电力信息系统身份鉴别技术的研究

胡朝辉 梁智强
(广东电网公司电力科学研究院智能电网所 广东 广州 510080)

摘 要 电力信息系统为电力的生产、输送、变电和分配提供了极大的帮助,是电力自动化系统的重要组成部分。电力信息系统的安全涉及到人民的切身利益和国家安全,其安全性必须得到保证。信息系统的等级保护为电力信息系统的安全提供了有力的保障,分析电力信息系统中身份鉴别技术的现状和特点,针对电力信息系统的特点,提出一种基于 SM2 算法的身份鉴别方法。SM2 算法相对于 RSA 算法具有运算速度快、安全性高等优点,目前已经成为国家密码管理局推荐的算法。首先介绍基于 SM2 算法实现身份鉴别的原理,阐述了在电力信息系统中基于 SM2 算法的身份鉴别系统的实现,最后给出了基于 SM2 算法的身份鉴别技术的结论。基于 SM2 算法的身份鉴别系统能够很好地解决电力系统身份认证的问题,并为系统用户行为的审计提供支持,具有很强的应用性。

关键词 非对称密码算法 SM2 身份鉴别 等级保护 电力信息系统

中图分类号 TP3 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2013.12.084

RESEARCH ON AUTHENTICATION TECHNIQUE IN ELECTRIC POWER INFORMATION SYSTEM

Hu Zhaohui Liang Zhiqiang
(*Smart Grid Institute, Electric Power Research Institute of Guangdong Power Grid Corporation, Guangzhou 510080, Guangdong, China*)

Abstract As one of the most important parts of the power automation system, power information system contributes greatly to the power generation, transmission, substation and distribution. Since the security of power information system relates to the vital interests and national security of the country and people, its safety must be guaranteed. Classified protection of information system security provides a strong guarantee for the safety of the power information system. We analyse present situation and features of authentication technique in power information system, in light of the feature of power information system, we propose an SM2 algorithm-based authentication method. SM2 algorithm has the advantages of fast operation speed and high security in contrast to RSA algorithm, and has been the algorithm recommended by the State Cryptography Administration. In the paper we first introduce the principle of authentication implementation based on SM2 algorithm, then expatiate on the implementation of the SM2 algorithm-based authentication system in power information system, and at last we provide the conclusion of the SM2 algorithm-based authentication technique. This authentication system can well solve the authentication issue in power information system, and is able to provide support for auditing the system users' behaviours, it has very strong applicability.

Keywords Asymmetric cryptographic algorithm SM2 Authentication Classified protection Power information system

1 电力系统中的信息系统安全等级保护

近年来,随着信息技术的发展,网络安全问题日益突出,黑客入侵以及网络攻击现象日益增多,而随着计算机网络技术的不断普及,公众使用计算机的次数越来越多,特别是公用信息基础设施建设使得政府、企业日益依赖信息系统,一些涉及国计民生的业务、系统受到了前所未有的安全挑战。如维基解密网站泄漏了大量政府的机密信息;花旗集团受到黑客攻击导致 36 万多的客户账户信息被窃取;CSDN 网站被攻击导致 600 余万用户资料被泄漏等。这些事故充分说明了网络安全对国家、政府和企业的重要性。

信息系统安全不仅受到了企业的重视,同样得到了政府的高度关注。公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合颁布了关于印发《信息安全等级保护管理办法》的通知,要求公民、法人和其他组织对信息系统分等级实行安全保护,对等级保护工作的实施进行监督、管理[1]。信息系统等级保护是指对国家、企业、公民的信息在存储、传输和处理等过程中按照国家的相应要求进行分级保护,对信息系统设备进行等级化管理,对信息系统安全事故进行等级化处理[2]。

