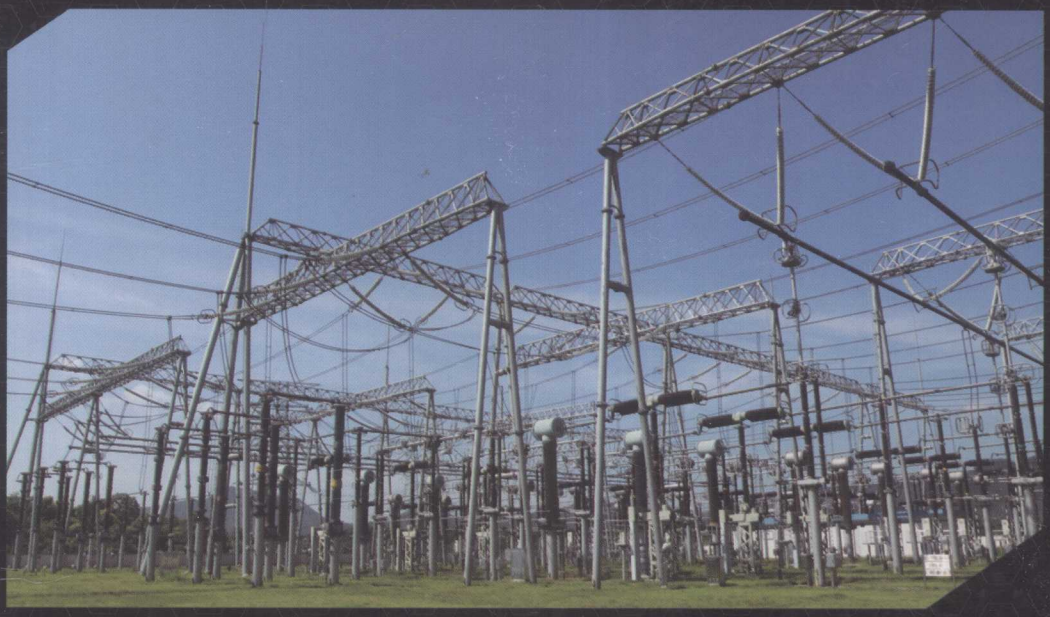
信息安全丛书

电力物联网安全技术研究

The Security in Power Internet of Things

张翼英 著



科学出版社

电力物联网安全技术研究

张翼英 著

科学出版社
北京

内 容 简 介

智能电网通过物联网感知设备（特别是无线传感器网络）获取智能电网各个环节的运行状态、环境状态和设备状态等参数。本书主要讲述了电力物联网安全技术的一些研究内容，共分为 7 章，主要包括电力物联网概述、无线传感器网络及安全概述、基于多跳模型的安全研究、基于层次模型的安全研究、基于秘密共享模式的安全研究、电力物联网安全评估、电力物联网发展及其安全趋势。

本书可以作为高等院校物联网相关专业本科生、研究生的教材，也可作为物联网、智能电网及其安全相关研究者的参考用书。

图书在版编目（CIP）数据

电力物联网安全技术研究/张翼英著. —北京：科学出版社，2016

ISBN 978-7-03-050923-9

Ⅰ. ①电… Ⅱ. ①张… Ⅲ. ①互联网络-应用-安全技术-研究②智能技术-应用-安全技术-研究 Ⅳ. ①TP393.4 ②TP18

中国版本图书馆 CIP 数据核字（2016）第 282366 号

责任编辑：赵丽欣 张瑞涛 / 责任校对：王万红

责任印制：吕春珉 / 封面设计：东方人华

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

三河市骏杰印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2016 年 11 月第 一 版 开本：787×1092 1/16

2016 年 11 月第一次印刷 印张：10

字数：237 000

定价：45.00 元

（如有印装质量问题，我社负责调换〈骏杰〉）

销售部电话 010-62136230 编辑部电话 010-62135319-2028

PREFACE

前　言

智能电网通过电力物联网部署大量智能终端、感知设备等形成感知末梢网络，紧密耦合协同互动的信息空间虚拟网络和物理空间实体网络组成二元异构复合大复杂系统。这些感知末梢网络处于信息物理耦合界面，使原本相对封闭、专业和安全的电力工控系统不断开放，管理网和生产控制网的双向信息交互成为常态，工业生产的控制权限不断上移，生产端、研发端、管理端、消费端都可以实现对底层工业系统访问，大大增加了攻击点、攻击面和信任网络边界，可以利用感知末梢节点脆弱性进行信息窃听、虚假信息注入、病毒、木马等攻击，使得安全威胁向工控领域迅速扩散。所以，为保证电力物联网数据的完整性、准确性和避免隐私泄露，都需要对数据的私密性进行保护。因此，电力物联网尤其是其中的无线传感器网络安全问题得到了广泛的重视。

