基于大数据的电力通信网的安全防护系统及实现研究

尹志成

国网朔州供电公司信通公司，中国·山西　朔州　036000

【摘　要】当前电网规模复杂度越来越高，对电力通信数据依赖程度也在增加，因此为了保证电网的安全可靠运行，本文对电力通信网数据的安全防护系统进行研究与分析。

【关键词】电网安全；电力通信网；安全防护

1　基于大数据的安全通信系统

文中设计的基于大数据的安全通信系统总体框架，如图1所示。在保留传统电力通信系统的结构和框架的基础上，增加了大数据处理中心。

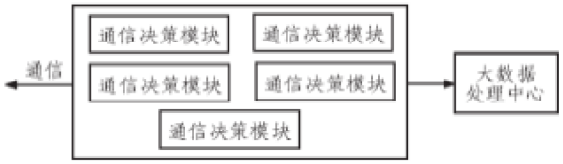

图　1　基于大数据的安全通信系统框架图

1.1大数据存储与处理中心

电力通信大数据处理中心主要是对各种设备信息、通信协议和指令进行存储，通过该数据库实现对电力通信网的资源整合与共享。本文设计了设备、数据、指令和参数4个数据库。

表1　电力设备数据库的逻辑表

字段名	数据类型	是否为主键
EquipNumber	INT	是
EquipID	varchar	否
EquipClass	varchar	否
EquipAdress	varchar	否
GeographyPosition	varchar	否
Status	varchar	否
SetupTime	varchar	否
Department	varchar	否
Priority	varchar	否

1.2数据库安全防护机制

为了保证电力通信大数据系统的安全性和可用性，本文使用“双机热备”模式搭建数据库服务器。该服务器使用虚拟化平台组成服务器集群，增大容灾半径并有效去除单点故障，系统架构如图1所示。

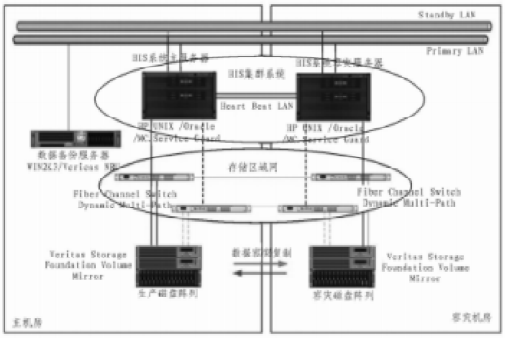

图1 数据库系统架构图

1.2.1数据库管理备份

数据备份的目的是保障数据安全，结合使用逻辑备份和物理备份，每隔一段时间将数据存储在备份服务器上。当系统发生损害或遭受攻击时，将备份数据调入到原数据库系统即可复原。文中使用MySQL提供的备份/恢复工具导出/导入数据，导出过程抽取MySQL的数据信息并保存为二进制文件，且对该文件进行加密，防止滥用；而导入过程则是将所保存的二进制文件恢复到数据库系统。

1.2.2数据库防火墙和审计机制

数据库防火墙即使用黑名单和红名单检测应用程序的合规性，建立数据库防火墙能有效的防止SQL注入攻击，保护大数据系统的安全性。

1.2.3访问控制与口令管理机制

为了保证数据库的安全，本文定期更换SYS和SYSTEM的口令，隔离应用系统管理员与数据库的系统管理员的权限。

2　仿真分析

2.1仿真平台搭建

本文使用Java语言实现整个系统的功能，并搭建仿真环境，模拟仿真系统的工作状况，测试系统的工作效率，以验证本文所提出的基于大数据的安全通信系统的有效性和可用性。仿真系统包括模拟电力设备装置、模拟电力通信平台和通信链路。

2.2系统测试

2.2.1数据分离与存储测试

通过测试系统对不同协议传输数据的识别和转换能力，来测试数据分离与存储功能。测试步骤为：1）设定为DLMS/COSEM通信协议；2）从电力设备发送数据，并观察通信平台接收的数据和数据转换，观察数据库是否成功添加该数据；3）设定为IEC61850通信协议；4）观察通信平台接收的数据和数据转换，并观察数据库是否成功添加该数据。可以发现，当通信协议从DLMS/COSEM切换到IEC61850时，新系统能正确识别传输的数据，并能将其存入数据库。

2.2.2通信协议适配测试

1）使用测试数据模拟通信协议的切换情况，设定协议切换的时间间隔；2）固定时间间隔为500ms，并以协议种类为变量，观察协议适配消耗的时间；3）固定切换协议为DLMS/COSEM到IEC61850，并以切换时间间隔为变量，观察协议适配消耗的时间。

3　结束语

该系统主要包括电力通信模块、大数据中心和数据库安全防护机制，包括：数据库备份机制、数据库防火墙和审计机制、访问控制与口令管理机制、数据加密与屏蔽等。仿真实验结果表明，该系统能高效稳定运行，为电力通信网络和智能电网的建设提供了有益参考。

参考文献：

[1]张旭,方钟,胡楠.面向大数据的电力通信平台建设研究[J].低碳世界,2016(25):21-22.

[2]阳书拥.面向大数据的电力通信平台设计与实现[J].中国新通信,2016,18(7):80-81.

[3]马海风.大数据时代通信网络数字化建设研究[J].中国新通信,2016,18(23):25.