一种多级安全防护的过滤模型在智能配电网通信系统的应用

李 貌， 滕 欢
(四川大学电气信息学院，四川 成都 610065)

摘 要: 为了实现全面和实时的监控,分布广泛的公用因特网将在智能电网通信系统中占有越来越多的比重。智能配电网的开放性为电力系统中公用网络接入了大量的恶意攻击入口。为了阻止恶意的终端接入到智能配电网通信系统,在智能配电网通信系统层次化结构设计的基础上,提出采用多级信息安全过滤模型和综合加密技术实现对智能配电网的信息系统的安全防护。综合加密通信编程实例表明,该方案增强电力网敏感信息安全性和实用性。

关键词: 智能配电网; 安全过滤; 数据加密; 通信

Abstract: In order to realize the comprehensive and real - time monitoring, the widespread public Internet in the communication system of smart grid occupies more and more proportion. In the public network of power system, the openness of smart distribution network gives the access of a large number of malicious attack entrances. In order to prevent the malicious terminal access to the communication system of smart distribution network, multilevel information security filtering model and integrated encryption technology are adopted so as to realize the security protection for information system of smart distribution network based on the hierarchical structure design of communication system in smart distribution network. The examples of integrated encryption communication programming show that the proposed scheme can improve the sensitive information security and practicability.

Key words: smart distribution network; security filtering; data encryption; communication
中图分类号: TM769 **文献标志码:** A **文章编号:** 1003 - 6954(2014)04 - 0076 - 05

0 引 言

智能电网,又称为知识型电网或者现代电网,是将现代先进的传感与测量技术、信息通信技术、控制技术和原有的输配电基础设施高度集成而形成的新型电网。国家电网公司提出以特高压电网为骨干网架、各级电网协调发展的坚强电网为基础,利用先进的通信、信息和控制技术,构建以信息化、自动化、数字化、互动化为特征的国际领先、自主创新、中国特色的坚强的智能化电网。

智能配电网,作为电力“发、输、调、变、配、用”的重要环节,是社会公众感知电网智能化服务的关键所在,智能配电网是智能电网的重要组成部分[1-2]。智能配电网需要监测和控制的设备数量更多,分布更广。为了实现全面和实时的监控,成本低廉的无线通信网和分布广泛的公用因特网将在智能电网通信系统中占有越来越多的比重。与此同时,智能配电网的开放性,电网和用户双向互动性增强,大量用户侧接入和访问,智能采集终端和移动作业终端的广泛应用和接入,无线公共网络传输通道的应用等对智能配电网的发展提出了新的安全问题。然而关于智能配电网信息安全方面的研究到目前为止并不多[3-5]。

由于智能配电网与终端有良好的交互,大量用户的接入对信息安全带来了一定的威胁。因此要过滤非授权的终端,而信息加密是保障电力系统信息安全的核心技术。在信息安全过滤理论上,通过一个综合加密通信编程实例,提出采用多级信息安全过滤模型和综合加密技术实现对智能配电网的信息系统的安全防护。

1 信息的安全过滤

信息过滤(information filtering, IF)也就是所谓的信息选择性传播。它是通过监控动态的信息源以

找到满足用户需求的信息或剔除用户不需要的信息及不合法的终端用户。安全过滤的主要方法如下。

(1) 名单过滤(URL / IP 过滤)。建立不良网站的 URL 或者 IP 地址列表数据库，并对该数据库进行定期的数据更新，当用户访问这些站点时，将访问站点的 URL 或者 IP 地址与数据库列表中的进行匹配，如果能够正确匹配，则给予阻断或封锁。

(2) 分级过滤。根据网页的内容属性或其他特征，并按照一定的分级标准，建立网站的分级标记，分级标记可以附在网页上，也可以保存在文件或数据库中，使用时以分级标记为过滤的依据。

(3) 关键词过滤(内容过滤)[6]。该方法是对文本内容、文档的元数据等进行关键词简单匹配或者布尔逻辑运算，对满足匹配条件的网页或网站进行的过滤。

2 加密技术

由于电网中含有许多敏感信息，为了防止未授权用户访问或获取电网运行和调度信息的安全性、完整性，只要通过认证、加密功能来实现数据的安全问题。

目前的数据加密技术根据密钥类型可分为私钥加密(对称加密)系统和公钥加密(非对称加密)系统。对称加密系统与非对称加密相比，在加密、解密处理速度、防范能力、数字签名和身份认证等方面各有优劣。

