数目如表 2 所示。

图 2 方案示例

表 1 案列参数

参数	数目
楼宇	5
楼层	8
单元数	6
楼间距离 /m	<30
楼房与服务器间距离 /km	5
ZigBee 网络最大节点数 / 个	50
集线器 ZigBee 接口数 / 个	4
电表数据长 / bytes	60
电表固件升级空间 / kb	60
数据更新时间 / min	15

表 2 设备数统计 个

参数	数目
端点	240
协调器	5
网桥数	4
集线器	2

3.1 识别和寻址

该系统由 240 用户构成，每个用户构成一个节点，共计240 个节点，因此要惟一地识别这 240 个节点，并将节点对应于一个客户。由于网络节点数目不是很大，在这里只需要使用虚拟 IP，C 类 IPv4 网络就足够了。但必须考虑到它的可扩展性，地址分配成如表 3 所示。

表 3 节点地址

网络参数	集线器 1	集线器 2
网段	192.168.1.0	192.168.2.0
IP 地址	192.168.1.1	192.168.2.1
网桥地址范围	192.168.1.10-192.168.1.20	—
端节点地址范围	192.168.1.128-192.168.1.254	192.168.2.128-192.168.2.254

当服务器平台需要对端点进行访问时,它只需要知道节点的 IP 地址, 并自动请求到相应的集线器,再通过网关将地址解析, 并将请求发送到相应的协调器。协调器再连接到惟一的一个端点,完成一次寻址,并对节点进行识别。

3.2 容量规划

在表 2 中, 已经计算出总节点数,ZigBee 协调器总数、集线器总数。现在来计算下每个设备的处理信息量,如表 4 所示。最终得出通信链路的容量要求,从而为电表读数和设备更新服务。

表 4 通过网络的每一单元流量统计

网络设备	电表读数	固化升级
端点	60 bytes	60 kb
协调器	3 kb	3 Mb
网桥	3 kb	60 kb
集线器 1	2.88 kb	60 kb
集线器 2	11.5 kb	240 kb
管理服务器	14.38 kb	120 kb

假设协调器和网桥有一个平均的处理能力,也就是说不管它们是单独工作还是在集线器下协同工作,处理信息量相同。本设计适应于一个分布式的网络,当在设备更新时,只需向集线器发送一次请求,再由设备负责发送必要的副本到每个端点, 完成升级功能。本系统网络简单,信息量也不是很大,但它反映了一个组网的模型, 如果要对一个中等城市进行组网,甚至更大,大约两百万电表。通过这种方式组网,大约需要 10 个集线器,每一个管理 12 kb,管理服务器只需要 120 Mb,带宽不受限制。

4 结束语

本文提出了一种基于无线传感网络技术建立大规模智能抄表系统平台。通过对平台组网结构、容量规划、安全与扩展性进行分析。能够有助解决电力公司发展复杂的计费方案,建立灵活、更有效管理模式。组网过程中,传感器将电表数据采集后通过 ZigBee 网络将数据传递给协调器,协调器再将数据传递给集线器,再通过远距离段无线技术,如 WiFi,WiMAX,3G,GPRS 将数据传到数据中心, 形成一个完整的远程自动抄表系统。平台通过虚拟 IP 地址方法,实现对每一传感器结点进行访问,解决端点惟一识别问题,同时还可以扩展成其他公共事业使用,如水或煤气等表的远程读数,可以与传感器网络集成结合使用。因此扩展性强,数据实时安全、可靠。

参考文献:

[1] 钱立军,李新家. 用电信息采集系统中数据比对功能的实现及应用[J]. 江苏电机工程,2013,32(2):64-65.

[2] 于海斌,梁 伟,曾 鹏,等. 智能无线传感器网络系统[M]. 北京:科学出版社,2006:5-37.

[3] 林 涛,郭 晓,陈 恩,等. 基于 Si4432 和 GPRS 远程智能抄表系统的研究[J]. 自动化仪表,2014(7):31-34.

[4] 金海红. 基于 ZigBee 的无线传感器网络节点的设计及其通信的研究[D]. 合肥:合肥工业大学硕士论文,2007.

[5] YAO C C, TING Y C, WEI C W, et al. Dynamic Software Update Model for Remote Entity Management of Machine-to-machine Service Capability[C]. IET Communications 2013(7):2-9.

[6] SIVANEASAN B, SO P L, GUNAWAN E. Modeling and Performance Analysis of Automatic Meter Reading Systems Using Power Line Communications[C]. Presented at the 11th IEEE Singapore International Conference on Communication Systems, 2008. ICCS 2008, Guangzhou; 2008.

[7] 刘 颖. 基于 ZigBee 和 GPRS 的远程无线抄表系统设计与实现[J]. 科学技术与工程,2012,30(12):8058-8062.

[8] GONG X. Realization and Application of Serial Communication in VS 2008[J]. Computer &Telecommunication, 2011,02(15):33-38.

[9] 成小良,邓志东. 基于 ZigBee 规范构建大规模无线传感器网络[J]. 通信学报,2008,29(11):158-164.

[10] LI C, ZHANG J. Research of ZigBee's Data Security and Protection[J]. International Forum on Computer Science Technology and Applications, 2009(9):298-302.

[11] 任秀丽,于海斌. 基于 ZigBee 技术的无线传感网的安全分析[J]. 计算机科学,2006,33(10):111-113.

[12] 彭 瑜. 低功耗、低成本、高可靠性、低复杂度的无线电通信协议 Zigbee[J]. 自动化仪表,2005,05(26):1-4.

[13] 杨 斌. 基于 TC 和 AES 的 ZigBee 标准安全性分析[J]. 计算机工程与设计,2010,31(11):2439-2441.

