智能电网中的信息安全技术

摘要:文章认为智能电网的信息安全问题必须在智能电网部署的过程中充分考虑。智能电网的信息安全主要包括物理安全、网络安全、数据安全及备份恢复等方面;智能电网还会面对由多网融合引发的新的安全问题，如智能电网感知测量节点的本地安全问题、智能电网感知网络的传输与信息安全问题、智能电网业务的安全问题。文章基于智能电网在信息采集、信息传输和信息处理3个层面所采用的信息安全技术，指出未来智能电网将会融合更多的先进的信息安全技术，如可信计算、云安全等。

通过数字化信息网络系统将能源资源流通的各个环节、终端用户的各种电气设备和其他用能设施连接在一起，通过智能化控制，提高能源利用效率和保障能源供应安全，这就是智能电网思想的起源。

关于智能电网，目前国际上尚无统一明确的定义。美国电力科学研究院将智能电网定义为：一个由众多自动化的输电和配电系统构成的电力系统，以有效和可靠的方式实现所有的电网运作，具有自愈功能;能快速响应电力企业业务需求;具有智能化的通信架构，以实现实时、安全和灵活的信息流管理，并为用户提供可靠、经济的电力服务。

智能电网是一种高度自动化的数字化电网。位于其中的用户端以及各个节点均可实现实时监控，采集到的双向功率流信息贯穿在整个发、输、配、用过程当中。智能电网在开放系统和共享信息模式的基础上，可以通过宽带通信系统、自动控制系统以及分布式智能设备等，实现电网中各部门的协调和实时互动，以及实时市场化交易，以达到优化电网的管理和运营目的。

整合后的智能电网的体系架构从设备功能上可以分为4个层次，分别是基础硬件层、感知测量层、信息通信层和调度运维层。

(1)基础硬件层

基础硬件主要分布在“发、输、配、用”4个环节中。发电涵盖风电、分布式电源、光伏电源、接入电源等;输电涵盖互济、超导、特高压、网架等;配电涵盖微网、虚拟电厂、高级电表设施等;用电涵盖电器、用电自动控制设备、分布式电力供应站、电力储能设备等。

(2)感知测量层

感知测量层主要通过智能测控设备来实现智能感知，以评估阻塞情况和电网稳定性，监控设备健康情况，防止窃电，以及实现控制策略支持等。该层由智能计读数装置、相角测量单元、广域测量系统、动态线路定级系统、电磁信号测量与分析系统、用电时间实时定价设备、数字继电器等组成。这些仪器仪表采用射频识别、传感器和短距离高速无线通信技术，实时与智能电网相连接。

(3)信息通信层

信息通信层采用的技术涵盖变电站自动化、配电自动化、监控和数据采集、需求响应、能量管理、无线网络、数字移动通信以及光纤通信等领域，能够实现实时控制、信息和数据交换，以保障达到最佳的系统可靠性、最好的资产利用率，实现最高的安全性。

(4)调度运维层

智能电网的灾备能力除面对电力系统外，还涉及自然和社会诸多因素，必须精确管理控制，因此需要与人工智能技术相结合。为了实现整个系统范围内的协调控制，分布式智能代理及网状控制结构等形式的设计将融入到系统建设中。系统可以被用来实施分布式决策控制，也可以进行集中协调。信息通信层将为调度运维中心的运行提供坚实的技术支撑。

在智能电网中，数字化、网络化、信息化技术主要分布于感知测量层、信息通信层和调度运维层中，因此本文对智能电网的信息安全技术的分析将主要围绕这3层展开。

1 智能电网的信息安全需求

智能电网作为物联网时代最重要的应用之一，将会给人们的工作和生活方式带来极大的变革，但是智能电网的开放性和包容性也决定了它不可避免地存在信息安全隐患。和传统电力系统相比较，智能电网的失控不仅会造成信息和经济上的损失，更会危及到人身和社会安全。因此，智能电网的信息安全问题在智能电网部署的过程中必须充分考虑。针对智能电网的运营特点，其安全需求主要包括物理安全、网络安全、数据安全及备份恢复等方面。