密钥管理是无线传感器网络安全的基础和关键技术。有效的密钥管理机制也是路由协议、能量管理、安全定位、数据融合等协议的基础之一。本书基于输电线路在线监测、数据中心感知系统、智能变电站等无线传感器网络具体应用，对电力物联网中的无线传感器网络的安全进行深入研究，设计几个安全密钥系统，主要包括以下几个方面。

（1）针对输电线路检测等应用，基于层次型无线传感器网络架构，设计了一种新的层次型的密钥协议（Hierarchical Key Management Scheme，HKMS），参照 LEACH 等分簇算法对簇进行重新组织，依据新的跳数来生成新的密钥替换过时密钥。HKMS 具有密钥系统局域化、低能量损耗、不需要特殊节点等特点。

（2）针对数据中心等应用，基于 Splay Tree 架构，设计了实时动态密钥管理方法（Real-time Dynamic Key Management，RDKM）。利用 Splay Tree 自平衡特性，建立查找-触发式的实时密钥管理机制，实现了基于 Splay Tree 的密钥再生。

（3）针对智能变电站等应用，基于秘密共享理论，设计了一个轻量级的秘密共

享密钥管理（Secret Sharing-based Key Management，SSKM）。在 SSKM 中，将加密的秘密利用拉格朗日插值公式分成多个子秘密。通过多项式组合恢复的秘密，并获得密钥。该解决方案试图以避免对手截获足够的参数进行密码破译。

以上几方面的研究，为电力物联网中的无线传感器网络应用提供了几种可实现的轻量级安全协议，为电力物联网提供了安全保障。

由于时间仓促，作者水平有限，书中难免有错误和不足之处，敬请读者批评指正。

CONTENTS

目　录

第 1 章　电力物联网概述

智能电网是将先进的传感量测技术、信息通信技术、分析决策技术、自动控制技术和能源电力技术相结合，并与电网基础设施高度集成而形成的新型现代化电网。电力物联网通过感知技术广泛应用在智能电网中，能够有效整合通信基础设施资源和电力系统基础设施资源，使信息通信服务于电力系统运行，有效地为电网中发电、输电、变电、配电、用电、调度等环节提供重要技术支撑，提高电力系统信息化水平，从而改善现有电力系统基础设施的利用效率，促进能源的高效利用。

然而，电力物联网通过部署大量传感器、智能终端和设备，利用感知技术并以多种方式接入智能电网，会给智能电网带来新的信息安全隐患。电力通信系统出现的任何安全方面的问题都可能影响电力系统的安全、稳定、经济运行，影响电网的可靠供电，因此信息安全已成为智能电网安全稳定运行和对社会可靠供电的重要保障。

1.1　智 能 电 网

电力系统是指由发电、输电、变电、配电和用电等环节组成的电能生产与消费系统，如图 1-1 所示。为实现这一功能，电力系统在各个环节和不同层次还具有相应的信息与控制系统，对电能的生产过程进行测量、调节、控制、保护、通信和调度，以保证各类用户获得安全、经济、优质的电能。

电力的广泛应用加速了人类社会的工业化进程，随着以数字化和网络化为特征的信息时代的来临，电力系统行业正面临诸多问题和新的挑战。

（1）电力系统运行的稳定性降低。随着现代电网的快速发展以及大电网互联的逐步形成，大型电力系统及其互联在优化资源配置、提高电能质量的同时，也带来了运行的复杂性，其中稳定性降低的问题最为突出。

（2）电网利用效率不高。据美国统计资料显示，目前电网的利用系数仅为 55%，浪费了大量的固定资产投入。电力运行要求功率实时平衡的特性导致电网中大量的发输变配资产的投入仅是为了满足峰荷需求，设备利用小时数不高。