2.1 RSA 算法

RSA 算法是一种非对称密码算法[7]，所谓非对称，就是指该算法需要一对公开密钥与私有密钥，使用公开密钥对数据进行加密，则只有用对应的私有密钥才能解密。但是速度一直是 RSA 的缺陷。一般来说只用于少量数据加密。

RSA 的算法涉及 3 个参数，n、$e1$、$e2$。其中，n 是两个大质数 p、q 的积，n 的二进制表示时所占用的位数，就是所谓的密钥长度。$e1$ 和 $e2$ 是一对相关的值，$e1$ 可以任意取，但要求 $e1$ 与 $(p-1)^*(q-1)$ 互质；再选择 $e2$，要求 $(e2^* e1) \bmod ((p-1)^*(q-1)) = 1$。$(n, e1)$、$(n, e2)$ 就是密钥对。其中 $(n, e1)$ 为公钥，$(n, e2)$ 为私钥。RSA 加解密的算法完全相同，设 A 为明文，B 为密文，则：$A = B\hat{}e2 \bmod n$；$B = A\hat{}e1 \bmod n$；(公钥加密体制中，一般用公钥加密，私钥解密) $e1$ 和 $e2$ 可以互换使用，即：$A = B\hat{}e1 \bmod n$；$B = A\hat{}e2 \bmod n$。因此 RSA 的加密速度随着密钥长度增加而变慢且运算更为复杂。所以如何提高这些高精度乘除运算的速度是 RSA 体制实用化的关键问题。

2.2 DES 算法

数据加密算法(data encryption algorithm，DEA)是一种对称加密算法，DES 采用的主密钥为 64bit，其中 8 bit 为奇偶校验位，实际主密钥为 56 bit，明文分组长度固定为 64 bit，不足加零。解密时用同样的密钥将密文作为输入，经过一系列相反的步骤得到的输出即明文。但是密钥的安全性和管理是它的不足之处。

2.3 RSA & DES 综合加密

基于 RSA 算法和 DES 算法两种典型密码算法的优缺点[8]。用 DES 算法作为数据的加密算法对数据加密，用 RSA 算法作为 DES 密钥的加密算法，对 DES 的密钥进行加密。要加密的数据量通常很大，而 DES 算法的加、解密速度效率高，对每个数据分组的处理仅需很短时间就能完成。因此，用 DES 算法对大量的数据加密不会影响整个系统的效率。DES 和 RSA 综合加密如图 1 所示。

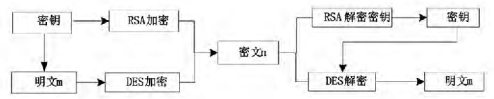

图1 DES & RSA 综合加密结构图

在加密、解密的处理效率方面，DES 算法优于 RSA 算法。在密钥的分配、管理、安全度方面，RSA 算法比 DES 算法更加优越。DES 和 RSA 综合加密算法既能发挥 DES 算法加密速度快、安全性好的优点，又能发挥 RSA 算法密钥管理方便的优点，二者各取其优，扬长避短。

3 智能配电网通信系统模型

从智能化的程度来讲，集中控制模式是智能配电网最为理想的控制模式(如图 2 所示)，而通信系统是建设智能配电网的一个关键环节。智能配电网需依靠有效的通信手段，将控制中心的命令准确地传送到众多的终端智能电子设备(intelligent electric device，IED)，并且将终端 IED 采集的各类实时信息传送到控制中心。

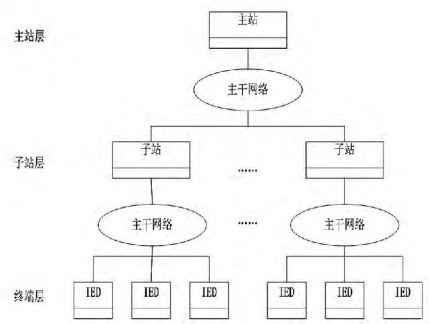

图2 智能配电网通信系统结构举例

4 多级信息过滤防护

该模型包括了第一级的基于Web缓存技术的地址安全过滤和第二级的共享密钥认证技术和综合加密技术的安全过滤两大模块。其中基于Web缓存技术的地址过滤包含了硬件设备认证子模块。此模型从硬件认证(设备身份认证)和软件认证(共享密钥和综合加密解密技术)两个方面,很好地提高了安全过滤的准确性和保障了电力网络敏感信息的安全性。