(1)物理安全

智能电网的物理安全是指智能电网系统运营所必需的各种硬件设备的安全。这些硬件设备主要包括智能计、测量仪器在内的各类型传感器，通信系统中的各种网络设备、计算机以及存储数据的各种存储介质。物理安全主要指保证硬件设备本身的安全和智能电网系统中其他相关硬件的安全，是智能电网信息安全控制中的重要内容。物理安全的防护目标是防止有人通过破坏业务系统的外部物理特性以达到使系统停止服务的目的，或防止有人通过物理接触方式对系统进行入侵。要做到在信息安全事件发生前和发生后能够执行对设备物理接触行为的审核和追查。

(2)网络安全

在传统电力系统基础上，智能化的通信网络架构的智能电网应具有较高的可靠性。该通信网络必须具备二次系统安全防护方案。防护的原则是：安全分区、网络专用、横向隔离、纵向认证。根据这个原则，智能电网的通信网络可划分为4个分区：安全区I(实时控制区)、安全区II(非控制生产区)、安全区III(生产管理区)、安全区IV(管理信息区)。其中，安全区I、安全区II和安全区III之间必须采用经相关部门认定核准的电力专用安全隔离装置，必须达到物理隔离的强度。网络纵向互联时，互联双方必须是安全等级相同的网络。要避免安全区纵向交叉，同时在网络边界要采用逻辑隔离。信息系统网络运行过程中要充分利用防火墙、虚拟专用网，采用加密、安全隔离、入侵检测以及网络防杀病毒等技术来保障网络安全。

(3)数据安全及备份恢复

在智能电网中，数据安全的含义有两点：其一，数据本身的安全。即采用密码技术对数据进行保护，如数据加密、数据完整性保护、双向强身份认证等。其二，数据防护的安全，即采用信息存储手段对数据进行主动防护，如通过磁盘阵列、数据备份、异地容灾以及云存储等手段保证数据的安全。

智能电网整体的信息安全不能通过将多种通信机制的安全简单叠加来实现。除了传统电力系统的信息安全问题之外，智能电网还会面临由多网融合引发的新的安全问题。

(1)感知测量节点的本地安全问题

由于智能电网中的智能设备可以取代人来完成一些复杂、危险和机械的工作，所以智能电网的感知测量节点多数部署在无人监控的环境中。攻击者可以轻易地接触到这些设备，从而对他们造成破坏，甚至通过本地操作更换机器的软硬件。

(2)感知网络的传输与信息安全问题

感知测量节点通常情况下功能唯一、能量存储有限，使得复杂的安全保护技术无法应用。而智能电网的感知网络形式多样，从功率测量到稳压监控，再到电价实时控制，它们的数据传输没有特定的标准，所以没法提供统一的安全保护体系。

(3)核心通信网络的传输与信息安全问题

核心通信网络具有相对完整的安全保护能力。但是由于智能电网中节点数量庞大，且以集群方式存在，因此会导致在数据传播时，由于大量机器的数据发送使网络拥塞，产生例如拒绝服务攻击等一系列安全威胁。此外，现有通信网络的安全架构都是从人与人之间通信的角度设计的，并不适用于机器之间通信。简单套用现有安全机制不符合智能电网的设备之间的逻辑关系。

(4)智能电网业务的安全问题

由于智能电网中的设备可能是先部署后连网，同时又会面临无人看守的情况，所以如何对智能电网中的设备进行身份认证和业务配置就成了难题。庞大且内部多样化的智能电网需要一个强大而统一的信息安全管理平台来统一管理，

否则独立化的子平台会被各式各样的智能电网应用所淹没。另外，如何在对智能电网中设备的日志等安全信息进行管理的同时，不破坏通信网络与业务平台之间的信任关系也是必须研究的问题。

2 智能电网信息安全关键技术

智能电网体系架构的4个层次中，除了不涉及到信息通信的基础硬件层以外，上面3层均有着对应的信息安全技术。感知测量层对应信息采集安全技术，信息通信层对应信息传输安全技术，调度运维层对应信息处理安全技术。