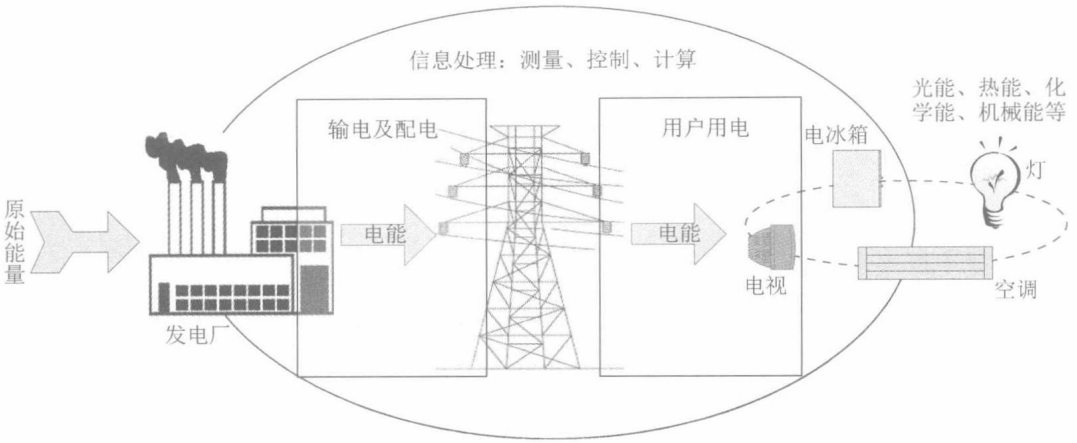


图 1-1　电力系统示意图

（3）高度信息化的需求增大。通信和信息技术的兴起，以及数字化技术在各行业的渗透普及，给电力网络的发展带来了契机，同时也对电网的供电服务质量提出了更高的要求。

（4）自动化调度的需求增加。调度是电网安全运行和资源优化配置的关键。电网层级增多，电气联系增强，电网运行特性更加复杂；同步运行的设备数量和用户数量大幅增长，交换功率容量显著提高，全局统一协调控制成为电网调度的必然，而这一目标又强烈依赖于高度信息化与自动化的技术支撑。

（5）环保与能源安全的需求。环境恶化和能源危机也给电力工业提出新的要求。有效解决风能、电能、太阳能等新型可再生能源的大规模开发、接入、远距离输送等问题，必将要求电网具备较强的兼容性和互动性。

（6）高质量及多元化的用电需求。随着生活水平的不断提高，用户对用电安全性、电能质量及电力多元化服务的需求会越来越高。然而，目前的电网状况还远未能满足人们对用电服务的期望。电网未来发展的一个方向就是通过创新的营销策略实现电网与电力用户的双向互动，引导用户主动参与市场竞争，实现有效的“需求侧响应”。

为了迎接上述电力系统面临的新挑战，解决电力系统遇到的诸多问题，全球电力企业和研究机构提出了智能电网这一概念。智能电网不是一个局部的解决方案，而是一个现代化或智能化的电力网络，是一系列能使电力网络智能化的技术的总称。

智能电网的智能化主要体现为：可观测、可控制、实时分析和决策、自适应和自愈。智能电网的实现，首先依赖于电网各个环节重要运行参数的在线监测和实时信息掌控，电力物联网作为“智能信息感知末梢”，可成为推动智能电网发展的重要

技术手段，再加上融合了传感、通信、计算机以及云计算等多种技术，从而实现信息的采集与传输、海量信息处理、智能控制以及智能辅助决策服务等功能。

其中，无线传感器网络（Wireless Sensor Network，WSN）是电力物联网主要感知部分，是智能电网的重要支撑环节，利用感知技术与智能装置对电网本身及其运行环境进行感知识别，并通过网络传输互联进行计算、处理和知识挖掘，实现人与物、物与物的信息交互和无缝链接，达到对智能电网的实时监控、精确管理和科学决策目的。

电力物联网通过无线传感器网络获取智能电网各个环节的运行状态、环境状态和设备状态等参数。然而，无线传感器网络常常工作在无人监管的区域，网络内的通信会被监听，传感器节点也非常容易被捕获、篡改和破坏，所以，保证电力物联网数据的完整性、准确性和避免隐私泄露，都需要对数据的私密性进行保护。因此，无线传感器网络的网络安全问题得到了广泛的重视。