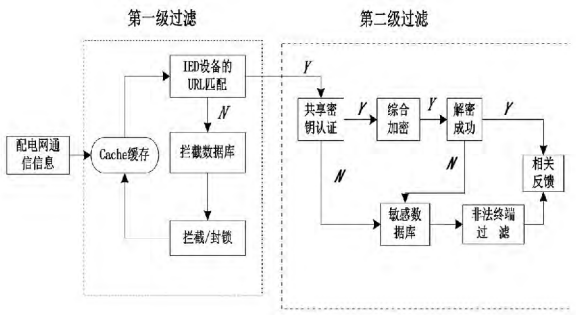

图3 多级过滤防护模型

4.1 第一级过滤

子站经过简单的URL(设备的IP地址)的过滤,由于IED的设备的MAC地址或者IP地址是终端设备的唯一标识符。Web高速缓存服务器技术可以缓存子站与终端互相访问过的对象,这一特点使得可以利用Web缓存技术在子站服务器不忙时启动地址判别、分析功能,采用MAC地址或者IP地址判别技术,使用"MAC判别引擎"或"IP判别引擎",并根据预先设定的规则对缓存数据进行判断,对主站与终端设备访问时提供的陌生的IP地址或者MAC地址进行登记,生成拦截"黑名单"添加到数据库中,同时对不匹配对象则给予阻断或封锁,这样在以后正常工作时,便可在这一级将不良对象过滤掉,从而实现了"一次扫描,多次服务"的高效服务模式。从而初步的防止未授权的对象访问或者获取非法的调度敏感信息以及各种破坏行为。

该技术采用"事后审计"的方式,避免了常用的基于"事先判别"的过滤技术中响应时间长、误判率较高的缺点。

4.2 第二级过滤

MAC地址虽然是一个网络硬件设备的标识,一般是固定的,但是可以通过硬件或软件的方法修改。攻击者可以利用MAC地址欺骗这一弱点,盗用合法IED的地址,从而进行窃取电力网络信息或者破坏电力网络。

设备身份认证成功后由于可能存在MAC地址或者IP地址的伪造,上一级的过滤有可能存在一些没有被过滤掉的访问对象及所携带的信息。此时进行共享密钥认证需要终端IED和子站配置相同的共享密钥。共享密钥认证的认证过程为:终端IED先向子站发送认证请求,子站会随机产生一个Challenge包(即一个字符串)发送给终端IED;终端IED会将接收到字符串拷贝到新的数据中,用密钥加密后再发送给子站;子站接收到该数据后,用密钥将该数据解密,然后对解密后的字符串和最初给终端IED的字符串进行比较。如果相同,则说明客户端拥有子站相同的共享密钥,即通过了Shared Key认证;否则认证失败。

终端IED的电力信息用DES加密算法为数据进行加密,用RSA算法作为DES密钥的加密算法作为终端IED的公开密钥,而子站保存私用密钥。对DES算法可以采用ECB(电子密本)或者是CBC(密文分组链接)工作方式加密能大大提高加密效率和增强了保密强度。终端IED设备在访问减轻了终端IED设备的计算和通信开销,从而简化了系统实现的复杂度和实施的难度。该加密算法既能发挥DES算法加密速度快、安全性比较高,同时也发挥了RSA算法密钥管理方便的优点。

由于可能存在MAC地址或者IP地址的伪造,上一级的过滤有可能存在一些没有被过滤掉的访问对象及所携带的信息。此时访问过滤方案描述如下。

(1)终端、子站、主站的IED携带信息进入信息网。

(2)终端IED和子站进行共享密钥认证。

(3)终端IED进行共享密钥认证技术后,将执

行如下操作: ①对于认证成功的终端 IED 所携带的电力敏感信息进行 DES 加密,然后对其密钥用 RSA 加密作为对应终端 IED 的公开密钥,把加密的数据和加密后的密钥传送给子站。子站收到终端 IED 的信息后,子站用保留的私用密钥先对密钥进行 RSA 解密,然后对其加密数据解密。②对于认证失败的终端,把终端的唯一标识符及其所携带的信息添加到敏感数据库,进行封存过滤。③对于数据解密成功,数据采集端保存数据。否则终止其访问权,将终端加入敏感数据库。