信息采集安全主要保障智能电网中的感知测量数据。这一层需要解决智能电网中使用无线传感器、短距离超宽带以及射频识别等技术的信息采集设备的安全性。信息传输安全主要保障传输中的数据信息安全。这一层需要解决智能电网使用的无线网络、有线网络和移动通信网络的安全性。信息处理安全主要保障数据信息的分析、存储和使用。这一层需要解决智能电网的数据存储安全以及容灾备份、数据与服务的访问控制和授权管理。

2.1 信息采集安全

2.1.1 无线传感器网络安全

无线传感器网络中最常用到的是ZigBee技术。ZigBee技术的物理层和媒体访问控制层(MAC)基于IEEE 802.15.4，网络层和应用层则由ZigBee联盟定义。ZigBee协议在MAC层、网络层和应用层都有安全措施。MAC层使用ABE算法和完整性验证码确保单跳帧的机密性和完整性;而网络层使用帧计数器防止重放攻击，并处理多跳帧;应用层则负责建立安全连接和密钥管理。ZigBee技术在数据加密过程中使用3种基本密钥，分别是主密钥、链接密钥和网络密钥。主密钥一般在设备制造时安装。链接密钥在个域网络(PAN)中被两个设备共享，可以通过主密钥建立，也可以在设备制造时安装。网络密钥可以通过信任中心设置，也可以在设备制造时安装，可应用在数据链路层、网络层和应用层。链接密钥和网络密钥需要进行周期性地更新。

2.1.2 短距离超宽带通信安全

短距离超宽带(UWB)协议在MAC层有安全措施。UWB设备之间的相互认证基于设备的预存的主密钥，采用4次握手机制来实现。设备在认证过程中会根据主密钥和认证时使用的随机数生成对等临时密钥(PTK)，用于设备之间的单播加密。认证完成之后，设备还可以使用PTK分发组临时密钥(GTK)用于安全多播通信。数据完整性是通过消息中消息完整性码字段实现的。UWB标准通过对每一个PTK或者GTK建立一个安全帧计数器实现抗重放攻击。

2.1.3 射频识别安全

由于射频识别(RFID)的成本有严格的限制，因此对安全算法运行的效率要求比较高。目前有效的RFID的认证方式之一是由Hopper和Blum提出的HB协议以及与其相关的一系列改进的协议。HB协议需要RFID和标签进行多轮挑战——应答交互，最终以正确概率判断RFID的合法性，所以这一协议还不能商用。由于针对RFID的轻量级加密算法现在还很少，因此有学者提出了基于线性反馈移位寄存器的加密算法，但其安全性还需要进一步证明。

2.2 信息传输安全

2.2.1 无线网络安全

无线网络安全主要依靠802.11和Wi-Fi保护接入(WPA)协议、802.11i协议、无线传输层安全协议(WTLS)。

(1)802.11和WPA协议

802.11中加密采用有线等效保密协议(WEP)。由于使用一个静态密钥加密数据，所以比较容易被破解，现在已经不再使用。WPA协议是对802.11的改进。WPA采用802.lx和临时密钥完整性协议(TKIP)来实现无线局域网的访问控制、密钥管理和数据加密。802.lx是一种基于端口的访问控制标准，用户只有通过认证并获得授权之后才能通过端口访问网络。

(2)802.11i协议

802.11i协议是对802.11协议的改进，用以取代802.11协议。802.l1i协议的认证使用可扩展认证协议(EAP)。基本思想是

基于用户认证的接入控制机制。具体内容包括用户认证、密钥生成、相互认证、数据包认证及防字典攻击等。可以使用各种接入设备，并且可以有效支持未来的认证方式。802.11i的数据保密协议包含TKIP和计数器模式/密文反馈链接消息认证码协议(CCMP)。TKIP采用RC4作为核心算法，包含消息完整码和密钥获取与分发机制。CCMP的核心加密算法采用128位的记数模式高级加密标准(AES)算法，不仅能够抵抗重放攻击，而且使用密码分组链接模式也可以保证信息的完整性。