1.2　电力物联网

电力物联网是指通过在电力系统中部署感知设备、智能终端和通信装置等，形成感知网络，实现有效的信息感知、获取和处理，经由无线或有线网络进行可靠信息传输，并对感知和获取的信息进行智能处理，实现针对性决策或精准控制的交互性网络。电力物联网在智能电网发电、输电、变电、配电、用电、调度等各个环节均有广泛应用。

智能电网的实现，首先依赖于电网各个环节重要运行参数的在线监测和实时信息掌控。电力物联网技术可有效整合电力系统基础设施资源和通信设施资源，促进先进信息通信系统服务于电力系统的运行，提高电网信息化水平和现有电力系统基础设施的利用效率，在电网建设、电网安全、生产管理、运行维护、信息采集、安全监控、计量及用户交互等方面发挥巨大作用，可以全方位提高智能电网各个环节的信息感知深度和广度，为实现电力系统的智能化以及信息流、业务流、电力流提供高可用支持。

1.2.1　电力物联网架构

与物联网架构类似，电力物联网由感知层、网络层和应用层组成，如图 1-2 所示。感知层部署在电力系统底层，实现对电力系统感知对象的智能感知识别、信息采集处理和自动控制，并通过电力专网（包括电力无线专网）、公网等通信系统组成

延伸网络，完成电力系统物理空间到网络层和应用层链接。网络层主要实现信息传递、路由和控制，包括接入网和核心网，网络层可依托公众电信网和互联网，也可以依托各行业的专用通信网络。应用层为物联网应用提供信息处理、计算等通用基础服务设施、能力及资源调用接口，以此为基础实现物联网在众多领域的应用。

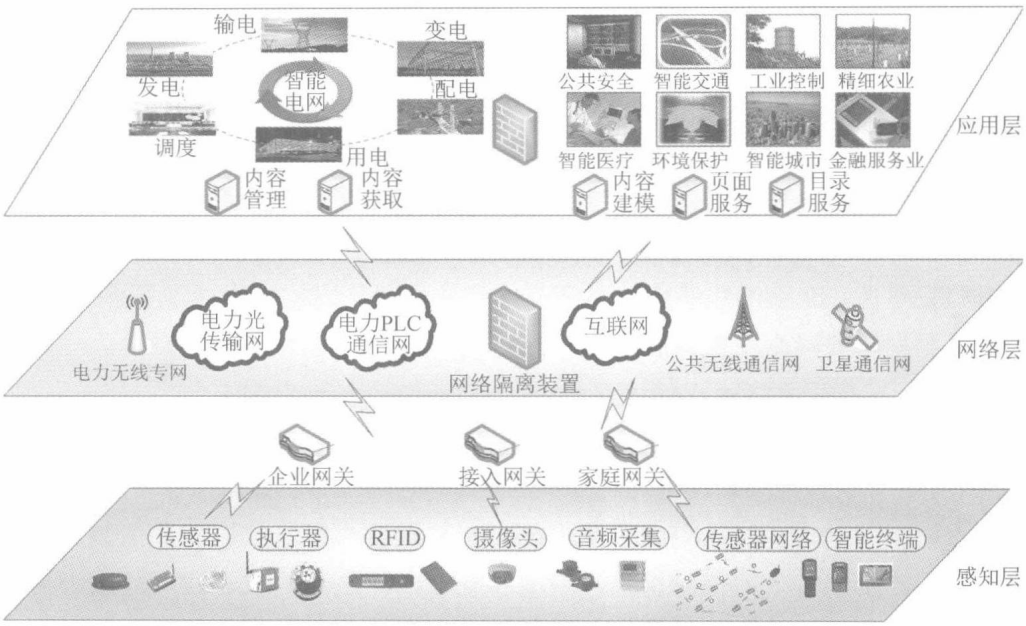


图 1-2　电力物联网三层架构

1.2.2　电力物联网基本特征

电力物联网的基本特征可以归纳为如下几个方面。

全面感知：实现对电力系统物理空间的全面智能识别、感知、信息采集及汇聚处理。电力物联网需要部署海量的多种类型传感器，不同类别的传感器所捕获的信息内容和信息格式不同。传感器获得的数据具有实时性，按一定的频率周期性地采集设备运行状态及环境信息。