5 实例分析

网络化的通信结构和多种通信技术在同一个网络中的综合运用,扩大了网络的规模,增加了网络的复杂性,给网络的运行维护增加了很大的困难。熟知智能配电网通信系统三层网络模型建立如图 4 所示的通信网络。为了方便演示,服务端采用的是单线程。在 VS2010 平台上用 c#开发时是一对一(一个服务器对一个客服端) ,但不影响在实际中的应用。

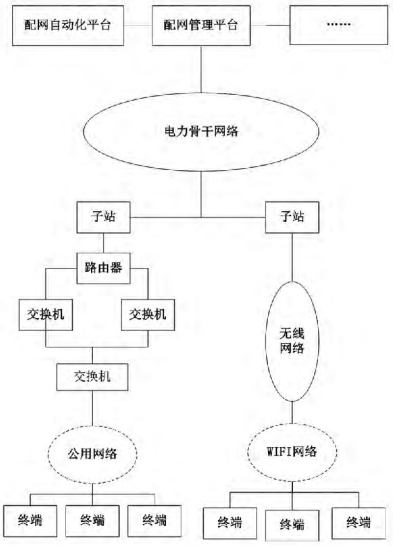

图 4 智能配电网通信系统三层网络模型

信息通信技术给系统带来保护与控制便利的同时[9],也带来了安全隐患。在安全通信领域,访问控制具有重要的基础性作用。基于上述通信系统模型,利用该方案,能够保证非法使用的终端 IED 无法接入到系统中,从而阻止非法入侵者对系统的恶意攻击。分析如下。

首先,由于电力自动化系统严格的集中化管理等特点,设备身份认证(Authentication) 技术和共享密钥认证有效保障智能电网的信息安全的可靠度,同时将不合法的终端 IED 的信息封存在数据库,提高了拦截效率。

其次,在终端 IED 经过第一级过滤和公共密钥认证后,客户端把需要发送的明文经过综合加密技术后,信息传送到服务端,服务端先用私钥解密加密过的密钥,经过解密的密钥再进行解密加密过的数据(如图 5 所示) ,因此防止了密钥泄漏问题。电力信息进行综合加密提高了加密效率和数据的安全性。即使对于有些侥幸不合法的终端 IED 获取访问或者获取电力敏感信息也是经过综合加密的信息,在保证信息的安全度的同时也给破解电力信息带来一定的难度。由于采用多重认证机制,该机制阻止了非授权使用的终端用户或者设备接入智能配电系统。

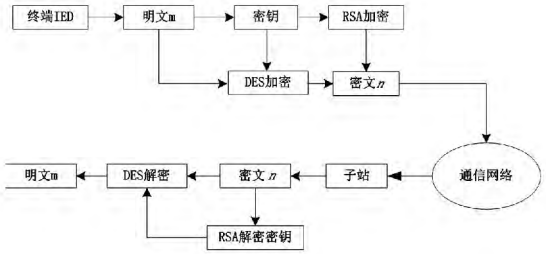

图 5 子站和终端综合加密解密

最后,对于采用的对称加密算法,不影响数据的实时性。由于多级的过滤非授权的终端,阻止了不法分子的访问、截获、篡改电力信息,为配电通信网的安全提供保障措施。

6 结 语

未来智能电网从整体上可以看作是由电力网和信息网构成的相互依存的复合网络,其中信息网络的安全及其对电力系统运行安全带来的风险不容忽视。在智能配电网通信系统结构设计的基础上,针对智能配电网存在的信息安全问题,采用基于多级过滤和综合加密体制,提出了一种适合智能配电网通信系统的信息控制访问方案。该方案减轻了终端 IED 设备的计算和通信开销,同时实现了终端合法性认证问题。尽管只是针对智能配电网而提出,该方案所基于的理论体系可很容易推广应用到智能电网信息安全的其他层次,从而为解决智能电网信息安全问题提供了一种新思路。

参考文献

[1] 刘振亚. 智能电网技术 [M]. 北京: 中国电力出版社, 2010.

[2] 余贻鑫, 栾文鹏. 智能电网述评 [J]. 中国电机工程学报, 2009, 29 (34): 1-8.

[3] 李文伟, 邱利斌. 配网自动化及通信系统的规划建设 [J]. 电力系统通信, 2009, 30(196): 5-7.

[4] Hamlyn A, Cheung H, Mander T, et al. Computer Network Security Management and Authentication of Smart Grids Operations [C]//IEEE Canada Electrical Power Conference. 2008: 31-36.