现阶段,电力的生产、输送、变电和分配广泛使用信息系统及各种自动化控制设备,如发电厂计算机监控系统、变电站自动化系统、能量管理系统、调度自动化系统和配网自动化系统等。电力系统的安全涉及到国家的安全,大面积停电事故不仅会带来严重的经济损失,而且会危及到国家安全及社会稳定,因此必须强化电力信息系统的安全防护。为此,国家电力监管委员会颁布了《电力二次系统安全防护规定》,用于指导电力信息系统的等级保护工作;国家电网公司、南方电网公司也分别制定了《国家电网公司信息化"SG186"工程安全防护总体方案(试

收稿日期:2012 - 08 - 14。**胡朝辉**,助理工程师,主研领域:通信安全,等级保护。**梁智强**,高工。

行)》和《中国南方电网电力二次系统安全防护技术规范》,用于电力信息系统的安全防护。

身份鉴别技术是等级保护的重要内容,电力行业使用的信息系统(如主机、数据库和应用系统)广泛使用口令技术对用户的身份进行验证,然而密码口令的安全强度有限,易被破解,特别是部分供电局为了系统维护的方便,将主机、数据库等管理密码交与厂家维护人员,极大地增加了系统的风险。

本文根据电力信息系统身份鉴别技术的现状,分析了现有身份鉴别技术的优缺点,本着易使用、高安全防护强度的原则,设计一种基于 SM2 算法框架的身份鉴别系统。本文的重点在于基于 SM2 算法的身份鉴别技术的原理分析及基于 SM2 算法的身份鉴别技术的系统实现。

2　身份鉴别技术

身份鉴别可以简单理解为一个人或者系统对另一个人或者系统关于其身份真实性的认证过程[3]。GB/T 22239 – 2008《信息安全技术信息系统安全等级保护基本要求》中对各级的信息系统的身份鉴别有着不同的要求:如对二级信息系统/三级信息系统均要求"操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点,口令应有复杂度要求并定期更换;应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别";对四级信息系统要求"操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点,口令应有复杂度要求并定期更换,并且身份鉴别信息至少有一种是不可伪造的"[4]。

2.1　身份鉴别技术的类型

身份鉴别技术是信息安全的第一道门槛,只有通过身份认证的用户才能拥有对系统的访问权、使用权等。根据身份鉴别技术实现鉴别的依据,其可以分为如下三类[5]:

1) 根据用户所知的信息来实现身份认证,如口令、密码等;

2) 根据用户所有的信息来实现身份认证,如证书、令牌等;

3) 根据用户的特征实现身份认证,如人脸、掌纹、虹膜、指纹和声音等[5]。

2.2　身份鉴别技术优劣性分析

基于用户所知的身份鉴别技术简单、灵活并且费用较低,因此广泛用于主机系统、数据库的登录。电力信息系统中的大部分主机、数据库均采用口令进行认证,但是该身份鉴别技术的缺点较明显:安全防护强度较低,容易被破解、窃取或者丢失,特别是部分供电局为了系统维护方便,将部分运行系统的口令交给厂家维护人员,极大地增加了系统的风险。

基于用户特征的身份鉴别技术具有很高的安全性,它一般基于个人独有的特征来实现身份认证,然而生物特征认证系统的成本较高,因此其一般用于银行、机场等。

在电力信息系统中,绝大部分信息系统均为三级信息系统。根据《信息安全技术信息系统安全等级保护基本要求》,必须采用两种以上组合的鉴别技术对管理用户进行身份鉴别[4]。由于电力信息系统均处于专用机房内,因此其门禁系统可作为第一种鉴别技术。第二种身份鉴别技术一般采用口令技术。考虑到口令技术过于简单,虹膜/指纹鉴别技术过于昂贵等特点,本文提出一种基于 SM2 算法的身份鉴别技术,该技术使用 USB-KEY 保存用户的信息,通过 SM2 算法实现用户信息和系统之间的身份认证。