IP 互联：传感器之间、传感器与应用系统之间通过基于 IP 的标准化协议，实现信息传递与交互。IPv6 协议凭借丰富的地址资源以及支持动态路由机制等优势，能够满足电力物联网对通信网络的地址需求、网络自组织以及扩展性等很多方面的要求。电力物联网要求对感知元素清晰辨识和精准定位，IP 互联可以实现对感知设备的有效访问和有序管理。

可靠传输：利用电信网、互联网或专用网络承载感知信息，实现感知层和应用层之间的可靠信息传递及路由控制。在感知信息传输过程中，通信网络介质不同、网络结构不同、传输规约不统一等将会影响信息传递的可靠性，为了保证感知信息

传输的服务质量，物联网传输层必须能够屏蔽异构网络的差异性。

智能处理：综合运用云计算、人工智能、大数据处理等技术，进行数据存储、数据挖掘、智能分析等数据分析，由从传感器获得的海量信息得出行业需求数据，并根据行业需求构建数据服务及应用平台，实现对各行业业务系统的应用支撑，满足不同行业应用需求，提高各行业的生产和管理水平。

1.3　电力物联网应用

智能电网是智能化的电力系统，它涉及传感与检测、通信、能源、新材料等诸多产业，先进的微传感器网络和通信技术是其中的基础和关键技术。电力系统中输电网络、配电网络分布在城市、乡村的各个角落，对各种电力参数的感知能够使我们及时有效地了解局部电网的运营状况，从而恰当合理地调整电力资源分配策略，以达到更合理利用电力资源的目的。

电网的可观测性是电网智能化的前提条件，只有在电力系统中广泛使用传感技术，通过对电力系统及其关键设备大量的运行数据进行全面监测，才能真正达到电力系统资源全面优化配置、提高系统可靠性和安全性的目的，如图 1-3 所示。电力企业利用各种物联网传感器，对电网中的发电、输电、配电、用电相关的各种设备的运行情况进行实时监测，提升对于远程设备的监控能力，从而及早发现故障迹象并加以维护，更快地定位并隔离故障区域。

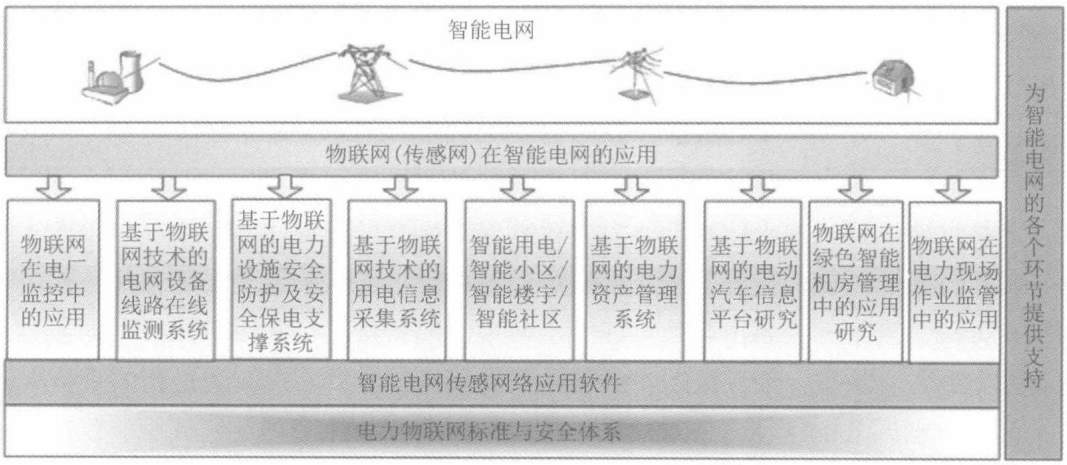


图 1-3　电力物联网在智能电网中的应用体系

智能电网可以作为电力运营方与消费方之间的桥梁，它能有效地协调二者之间的关系。作为运营方，电力企业可以自动地采集用户的用电信息，并做相关的统计

分析，为营销行为提供实时的依据，同时可为电力建设决策提供依据，真正做到需求侧的智能管理。作为消费方，电力用户可以利用传感器网络提供的信息，更好地了解自己的用电情况，居民还可以通过传感网络将家用电器和智能电表互联来实现智能家居，以达到互动、高效、经济、安全、可靠的用电。

