基于 USB Key 的配电网自动化系统身份认证机制研究与设计

周振华[1]，吕继伟[1]，徐若然[1]，冒蕾蕾[2]
（1. 国网电力科学研究院，北京 102200；2. 北京电研华源电力技术有限公司，北京 102200）

摘 要：现有配电网自动化系统终端设备面临来自外部网络攻击的风险。通过提出一种利用 USB Key 简便型硬件载体作为身份认证的安全机制，提升配电网自动化终端设备就地操作的安全性和可靠性，从而减小外部攻击通过末端设备侵入系统网络的概率。针对配电网系统容易面临的安全风险对基于 USB Key 的安全身份验证等关键性问题进行了分析，并设计了配电网系统安全身份验证的总体架构和基于“一次一密双向验证”以及“多因子验证”机制的流程。该机制采用请求－响应模式，增强了认证强度，提高了机制的安全性，并且降低运算时间复杂度，提高了加解密算法的整体运行效率。

关键词：配电网；身份认证机制；双向认证；多因子认证

作者简介：周振华（1983），男，硕士，工程师，研究方向为配电自动化技术。

中图分类号：TM764.2　　**文献标志码**：A　　**文章编号**：2095－1256(2015)01－0053－05

Research and Design of Power Distribution Network Automation System Authentication Mechanism Based on USB Key

ZHOU Zhen-hua[1], LV Ji-wei[1], XU Ruo-ran[1], MAO Lei-lei[2]
(1. State Grid Electric Power Research Institute of China, Beijing 102200, China;
2. Huayuan Electric Power Technology Co., Ltd., Beijing 102200, China)

Abstract: The existing distribution network automation system terminal equipment may be at risk from the external network attack. In this paper, a convenient hardware carrier based on USB Key is presented as authentication security mechanism in order to improve security and reliability of the terminal equipment in operation, and reduce the probability of external attack intrusion via the terminal equipment. In view of the security risk of the distribution network system, this paper analyzes such key problems as security authentication based on USB key, and designs the overall architecture of security authentication, as well as the authentication process based on "one password at a time two-way authentication" and "multifactor authentication mechanism". The mechanism adopts the request-response model to enhance the certification strength, improve the system security, reduce the computing time and complexity, and improve the overall efficiency of encryption algorithm.

Key words: power distribution network; identity authentication mechanism; two-way authentication; multifactor authentication

1 配电网自动化二次系统安全防护概述

随着网络信息技术的不断发展，网络信息安全已成为社会关注的热点。智能配电网建设过程中实施的配电自动化系统，主要包括配电终端、配电网通信设备、数据网络以及监控主站系统设备等，是电力系统面向最终用户供电的重要基础设施。配电环节作为用户供电的最后一个环节，在保证供电可靠性和质量的基础上，进一步完善信息安全和防止恶意破坏是系统需要考虑的另一重要问题。作为电力系统二次设备，其安全防护的目标是抵御病毒、黑客等通过各种形式发起的恶意破坏和攻击，尤其是集团式攻击，重点保护电力实时闭环监控系统及调度数据网络的安全，防止由此引发的电力系统事故。随着配电网快速发展，配电二次系统的安全问题已经非常突出。2006 年电监会发布了《电力二次系统安全防护总体方案》及配套的《配电二次系统安全防护方案》，对配电网自动化系统、电力负荷管理系统等二次系统的安全防护措施做出了原则性规定。2011

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

年国家电网公司制定了《中低压配电网自动化系统安全防护补充规定(试行)》,对配电网二次系统安全防护方案中的相关措施做进一步细化与补充。

电力二次系统安全防护的总体原则是"安全分区、网络专用、横向隔离、纵向认证"。配电网自动化系统主站与子站及终端的通信方式原则上以电力光纤通信为主,对于不具备电力光纤通信条件的末梢配电终端,采用无线通信方式,这样就容易使配电二次系统面临来自公共网络攻击的风险,可能会引起恶意攻击设备事故。因此,配电网自动化系统的安全防护,除了遵循电力二次系统安全防护总体原则,还应防止通过公共网络对子站终端进行攻击,造成用户供电中断,同时防止通过公共网络和用户终端入侵主站,造成更大范围的安全风险。目前的解决方案是在终端设备上配置安全加密模块,安全加密模块对来源于主站系统的控制命令和参数设置指令采取安全鉴别和数据完整性验证措施,以防范冒充主站对子站终端进行攻击,恶意操作电气设备,影响供电安全。

