电力系统通信技术中的信息安全及应用

张冲　张海宁

国网天津静海供电有限公司　天津　301600

[摘　要]近年来，随着国民经济的不断发展，人们对供电质量的要求也越来越高，同时随着数字化社会的不断推进，电力系统的发展日益庞大复杂，而它担负着集中管理、统一调度、数据收集等重要职能，因此保障这一-系统的信息通信安全至关重要。一旦系统存在漏洞或被认为破坏，就会使得电网存在失控、误控的风险，导致供电失误甚至引起整个电力系统的瘫痪。因此，我们必须注重电力系统信息通信的安全性，加强信息的安全防范工作，实现供电系统的安全、高效、稳定的运行。

[关键词]电力系统；通信技术；信息安全；签名认证

【DOI】10.12252/j.issn.2096-627X.2021.10.360

一、电力系统信息安全现状及面临的挑战

1.1现状和存在的问题

1.无法保障电力系统的安全和稳定

从实际运行情况来看，网络技术和能源系统的复杂性增加了对能源系统进行安全保障的困难，一些犯罪分子试图利用黑客技术渗透电力公司的网络，并破坏电网完整性。现阶段，管理成为降低电力信息安全隐患的关键，部分单位由于缺乏对系统中电力信息保护的意识，导致使用互联网在传输、存储、处理涉密信息时出现泄漏，或是遭到人为、木马病毒的破坏，使得电力行业的系统安全稳定运行遭到威胁。

2.操作系统还无法统一运行

电力系统的信息传输以因特网为基础，通过广泛的应用程序和相关的通信设备，与不同区域和不同功能的电子设备连接，从而使因特网平台能够发挥确保信息安全的功能，最终实现数据传输和实时共享信息的功能。目前电力系统在使用因特网信息传播平台时，也具有因特网的特点，设备分布很广，但还没有实现相互连接和统一运行管理。

1.2面临的挑战

1.电力系统自身运行面临的挑战

现阶段，电力信息系统面临的挑战有：

（1）系统组件性能有待提高。（2）电力系统对外界环境以及自然灾害的抵抗能力有待提高。（3）抵御不确定因素的能力有待提高，如不正确的操作、配置、设计或人员的疏忽大意等。（4）电力系统工作人员意识、信息安全管理机制、系统运行安全评估体系等，应在信息系统规划中得以重视，从而降低电力系统安全问题发生概率，为电力数字平台的建立提供坚实保障。

2.新技术的应用与兴起带来的挑战

大数据等新兴技术作为现阶段电力系统信息化提升的关键，可为电力系统运行提供获取、储存、分析等能力，有规模大、流动速度高、类型多样和数据价值密度低等特点。通过应用大数据等信息通信技术，电网智能化和数字化水平进一步提升，客户和电力企业关系更加紧密，通过电力替代、转化、交易和调度业务集成，实现电力生产、传输、消费协调控制，推动电力消费革命。

二、提升信息安全措施

2.1明确划分好网路安全区域

网络安全区域划分主要是从网络信息的基本性能、承载对象以及网络安全对象的角度出发，将网络信息换分成多个逻辑子网，通过此种方式，在同一个逻辑子网络中，可以使用相应的安全访问手段，不仅可以实现对边界控制，同时还能够加强对不同逻辑子网访问的监督管理工作。利用此种方式，可以达到以下目的：第一，通过将复杂的信息系统安全问题，转变成为一些小区域的安全问题，可以降低系统安全隐患。第二，充分发挥安全域划分技术，可以更好地理顺网络，做好地信息指导系统的规划、设计以及联网验收等工作。第三，确定安全区域的保护重点，利用有限的信息设备，充分保护系统信息资产，确保设备的有效性。第四，优化信息安全的运行管理工作，科学合理地规划安全审计设备，为信息检查和审核提供良好的依据。

2.2采用虚拟专网（VPN）技术

虚拟专网是指采用隧道技术以及加密、身份认证等方法，在公共网络上搭建专用的虚拟网络，使数据通过安全的“加密隧道”在公共网络中传输。虚拟专网虽然属于临时链接，但是其具备较高的安全性以及访问控制功能，可以对数据进行加密，也可以阻止入侵者访问网络，大大提升网络的安全性。有效应用虚拟专网技术还可使用户和企业通过公共的互联网络，连接到远程服务器和网络，或作用于多个企业之间，同时保护通信的安全。

2.3通过数字证书执行相关操作

安全系统的设计使用一个计算机化的证书服务器，配置证书发件人，以便其他用户可以向证书发件人申请证书确定。进入系统进行某一特定操作的用户需要严格的加密认证，才能操作一个重要的服务器或访问数据，安全系统首先核实用户的身份，并核查用户是否是通过签发人签发证书的用户，然后用户的相关操作请求被发送到服务器，并通过用户证书发送给用户。在用私人钥匙签署证书之后，服务器还核查签字证书，确认证书是合法的，从证书中撤销公用钥匙，核证用户证书的签字，并在用户身份确定之后，才可访问该网页进行相关的操作。

2.4实现数字签名认证

为加强电力网络系统平台的安全，需要在数字证书用户身份认证技术的基础上，对电子文件数据进行数字签名，这将在一定程度上确保信息的完整性，并确认数据的真实性，防止数据受到否定和伪造。首先，发送方用HASH函数从明文文件中生成一个数字[摘　要]，用自己的私钥对这个数字[摘要]进行加密形成发送方的数字签名；选择一个对称密钥对文件加密，然后发送到接收方，最后将该数字签名作为附件和报文密文一起传输给接收方；再用接收方的公钥加密对称密钥，并通过网络将加密后的对称密钥传输到接收方。最后通过数据[摘　要]的比较对数据签名进行验证。通过此种方式，可以保障验证签署工作的有效性，一旦系统确定签名有效，则可以自动从签名者的证书中找到公钥，从而去验证被HASH函数作用的数据内容，如果内容匹配，最终返回验证成功值。

三、结语

本文通过对电力系统常见的通信技术现状及应用过程中面临的信息安全挑战进行分析讨论，目前电力系统信息安全技术的应用仍处于探索阶段，面临许多的难题与挑战。但随着智能电网的逐步发展与壮大，以及与之相关的大数据、云计算、5G、物联网等新技术的研究和应用，相信将来会有更多、更加先进的信息安全技术与电网相结合，并针对电网的通信特点来解决信息安全防护问题。

参考文献

[1]付彦哲.大数据技术在电力系统信息安全防护中的应用[J].电子世界，2020（11）.

[2]李亚方.探究如何实现PKI在电力系统信息网络安全中的应用[J].现代工业经济和信息化，2020（01）.