3　基于 SM2 算法的身份认证原理

3.1　SM2 算法加解密过程

SM2 算法由国家密码管理局提出,其实质为椭圆曲线公钥密码算法,国家密码管理局为满足电子认证服务系统等应用需求,对 SM2 椭圆曲线公钥密码算法推荐了曲线参数[6,7]。公钥密码算法一般用于身份认证和进行数据通信加密的会话密钥协商。公钥密码算法又称非对称密码算法,其思想最初由 Deffie 和 Hellman 于 1976 年提出[8,9],该算法拥有一对密钥:公钥和私钥,其加解密过程如图 1 所示。

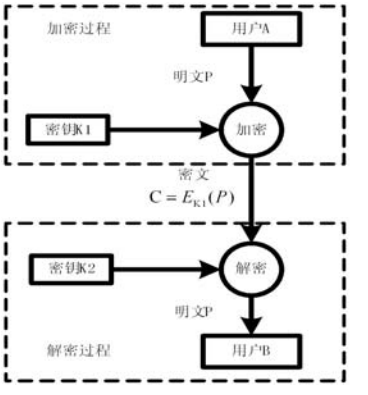

图 1　非对称密码算法加解密示意图

图 1 适用于用户 A 向用户 B 发送数据。其中密钥 K1 用于数据的加密,密钥 K2 用于数据的解密;K1 和 K2 必须配合使用,否则将不能得到正确的明文 P;$E_{K1}(P)$ 代表使用密钥 K1 对数据 P 进行加密运算;K1 和 K2 有公私钥之分,私钥由用户保存,不公开且不进行传输,公钥是公开的,由发布机构进行认证和发布;公钥和私钥在数值上不相等,且由 K1 并不能推导出 K2,反之亦然。K1 和 K2 是非对称密码算法的 2 个参数,一般由通信实体产生。

3.2　SM2 算法的应用形式

在电力信息系统中,数据的传输广泛采用加密技术,如各级调度机构之间的数据传输、主站和厂站之间的数据传输等,生产业务系统的数字证书系统同样采用 RSA 密码算法。由于 RSA 算法在运算速度和加密强度等方面均弱于 SM2 算法,因此,电力信息系统将逐渐淘汰 RSA 算法,而采用国家密码局推荐的 SM2 算法。在实际应用当中,SM2 算法有三种应用形式,如图 2 所示。

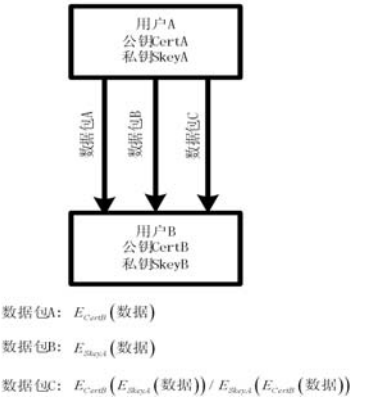

图 2　非对称密码算法的应用形式

图 2 适用于用户 A 向用户 B 发送数据,用户 A 和 B 的公私钥对分别为(CertA,SkeyA)和(CertB,SkeyB)。

1) 使用 B 的公钥 CertB 加密数据,则即使窃取了密文数据包 E_{CertB}(数据),亦无法对其破解,因为只有用户 B 才拥有私钥 SkeyB,这就实现了数据传输的机密性;

2) 使用 A 的私钥 SkeyA 加密数据,B 接收到信息后,使用

A 的公钥 CertA 进行解密。若数据经过验证是正确的(非第三方冒充),就能得出数据肯定由 A 发出,A 不可抵赖的结论(因为第三方不可能拥有 A 的私钥),这就实现了数据传输的不可抵赖性;

3) 使用 B 的公钥 CertB 和 A 的私钥 SkeyA 进行双重加密,就能实现数据传输的机密性和不可否认性。

3.3 数字签名算法

SM2 的第二种应用形式实现了数据传输的不可抵赖性。在电力信息系统中,很少采用私钥对整个数据加密进行不可抵赖的运算,而是首先对数据进行 hash 运算,再使用私钥加密,并将加密结果添加到源数据中,这就是数字签名算法,其发送端和接收端处理数据的过程如图 3 所示。