但对于终端以及子站设备的就地操作,目前还缺乏有效的信息安全防护机制,尽管目前终端设备具备基本的防窃、防火、防破坏等物理安全防护措施,以及控制远程操作的软硬压板,然而设备一旦通过外部暴力开启物理防护措施后,即可通过操作面板的控制按钮对设备进行操作,或者直接绕开安全加密设备连接子站及终端设备,按照标准规约查看终端的相关数据以及对设备进行遥控操作等,从而进一步侵入配电自动化系统网络。

如何有效防护终端设备的就地安全操作是一个值得思考的问题,借鉴目前互联网的安全防护以及身份识别技术,对配电主站系统以及子站终端采用身份识别技术,增加身份识别机制,从源头确保设备操作的安全和稳定。不论从主站对设备进行远程操作、对终端设备就地进行操作以及数据查看等都需要先进行身份验证,具有不同权限的身份经鉴别后才允许对设备进行操作,同时设备的控制闭锁环节才会打开,允许运维人员的进一步操作。未经身份验证的物理连接和操作控制都被视为非法操作,一旦发生,将会自动提升设备安全防护级别,闭锁全部相关设备的操作控制,并及时向主站上传报警信息并定位,提示系统的异常侵入。

身份认证服务是提供网络系统安全中其他安全服务的前提和基础。如果不能准确识别网络通信端对端实体的真实身份,就不可能建设一个稳定、有序、安全可靠的自动化系统。因此,研制和开发适合配电网自动化系统的身份认证安全机制及技术具有重要意义,能够极大地提升社会经济效益,促进配电网建设的信息化、智能化发展。

2 基于 USB Key 的身份认证技术

USB Key 是一种便携式的硬件载体,具备通用的 USB 接口,内置控制核心或智能芯片,并且可以存储持有人的私有密钥和数字签名证书,利用 USB Key 进行身份验证可以通过内置公钥算法进行,而身份认证的安全性在于私钥保存在 USB Key 中,常规方法难以获得。

USB Key 的优点包括:体积小巧,携带方便,个人 PIN 码保护,安全存储,内置硬件算法。一般地,用户可以通过 USB Key 内部的加密算法生成密钥或者设置个人 PIN 码,来实现内部文件的操作权限。USB Key 的安全性保障从原理上讲,一是提供双因子认证,即 USB Key 硬件介质和个人 PIN 码(密钥),获得 USB Key 的操作权限需要同时获取内外部验证,操作权限获得后要想对其内部文件进行操作还需要持有人提供个人 PIN 码或由 USB Key 内部生成的私钥来实现;二是私钥只从 USB Key 内产生,不会出现在注册计算机中,外部不可见;三是 USB Key 只进行加解密和证书验证操作,不会泄露密钥实现算法,可以确保数据的安全。基于以上优点,USB Key 被广泛应用于电子商务、金融等信息安全要求极高的场合来进行身份验证识别,因此考虑配电网自动化系统采用 USB Key 进行安全身份验证[1]。

针对配电网自动化系统面临的安全风险,USB Key 作为其安全身份验证要着重考虑以下几个问题[2-5]:

(1) 抵抗重放攻击 利用二维认证消息加时间戳、为认证消息添加当前时标以及动态推进认证消息等方法确保认证信息的及时有效,抵抗重放攻击。

(2) 抵抗密码分析攻击 通过对称、非对称加密算法保护以及散列函数(HASH)的单向性

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

来实现认证过程抵抗密码分析攻击，确保加密的安全性。

（3）双向身份认证功能　主站和终端应均能对对方的身份进行验证，防止信息单向传递过程中泄露。

（4）多因子身份认证　高安全强度的身份认证服务往往需要多重因子，即使单一因子的丢失或者泄露也不会引起认证系统的危机或被冒充的风险。

（5）提高身份认证协议的效率　简练并且安全的认证协议可以减少认证通信的次数，提供可靠性，减弱被攻击的风险。

3　基于 USB Key 的配电网自动化系统安全性身份认证机制流程

配电网自动化系统的安全身份认证机制采用动态口令认证机制中的请求—响应方式，可实现客户端和认证服务器的双向认证，同时保证了客户端和服务器认证信息的同步。基于 USB Key 的配电网自动化系统安全性身份认证也需要配电网系统对于该接口设备的支持，系统主站侧和终端侧需要有支持 USB Key 对应的接口，而且还需要支持客户端代理程序的运行。一般地，终端应具备人机交互的显示界面和键盘输入设备，能够输入身份认证的相关信息提供给 USB Key 进行验证。

配电网自动化安全验证系统总体构架如图 1 所示，架构共分为 3 层：第一层主站安全认证系统层，包括配电自动化系统主站服务器、安全认证服务器、Key 注册服务器；第二层为网络层，主要包括系统通信光纤网及通信设备；第三层是设备层，主要包括用户数据、运维操作人员、USB Key 接入设备、终端以及安全加密设备等部分。