[14] ZigBee Alliance document[EB/OL]. http://www. zigbee. Org.

[15] AKYILDIZ L, SU W, SANKARASUBRAMANIAM Y, et al. A Surveyon Sensor Networks [J]. IEEE Communications Magazine, 2002,40(8):102-114.

[16] LI C, ZHANG J. Research of ZigBee's Data Security and Protection[J]. International Forum on Computer Science Technology and Applications, 2009(9):298-302.

作者简介:

金 萍(1968),女,江苏徐州人,高级工程师,研究方向为电能计量技术;

田正其(1987),男,江苏南通人,工程师,研究方向为电能计量技术;

彭宇菲(1995),女,江苏南京人,本科大三在读。

(下转第 43 页)

参考文献:

[1] 王梅义. 大电网事故分析与技术应用[M]. 北京:中国电力出版社,2008: 27-34.

[2] 葛 乐,杨志超,胡 波,等. 面向复杂工况的输电线路本体结构安全评价[J]. 电力系统自动化,2013,37(20):108-113.

[3] 杨万里,鲍务均,龙小乐. 输电杆塔结构的非线性有限元设计分析[J]. 湖北电力,1999,23(1):25-27.

[4] 喻明志,龙小乐,鲍务均. 输电杆塔结构受力线性及非线性设计分析[J]. 山东电力技术,1998,18(2):39-41.

[5] 李英明,韩 军,刘立平. ANSYS 在砌体结构非线性有限元分析中的应用研究[J]. 重庆建筑大学学报,2006,28(5):90-96.

[6] 施 刚,石永久,王元清. 钢框架梁柱端板连接的非线性有限元分析[J]. 工程力学,2008,25(12):79-85.

[7] 丁 薇,谭向宇. 基于有限元分析的悬式绝缘子串电场仿真 [J]. 云南电力技术,2015,43(2):11-13.

[8] 陈剑宇,刘文懋. 基于有限元法的超大型间接式冷却塔结构参数分析计算[J]. 内蒙古电力技术,2015,33(2):57-60.

[9] 陈 祺,王新芳. 输电铁塔 ANSYS 建模及有限元分析[J]. 山西建筑,2009,35(20):60-63.

[10] 季善浩. 输电铁塔的结构分析与管理研究[D]. 北京: 华北电力大学硕士学位论文,2011.

[11] 周新华. 高压输电铁塔结构强度分析[D]. 河北:华北电力大学硕士学位论文,2002.

[12] 杨万里,龙小乐,鲍务均. 输电杆塔的结构设计分析[J]. 武汉水利水电大学(宜昌)学报,1999,21(1):58-61.

[13] 龙述尧,刘腾喜. 计算力学[M]. 长沙:湖南大学出版社,2007: 259-263.

[14] 朱贤俊. 输电线路塔—线混合体系的动力学模型分析[J]. 江苏电机工程,2006,25(2):48-50.

[15] 任学平,高耀东. 弹性力学基础及有限单元法[M]. 内蒙古:华中科技大学出版社,2007:56-62.

[16] 孙 燕. 500 kV 输电铁塔结构的几何非线性数值模拟[D]. 河北:华北电力大学硕士学位论文,2007.

作者简介:

陆文伟(1991),男,江苏常州人,硕士研究生,研究方向为电网主设备及系统安全运行;

马寿虎(1990),男,江苏淮安人,硕士研究生,研究方向为电网主设备及系统安全运行;

葛 乐(1982),男,江苏泰州人,副教授,研究方向为电网主设备及系统安全运行、分布式能源与主动配电网;

杨志超(1960),男,江苏常州人,教授,研究方向为电力设备在线监测与状态评估、主动配电网运行与控制技术。

Research on Transmission Tower Stress Exact Distribution Based on Lagrange Interpolation Function Analysis

LU Wenwei, MA Shouhu, GE Le, YANG Zhichao

(School of Electric Power Engineering, Nanjing Institute of Technology, Nanjing 211167, China)

Abstract: Using nodes stress as maximum stress to evaluate tower component's safety is not accurate. A Lagrange interpolation function method for transmission tower stress calculation is proposed, and a power transmission tower stress calculation software is developed. Firstly, the method uses hybrid truss beam model for transmission tower, and finite element linear analysis and nonlinear finite element analysis are implemented on the structure of rigid and flexible units of tower. Then, the stress of each node is calculated, and through the Lagrange interpolation function the maximum stress can be obtained. Through the developed transmission tower stress calculation software, the process of tower accident is simulated. The simulation calculation results show that the calculation method has a high accuracy and can improve the accuracy of transmission tower structure safety assessment.

Key words: transmission tower; safety evaluation; node stress; Lagrange interpolation function; maximum stress

(上接第 39 页)

Intelligent Meter Reading System of Wireless Sensor Network Based on ZigBee

JIN Ping[1], TIAN Zhengqi[1], PENG Yufei[2]

(1.State Grid Jiangsu Electric Power Company Electric Power Research Institute, Nanjing 211103, China;

2.Nanjing Normal University, Nanjing 210023, China)

Abstract: At present, the solution to energy supply and demand balance of electric power company is based on the experience of controlling power consumption. Because of lacking detailed user consumption records, it is unable to predict the future consumption of power grid based on historical demand data. Intelligent meter reading system is based on wireless sensor network, such as short distance ZigBee network. Therefore, the system has the features of data security and user node scalability. The example model shows that the reasonable capacity planning can realize the automatic and real-time monitoring of remote user's electric meter. The accurate records and real-time data backup reduces the material consumption of paper documents, and the statistical analysis of household consumption data improves the efficiency of management and provides a valuable basis for energy saving.

Key words: wireless sensor network; ZigBee; extensibility; intelligent meter; remote monitoring