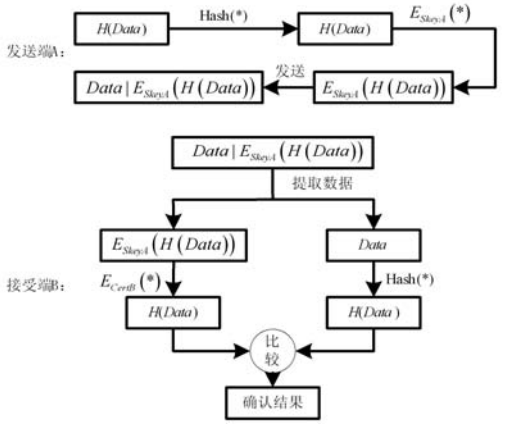

图 3 数字签名算法示意图

3.4 SM2 算法的数字证书系统

SM2 算法仅仅解决了数据传输机密性及数据传输的不可抵赖性问题,并未解决通信实体本身身份的合法性问题。在基于 SM2 算法的身份认证系统中,还需要证书机构 CA 和注册机构 RA 来确定用户实体的身份合法性。在本系统中,采用 X.509 的证书标准,证书的格式如表 1 所示[10,11]。

表 1 X.509 数字证书标准

英文域名	含义
Version	数字证书的版本号
Serial number	数字证书的序列号
Issuer	数字证书颁发者的名字
Validity period	数字证书的有效期
Subject name	数字证书所有者的名字
Public key	数字证书所有者的公钥
Issuer ID	数字证书颁发者的 ID
Subject ID	数字证书所有者的 ID
Extensions	扩展域
Signature	使用 CA 中心私钥对证书所有者的公钥的签名

通信实体首先向注册中心提出申请,注册机构审核通信实体的资料,将合法的申请者的资料提供给证书机构。证书机构 CA 是整个系统的信任机构,它为通信实体制作数字证书。通信实体的数字证书包含 CA 对通信实体公钥的数字签名,因此通过 CA 的数字证书验证通信实体的公钥。

此外系统中还包含有目录服务器,用于公布证书列表和证书撤销列表 CRL,通信实体接收到数据包以后就会根据数据包的内容到目录服务器中查找相应的数字证书,并确定其合法性。

4 基于 SM2 算法的身份认证的实现

供电局内的生产业务系统的典型配置如图 4 所示,部署有 EMS 能量管理系统服务器、历史数据服务器、SCADA 服务器等,调度员通过管理终端工作站来管理、监控电力生产系统。

基于 SM2 算法的身份认证系统采用 USB-KEY 的登录方式。USB-KEY 中包含用户的身份及私钥信息,并通过认证中心的认证获得其访问系统的权限,其主要基于 PKI 的认证体系。基于 SM2 算法的身份认证系统的证书目录服务器和认证服务器在生产业务系统中离线部署。

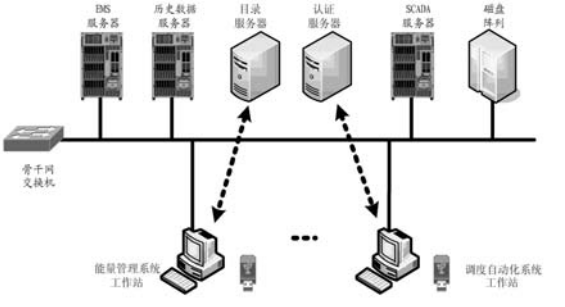

图 4 基于 SM2 算法的身份认证系统逻辑图

4.1 USB-KEY 的证书签发

数字证书系统为 USB-KEY 制作证书的过程(如图 5 所示):

1) USB-KEY 接入数字证书系统,数字证书系统对其初始化处理,USB-KEY 内部电路产生公私密钥对;

2) USB-KEY 产生证书请求,并将证书请求文件 P#10 发送至数字证书系统;