身份验证机制的流程要依赖于 3 层系统架构，具体实现分为 3 个阶段：第一阶段为设备注册阶段，主要在主站系统层实现；第二阶段为双向认证及 ID 识别阶段，需要 3 层架构配合实现；第三个阶段为用户注销阶段，由主站系统层实现。

在认证流程执行中，主要用到的加密算法包括：SHA-1，3DES，ECC 等。用户 PIN 为身份识别码，ID 为 USB Key 的 ID 号，此号唯一；R 为随机数；$h_c()$为认证服务器 SHA-1 加密算法的消息函数；$h_u()$为 USB Key 中 SHA-1 加密算法的消息函数；K，K_R，K_L 为 3DES 的算法密钥；$h()$为单项散列函数。

3.1　设备注册阶段[2]

设备注册阶段首先需要在身份认证服务器端完成注册用户接入设备的认证，注册通过后才可以参与设备接入的身份认证。对于用户接入的认证信息，首先由注册服务器为申请用户分配一个 USB Key，并记录该 Key 唯一的 ID 序列号。服务器在本地数据库中为该用户创建一条包含 ID 号、服务器端上次认证信息、服务器端本次认证信息的消息记录。

随后，USB Key 还需要进行 PIN 码和 ID 的

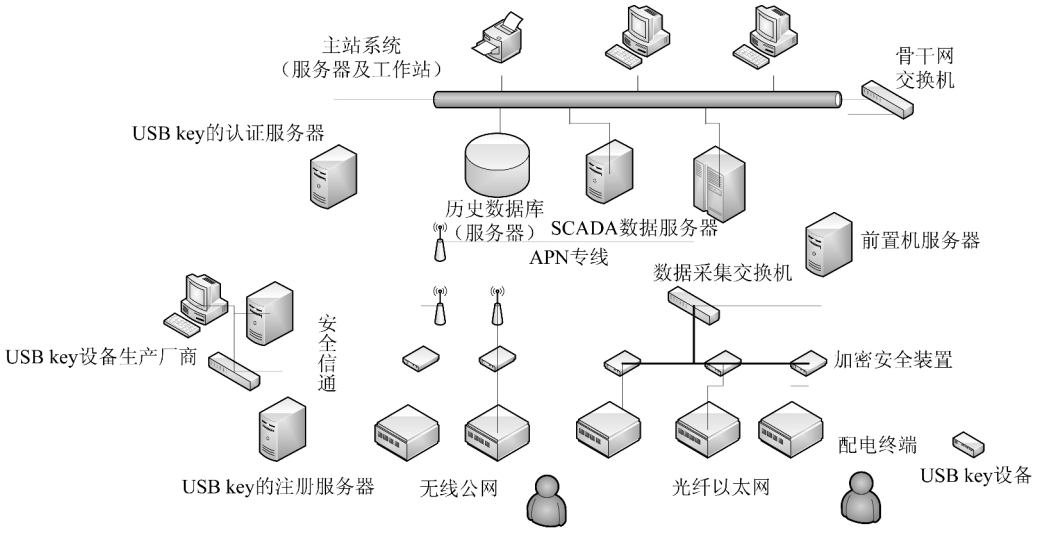

图 1　配电网自动化安全验证系统总体构架

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

注册写入，将两者信息写到 USB Key 硬件存储区域，并且 USB Key 存储该用户 ID 认证过程中所需要的加解密算法。

3.2 认证阶段[2]

3.2.1 用户 PIN 码验证

用户插入 USB Key 至终端设备的 USB 接口，终端液晶界面显示客户端代理程序窗口，用户通过键盘输入 PIN 码，客户端代理程序向 USB Key 端申请发送随机数。

USB Key 收到请求向客户端程序发送一个随机数 R，并标记一次认证。

客户端程序将得到的 R 和 PIN 码进行 3DES 加密得到 E，加密过程算法对应于 $E=DES(K_L)[DES^{-1}(K_R)][DES(K_L[R+PIN])]$，加密后的密文传输给 USB Key。

USB Key 通过 3DES 算法解密 E 得到 R 和 PIN 码，分别与内部存储的 R 和 PIN 码做比对，如果对比一致说明用户为合法用户，然后开启 USB Key－ID 验证程序，同时向终端发送合法用户验证信息，授权用户使用通信信道进行 ID 验证；否则说明用户为非法，将结果返回给客户端的认证程序，显示非法用户信息，并通过终端的通信通道向主站服务器发送报警信息，提示异常非认证接入终端节点。USB Key 用户 PIN 码验证流程图如图 2 所示。