1.3.1 发电方面

电力物联网在发电方面的应用包括电厂设备的状态检测、生物质能发电、风电场监控、功率预测、光伏发电、设备管理、巡视、巡检等。利用感知技术在常规机组内部布置传感监测点来了解机组运行情况，如表 1-1 所示。根据统计，电机损坏事故中有 50%是由定子绕组绝缘损坏引起的，但由于局部放电电流小，通过常用的电流、电压互感器难以监测和识别，电机绕组局部放电一直是困扰设备安全运行的重大隐患。目前常用监测方法包括耦合电容法、定子槽耦合器法、射频监测法。

表 1-1 发电机/电动机主要监测用传感器一览表

传感器	适用功能
电容传感器	局部放电：监测沿电机引出线传输的局部放电脉冲信号
定子槽耦合器	局部放电：监测沿定子槽的局部放电电流脉冲信号
电流传感器	局部放电：监测空间传播的局部放电射频脉冲信号
光纤振动传感器	定子绕组的径向振动、轴向振动或周向振动
多种类型传感器	电机转矩转速测量
温度传感器	电机绕组温升

此外，可以通过在水电站坝体设置传感器网络来监测坝体变化情况，规避水库运行可能存在的风险。另外，电厂的生产设备相对于电网来说是采用并联结构，并都编上号码，当某一设备出现故障或周围环境出现变化时，利用感知技术，通过采集器采集到各种数据，经判断后将必要的预警和报告信息准确发送给相关负责人。

例如发电厂基础建设，分布式电厂监控、厂区监控污染物及气体排放监控、能耗监控、煤料监控、抽水蓄能监控、风电厂监控、功率预测、储能监控等，通过电厂生产监控系统，协助电厂从定时的人工监控转变为全时的自动监控。这些应用的实现都是基于物联网利用传感器对数据的采集和传输的基础之上的。

1.3.2　输电方面

输电环节是智能电网中一个极为重要的环节，而输电线路状态检测是输电环节的重要应用，主要包括雷电定位和预警、输电线路气象环境监测与预警、输电线路覆冰监测与预警、输电线路在线增容、导地线微风振动监测、导线温度与弧垂监测、输电线路风偏在线监测与预警、输电线路图像与视频监控、输电线路运行故障定位及性质判断、绝缘子污秽监测与预警、杆塔倾斜在线监测与预警等方面，如图 1-4 所示。这些方面都需要感知技术的支持，包括各种传感器技术、分析技术和通信技术等。

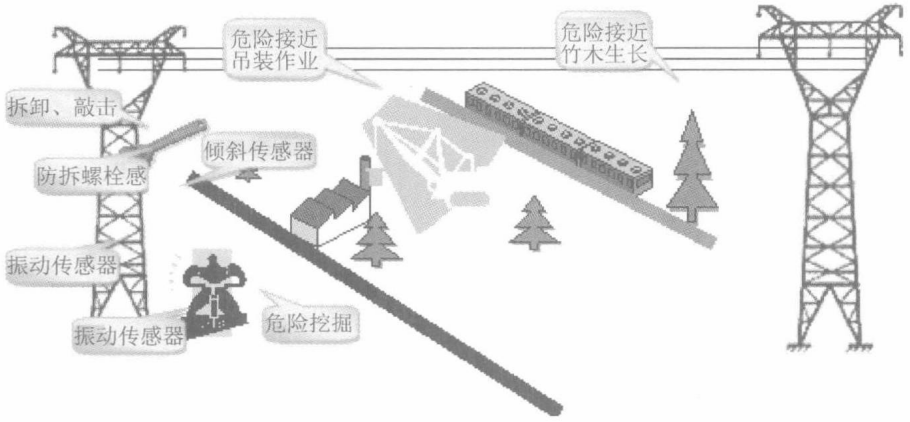


图 1-4　杆塔防范示意图

输电线路在线监测系统的总体架构包括通过在整条输电线路上部署多功能骨干节点、加速度（陀螺仪）传感器节点，并在高压杆塔上布设泄漏电流传感器节点、通信骨干节点来构成一个传感器簇，多个这样的簇构成线状网络并通过无线或光纤通信装置构成整个智能电网输电线路在线监测系统。