(3)无线传输层安全协议

WTLS位于国际标准化组织(ISO)7层模型的传输层之上。WTLS基于安全套接层(SSL)并对传输层安全协议(TLS)进行了适当的修改，加入了对不可靠传输层的支持，减小了协议开销，使用了更先进的压缩算法和更有效的加密方法，可以用于智能电网的无线网络部分。WTLS主要应用于无线应用协议(WAP)，用于建立一个安全的通道，提供的安全特性有：鉴权、信息可信度及完整性。同SSL一样，WTLS协议也分为握手协议和记录协议两层。

2.2.2 有线网络安全

有线网络安全主要依靠防火墙技术、虚拟专用网(VPN)技术、安全套接层技术和公钥基础设施(PKI)。

(1)防火墙技术

防火墙技术最初的原型采用了包过滤技术，通过检查数据流中每个数据包的源地址、目的地址、所用的端口号、协议状态或它们的组合来确定是否允许该数据包通过。在网络层上，防火墙根据IP地址和端口号过滤进出的数据包;在应用层上检查数据包的内容，查看这些内容是否能符合企业网络的安全规则，并且允许受信任的客户机和不受信任的主机建立直接连接，依靠某种算法来识别进出的应用层数据。

(2)虚拟专用网

虚拟专用网是指在一个公共IP网络平台上通过隧道以及加密技术保证专用数据的网络安全性。VPN是一种以可靠加密方法来保证传输安全的技术。在智能电网中使用VPN技术，可以在不可信网络上提供一条安全、专用的通道或隧道。各种隧道协议，包括网络协议安全(IPSec)、点对点隧道协议(PPTP)和二层隧道协议(L2TP)都可以与认证协议一起使用。

(3)安全套接层

安全套接层技术提供的安全机制可以保证应用层数据在智能电网传输中不被监听、伪造和窜改，并且始终对服务器进行认证。SSL还可以选择对客户进行认证，提供网络上可信赖的服务。SSL可以用于智能电网的有线网络部分。SSL是基于X.509证书的PKI体系的一种应用，主要由纪录协议和握手协议构成。SSL记录协议建立在可靠的传输协议(如TCP)之上，为高层协议提供数据封装、压缩、加密等基本功能支持;SSL握手协议建立在SSL记录协议之上，用于在实际的数据传输开始前，通信双方进行身份认证、加密算法协商、加密密钥交换等。

(4)公钥基础设施

公钥基础设施能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。PKI可以为不同的用户按不同安全需求提供多种安全服务，主要包括认证、数据完整性、数据保密性、不可否认性、公正和时间戳等服务。

2.2.3 移动通信网络安全

移动通信网络安全包括GSM网络安全、3G网络安全、LTE安全。

(1)GSM网络安全

在GSM网络中，基站采取询问-响应认证协议对移动用户进行认证，制止非授权用户使用网络资源。在无线传输的空中接口部分对用户信息加密，防止窃听泄密。

(2)3G网络安全

在3G网络中，终端和网络使用认证与密钥协商(AKA)协议进行相互认证，不仅网络可以识别终端的合法性，终端也会认证网络是否合法，并在认证过程中产生终端和网络的通信密钥。3G网络还引入了加密算法协商机制，加强了信息在网络内的传送安全，采用了以交换设备为核心的安全机制，加密链路延伸到交换设备，并提供基于端到端的全网范围内的加密。

(3)LTE安全

在长期演进/3GPP系统架构演进(LTE/SAE)中将安全措施在接入层(AS)和非接入层(NAS)信令之间分离开，无线链路和核心网需要有各自的密钥。这样，LTE系统有两层保护，第一层为用户层安全，第二层是EPC中的网络附加存储(NAS)信令安全。用户和网络的相互认证和安全密钥生成都在AKA流程中进行。该流程采用了基于对称加密体制的挑战-响应机制，产生128比特的密钥。