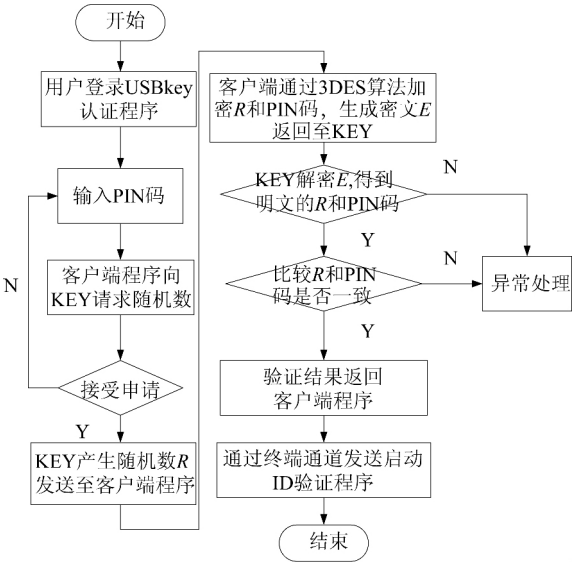

图 2 USB Key 用户 PIN 码验证流程图

3.2.2 USB Key-ID 验证

USB Key-ID 验证过程实际为双向验证，即分别对接入的 USB Key 和认证服务器系统分别进行验证，验证过程如下。

认证服务器接到 USB Key，通过终端发送的请求身份验证信号后，产生随机数 C 传给 USB Key，并用 SHA-1 算法加密 C 得到 $h_c(C)$。

USB Key 接收 C 后，根据 ECC（Elliptic Curve Crypto）算法产生一对密钥（公钥 K_1 和私钥 K_2），并通过同样的 SHA-1 算法加密 C 得到 $h_u(C)$，同时生成一个时间戳 t，发送密文 $m=\{h_u(C),K_1,t\}$ 到认证服务器，请求服务器验证 USB Key 身份，最后再利用 SHA-1 算法加密 K_1，得到 $h_u(K_1)$。认证服务器接收密文 m，解密 m 并提取 $h_u(C)$，与 $h_c(C)$ 对比，如果不相等拒绝对方的链接。

除了验证随机数还需要验证 t' 与 t 之间的有效性。如果 $(t'-t))\geqslant\Delta t$，认证服务器将断开连接，小于间隔时间则接受。其中，t' 是认证服务器的当前时间戳，Δt 是期望的有效时间间隔，此时，USB Key 身份验证完毕。同时，认证服务器将 K_1 用内部存储的 SHA-1 算法加密得到 $h_c(K_1)$，同时生成一个时间戳 T，根据 ECC 算法生成一对密钥（公钥 P_1 和私钥 P_2），发送密文 $M=\{P_1,h_c(K_1),T\}$ 给 USB Key，使 USB Key 验证认证服务器的身份，USB Key 端接收到密文 M 后，通过解密算法提取 $h_c(K_1)$ 并比较 $h_u(K_1)$ 与 $h_c(K_1)$ 是否相等，如果不相等断开链接。

同样地，还需要验证 T' 与 T 之间的有效性。如果 $T'-T\geqslant\Delta T$，USB Key 将断开与服务器连接，否则接受。当 USB Key 确认对方为合法认证服务器身份后，即双向认证过程通过，认证服务器还要验证 USB Key 的 ID 信息，通过 ID 信息可以识别出连接发起人的权限和身份等相关信息，便于开放相应的操作权限，具体过程：USB Key 将 P_1 和 K_2 利用 ECC 加密 $h(ID)$ 和 T，发送 $Z=E_{p1}(E_{K2}(h(ID)+T))$ 给认证服务器。

认证服务器得到 Z 后利用 P_2 和 K_1 进行解密，得到明文 $Z'=D_{P2}(D_{K1}(Z))=h(ID)+T$，比对 T 是否一致，如果一致就将 $h(ID)$ 与数据库中存储的字段进行匹配以确认身份，以便赋予其相关权限；否则断开链接。接入 Key 和认证服务器的双向验证以及 ID 验证流程如图 3 所示。