[5] BOYER W F, MCBRIDE S. Study of Security Attributes of Smart Grid Systems - Current Cyber Security Issues [EB/OL]. [2009-04-29]. http://www.inl.gov/scada/publications/d/securtng the smart grid current issues.pdf.

[6] 苏贵洋, 马颖华, 李建华. 一种基于内容的信息过滤改进模型 [J]. 上海交通大学学报, 2004, 38(12): 2030-2034.

[7] 刘晓星, 胡畅霞, 刘明生. 公钥加密算法 RSA 的一种快速实现方法 [J]. 微计算机信息, 2006(22): 118-119.

[8] 朱作付, 徐 超, 葛红美. 基于 DES 和 RSA 算法的数据加密传输系统设计 通信技术 [J]. 2010, 4(43): 90-93.

[9] 孙中伟, 马亚宁, 王一蓉, 等. 基于 EPON 的配电网自动化通信系统及其安全机制研究 [J]. 电力系统自动化, 2010, 34(8): 72-75.

[10] SUN Zhong-wei, HUO Si-tian, MA Ya-ning. Security Mechanism for Smart Distribution Grid [C]//The 2nd IEEE International Conference on Advanced Computer Control. 2010: 967-971.

[11] Lim I H, Hong S, Choi M S, et al. Security Protocols against Oyber Attacks in the Distribution Automation System [J]. IEEE Trans on Power Delivery, 2010, 25(1): 448-455.

作者简介:

李 貌(1988), 硕士研究生, 研究方向为调度自动化及计算机信息处理;

滕 欢(1965), 高级工程师, 硕士研究生导师, 长期从事电力系统及其自动化科研、教学及工程实践工作。

(收稿日期: 2014-04-10)

(上接第65页)

估方法, 并经过实际测试计算数据与仿真模型计算数据对比, 验证了电力机车模型的正确性以及多谐波源负荷谐波电流评估方法的正确性, 为今后做电气化铁路谐波电流评估提供了可以借鉴的数据和参考方法。

参考文献

[1] 陶骞. 多谐波源系统谐波叠加算法的研究 [J]. 湖北电力, 2008, 32(6): 6-8.

[2] 江佩斯. 多谐波源随机谐波电流叠加问题的研究 [D]. 北京: 华北电力大学, 2008.

[3] 刘友梅. 韶山3型电力机车 [M]. 北京: 中国铁道出版社, 1990.

[4] 余卫斌. 韶山9型电力机车 [M]. 北京: 中国铁道出版社, 2006.

[5] 廖洪涛. 和谐 HXD1 型大功率交流电力机车概述 [J]. 电力机车与城轨车辆, 2007, 30(1): 7-10, 32.

[6] 张忠玉. HXD3 电力机车交流传动系统设计研究 [D]. 大连: 大连交通大学, 2008.

[7] 王立民, 郝凤荣. HXD3 型交流传动电力机车电气系统 [J]. 铁道机车车辆, 2008, 28(增刊): 5-8, 23.

[8] 余新才, 彭昌永, 施通勤, 等. CRH2 型电力机车建模与谐波电流分析 [J]. 武汉大学学报: 工学版, 2012, 45(1): 107-110.

[9] A. Mansoor, W. M. Grady, A. H. Chowdhury, M. J. Samotyj. An Investigation of Harmonics Attenuation and Diversity Among Distributed Single-phase Power Electronic Loads [J]. IEEE Transactions on Power Delivery, 1995, 10(1): 467-473.

[10] J. M. Crucq, A. Robert. Statistical Approach for Harmonics Measurements and Calculations [J]. IEE Conference Publication No. 305, Part 1: Contributions, Subject Area: 2, 1989(2): 91-96.

[11] V. Cuk, J. F. G. Cobben, W. L. Kling, R. B. Timens. An Analysis of Diversity Factors Applied to Harmonic Emission Limits for Energy Saving Lamps [C]. 2010 14th International Conference on Harmonics and Quality of Power (ICHQP), 2010: 1-6.

[12] Sahel Uddin, Hussain Shareef, Azah Mohamed, MA Hannan. An Analysis of Harmonic Diversity Factors Applied to LED Lamps [C]. 2012 IEEE International Conference on Power System Technology (POWERCON), 2012: 1-5.

作者简介:

沈 峰(1973), 工程师, 硕士, 主要从事工厂供配电设计、施工、运行, 电能质量研究与治理。

(收稿日期: 2014-04-23)