例如，通过部署在输电线路上的多种传感器进行输电线路状态在线监测，如温度传感器、加速度传感器、湿度传感器、风速传感器，以及高压杆塔上的倾斜传感器、振动传感器等，如图 1-5 所示。结合先进的视频识别技术、传输技术、三维空间地理信息系统（Geographic Information System，GIS）技术、无线宽带通信技术组成面向输电线路应用的物联网网络，实现对输电线路的各种状态（如覆冰、污秽、温度、舞动、微气象等信息）的多方位可视化实时监控，并根据监测情况发布故障预警信息，保障输电线路的安全可靠运行。

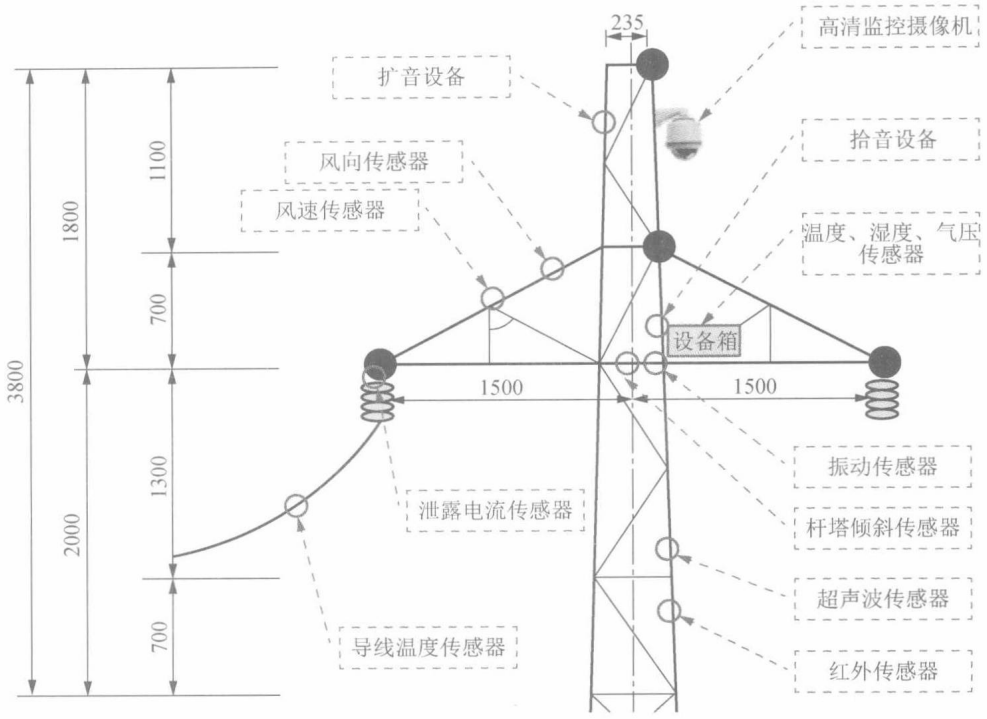


图 1-5　输电杆塔上面的传感器示意图

1.3.3　变电方面

智能变电站是采用先进、可靠、集成、低碳、环保的智能设备，以全站信息数字化、通信平台网络化、信息共享标准化为基本要求，自动完成信息采集、测量、控制、保护、计量和监测等基本功能，并可根据需要支持电网实时自动控制、智能调节、在线分析决策、协同互动等高级功能，实现与相邻变电站、电网调度等互动的变电站，常见的一些变压器监测用传感器如表 1-2 所示。

表 1-2　变压器主要监测用传感器一览表

传感器	适用功能
气体传感器	绕组局部放电中特定气体（如 CH_4、C_2H_6、C_2H_4、C_2H_2、H_2、CO 和 CO_2 等）的释放
超声波传感器	局部放电所伴随的爆裂状的声发射
超高频（UHF）传感器	局部放电的高频电流
温度传感器	内部短路、放电、过负荷等造成的温度异常
压力传感器	局部放电引起的气体释放而使得变压器内部压力增大
振动传感器、噪声传感器	铁心松动或变形等情形