3) 数字证书系统根据 P#10 文件,按照 X.509 的格式制作该 USB-KEY 的数字证书,该数字证书中包含数字证书系统的数字签名。

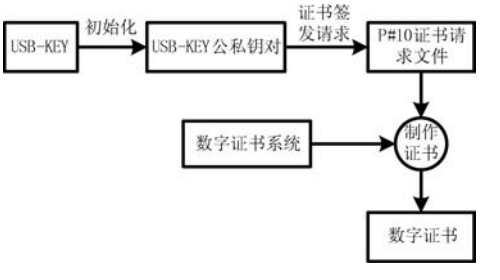

图 5 USB-KEY 的数字证书制作过程

USB-KEY 获取到数字证书系统签发的数字证书以后,将对 USB-KEY 使用者的信息进行数字签名,如图 6 所示。

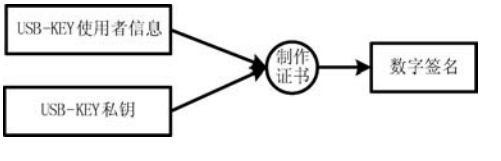

图 6 USB-KEY 对使用者的信息进行数字签名

4.2 管理终端的证书签发

数字证书系统同样需要为管理终端工作站签发数字证书,主要是指为管理终端工作站安装数字证书系统的根数字证书,该数字证书中包含证书系统的公钥。

签发证书的格式类始于 USB-KEY 的证书签发过程,同时数

字证书系统将管理终端工作站的登录方式更改为 USB-KEY 的登录方式。

4.3　基于 SM2 算法的身份认证过程

基于 SM2 算法的身份认证过程主要基于数字证书系统签发的数字证书和 USB-KEY 的数字签名来实现,其过程简述如下:

1) USB-KEY 接入管理终端工作站,用户通过 PIN 码认证的方式获得 USB-KEY 的认证;

2) 管理终端工作站读取 USB-KEY 中的数字证书、序列号、使用者的数字签名信息等;

3) 管理终端工作站根据自身安装的数字证书及 USB-KEY 的数字证书来验证 USB-KEY 的合法身份,其主要过程是根据证书系统的公钥验证 USB-KEY 中数字证书的签名,根据验证签名的结果判断 USB-KEY 的数字证书系统是否是伪造。若签名验证通过,则可以判断 USB-KEY 设备公钥属于真实的设备公钥;

4) 管理终端工作站根据获取的 USB-KEY 设备公钥验证 USB-KEY 对使用者的数字签名,若通过该数字签名的验证,则判断用户身份合法,并允许该用户登录,否者阻止该用户登录。

5　结　语

本文讨论了电力信息系统中的等级保护技术,分析了电力信息系统中身份鉴别的现状,针对现存使用的口令方式身份鉴别安全强度较低的缺点,提出了一种基于 SM2 算法的身份鉴别技术。

本文分析了在电力信息系统中使用 SM2 算法实现身份鉴别的原理,并给出了使用该算法实现身份鉴别的主要过程,采用 USB-KEY 方式的身份鉴别系统具有较强的操作性。相比于 RSA 等非对称密码算法,SM2 密码算法具有加密速度快、加密强度高等特点,因此,基于 SM2 算法的身份鉴别技术系统能够达到很高的身份鉴别强度。

参　考　文　献

[1] 公安部,国家保密局,国家密码管理局,国务院信息化工作办公室. 关于印发《信息安全等级保护管理办法》的通知[S]. 2007.

[2] 王超,卢志刚,刘宝旭. 面向等级保护的漏斗扫描系统的设计与实现[J]. 核电子学与探测技术,2010(7).

[3] 黄泽鑫. 基于动态密码认证的防火墙研究[D]. 武汉科技大学,2009.

[4] GB/T 22239-2008/信息安全技术信息系统安全等级保护基本要求[S]. 2008.

[5] 吕鑫. PKI 中的私钥管理研究[D]. 天津财经大学,2009.