整个身份安全验证算法过程如图 4 所示。

3.3 注销阶段

用户忘记 PIN 码或丢失 USB Key 硬件设

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

备，需立即联系生产厂商进行索取 PIN 码或者注销。

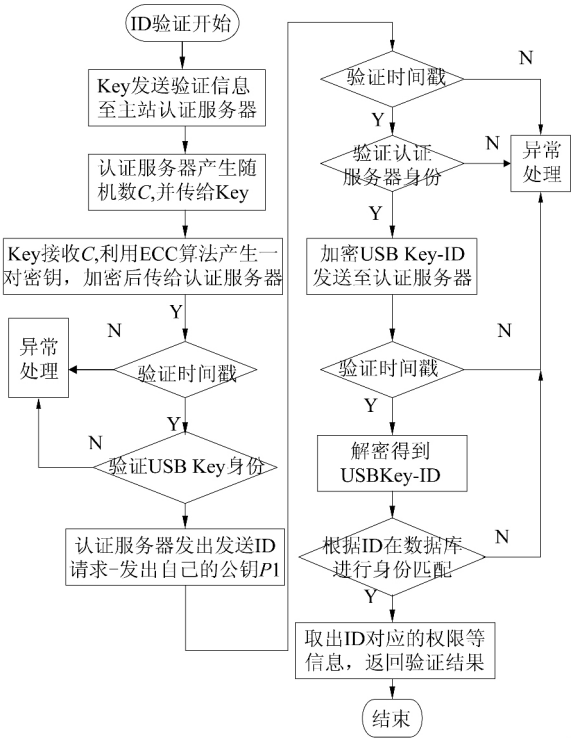

图 3 双向验证以及 ID 识别流程

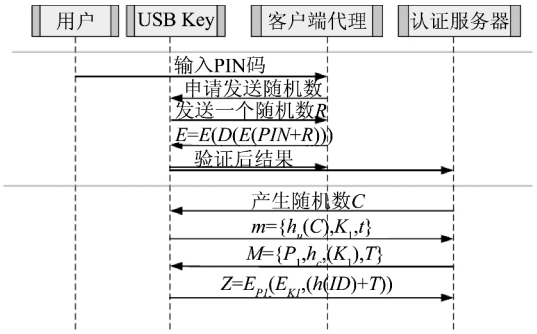

图 4 认证服务器算法过程

4 结论

本文研究了基于 USB Key 技术的配电网自动化安全身份认证机制，设计了配电网自动化安全验证系统总体架构，采用的 USB Key 通过软硬件相结合双向双因子认证模式并基于动态口令认证的请求—响应方式认证协议，实现了配电网末端安全风险的有效防控，并具备了如下功能：

(1)能够抵抗重放攻击；

(2)能够抵抗密码分析攻击；

(3)可实现双向身份认证和多因子身份认证；

(4)提高了身份认证协议的效率。

未来随着保密需求的不断加强，将生物特征识别引入 USB Key，利用生物特征作为 PIN 码，从而确定使用者的确是被授权者，这将在今后 USB Key 发展中成为主要的发展方向。

参考文献：

[1] 宫立圆. 公钥密码算法在 USB Key 中关键技术的研究[D]. 济南：山东大学，2010.

[2] 曹喆. 基于 USB Key 的身份认证机制的研究与实现[D]. 上海：东华大学，2010.

[3] 候孟波. 基于身份和无证书的两方认证密钥协商协议研究[D]. 济南：山东大学，2010.

[4] ZHANG Ping, PEI Ya-nan. A Technology of User Access-Control Table and Identity Authentication Based on USB in LAN[C]. Biomedical Engineering and Computer Science (ICBECS), Wuhan, 2010.

[5] YU Jiang, ZHANG Chuan-fu. Design and Analyis of a USB-Key Based Strong Password Authentication Scheme [C]. Computational Intelligence and Software Engineering (CISE), Wuhan, 2010.

收稿日期：2014-11-19

（本文编辑：赵艳粉）

电力简讯 2014 年我国能源消费增速增速创 16 年来(1999 年至今)最低值

根据中国能源研究会测算，2014 年我国能源消费总量为 38.4 亿吨标准煤左右，同比只增长 2.3%，比 2013 年下降 1.4 个百分点(2013 年能源消费总量增长 3.7%)。能源消费增速增速创 16 年来(1999 年至今)最低值。在这样的基调下，2015 年能源消费总量控制在 40 亿吨标准煤的目标有望实现。

能源局数据显示，2014 年全国用电总量同比增长 3.8%，也创下新世纪以来最低增速。2014 年我国国内生产总值同比增长 7.4%，由此可以测算能源弹性系数为 0.30，电力弹性系数为 0.51，均为近年来的最低水平。这说明，随着经济增速下滑，以及国内产业结构的调整，经济发展对能源的依赖性正在逐步减弱。尤其是在环境保护的约束下，对煤炭、石油等化石能源的需求强度减弱，未来水电、风电等清洁能源将是优先利用资源。

（本刊讯）

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net