2.3 信息处理安全

2.3.1 存储安全

存储可以分为本地存储和网络存储。本地存储需要提供文件透明加密存储功能和加密共享功能，并实现文件访问的实时解密。本地存储严格界定每个用户的读取权限。用户访问数据时，必须经过身份认证。网络存储主要分NAS、存储区域网络(SAN)与IP存储3类。在文件系统层上实现网络存取安全是最佳策略，既保证了数据在网络传输中和异地存储时的安全，又对上层的应用程序和用户来说是透明的;SAN可以使用用户身份认证和访问控制列表实现访问控制，还可以加密存储，当数据进入存储系统时加密，输出存储系统时解密;IP存储安全需要提供数据的机密性、完整性及提供身份认证，可以用IPSec、防火墙技术等技术实现，在进行密钥分发的时候，还会用到PKI技术。

2.3.2 容灾备份

容灾备份可以分为3个级别：数据级别、应用级别和业务级别。从对用户业务连续性的保障程度来看，它们的可用级别逐渐提高。前两个级别都仅仅是对通信信息的备份，后一个则包括整个业务的备份。智能电网业务的实时性需求很强，应当选用业务级别的容灾备份。备份不仅包括信息通信系统，还包括智能电网的其他相关部分。整个智能电网可以构建一个集中式的容灾备份中心，为各地区运营部门提供一个集中的异地备份环境。各部门将自己的容灾备份系统托管在备份中心，不仅要支持近距离的同步数据容灾，还必须能支持远程的异步数据容灾。对于异步数据容灾，数据复制不仅要求在异地有一份数据拷贝，同时还必须保证异地数据的完整性、可用性。对于网络的关键节点，要能够实时切换。网络还要具有一定的自愈能力。

2.3.3 访问控制和授权管理

访问控制技术分为3类：自主访问控制、强制访问控制、基于角色的访问控制。自主访问控制即一个用户可以有选择地与其他用户共享文件。主体全权管理有关客体的访问授权，有权修改该客体的有关信息，而且主体之间可以权限转移。强制访问控制即用户与文件都有一个固定的安全属性系统，该安全属性决定一个用户是否可以访问某个文件。基于角色的访问控制即授予用户的访问权限由用户在组织中担当的角色来确定。根据用户在组织内所处的角色进行访问授权与控制。当前在智能电网中主要使用的是第三类技术。

授权管理的核心是授权管理基础设施(PMI)。PMI与PKI在结构上非常相似。信任的基础都是有关权威机构。在PKI中，由有关部门建立并管理根证书授权中心(CA)，下设各级CA、注册机构(RA)和其他机构。在PMI中，由有关部门建立授权源(SOA)，下设分布式的属性机构(AA)和其他机构。PMI能够与PKI和目录服务紧密集成，并系统地建立起对认可用户的特定授权。PMI对权限管理进行了系统的定义和描述，完整地提供了授权服务所需过程。

3 结束语

未来的信息安全技术必须要与智能电网信息通信系统相互融合，而不仅仅是简单的集成。在制订智能电网标准的时候就需要考虑到可能存在的各种信息安全隐患，而不能先制订标准再去考虑信息安全，否则就会重蹈互联网的覆辙。

未来智能电网作为物联网在电力行业的应用，将会融合更多的先进的信息安全技术，如可信计算、云安全等。智能电网将会发展成基于可信计算的可信网络平台。智能电网中的可信设备通过网络搜集和验证接入者的完整性信息，依据安全策略对这些信息进行评估，从而决定是否允许接入，以确保智能电网的安全性。同时，可信计算还可以协助智能电网建立合理的用户控制策略，并依据用户的行为分析数据来建立统一的用户信任管理模型。智能电网还将会融合

云安全技术，借助于云端的数据信息，在病毒未危害到设备时就提前阻止危害发生。云端数据信息的实时更新将会是物联网时代应对病毒的有效手段。

原文地址：http://www.china-nengyuan.com/tech/63160.html