[6] 国家密码管理局. SM2 椭圆曲线公钥密码算法[S]. 2010.

[7] 国家密码管理局. SM2 椭圆曲线公钥密码算法推荐曲线参数[S]. 2010.

[8] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22: 644 - 654.

[9] William Stallings. 密码编码学与网路安全:原理与实践[M]. 刘玉珍,王丽娜,傅建明,译. 2 版. 北京:电子工业出版社,2004.

[10] Housley R, et al. Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile[EB/OL]. 2002. http://www. ietf. org/rfc/rfc3280. txt.

[11] 杜海. X. 509 证书和 RBAC 在 Web 中的应用[D]. 电子科技大学,2005.

(上接第 283 页)

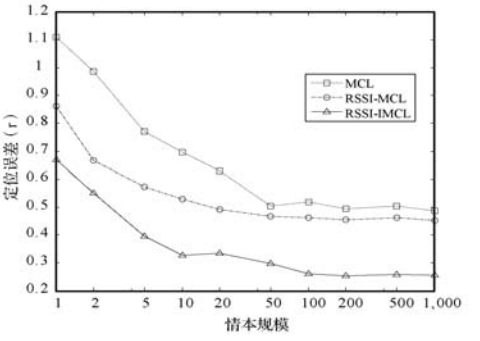

图 6　定位误差随样本规模变化曲线

3　结　语

本文对基于 RSSI 的蒙特卡罗无线传感器定位算法进行了深入研究,提出了一种基于 RSSI 的改进蒙特卡罗定位算法。该算法在定位精度、收敛速度、计算量、对锚节点密度的要求、对粒子样本的要求等多个方面的性能均有提升,证明该算法是一个可以在无线传感器网络环境中使用的高效的定位算法。该算法可广泛运用于室内人员定位系统、矿井人员定位跟踪系统等诸多领域。

参　考　文　献

[1] Hu L, Evans D. Localization for mobile sensor networks[C]//Proceedings of MobiCom'04, Philadelphia, Pennsylvania, USA, 2004: 45 - 57.

[2] Baggio A, Langendoen K. Monte Carlo localization for mobile wireless sensor networks [J]. Ad Hoc Networks, 2008, 6(5): 718 - 733.

[3] Rudafshani M, Datta S. Localization in wireless sensor networks[C]// The 6th International Symposium on IPSN, Cambridge, MA, USA, 2007: 51 - 60.

[4] Stevens-Navarro E, Vivekanandan V, Wong V W S. Dual and mixture Monte Carlo localization algorithms for mobile wireless sensor networks [C]//IEEE Wireless Communications and Networking Conference, Hong Kong, China, 2007: 4027 - 4031.

[5] Yi J, Yang S, Cha H. Multi-hop-based Monte Carlo Localization for Mobile Sensor Networks[C]//Proceedings of IEEE SECON'07, San Diego, California, USA, 2007: 162 - 171.

[6] Dil B, Dulman S, Havinga P. Range-based localization in mobile sensor networks [C]//Proceedings of EWSN'06, Zurich, Switzerland, 2006: 164 - 179.

[7] Wang W D, Zhu Q X. RSS-based Monte Carlo localization for mobile sensor networks [J]. IET Communications, 2008, 2(5): 673 - 681.

[8] Patwari N, Hero A. O, Perkins M, et al. Relative location estimation in wireless sensor networks[J]. IEEE Trans. Signal Process. 2003, 51(8): 2137 - 2148.

[9] Rappaport T. Wireless communications: principles and practice [M]. Prentice-Hall: New Jersey, 2002.

[10] Doucet A, Godsill S, Andrieu C. On sequential Monte Carlo sampling methods for Bayesian filtering [J]. Statistics and Computing, 2000, 10 (3): 197 - 208.

[11] Camp T, Beleng J, Davies V. A survey of mobility models for ad hoc network research [J]. Wireless Communications & Mobile Computing, 2002, 2(5): 483 - 502.