[控制系统]

基于IEC 62351的智能变电站通信系统研究

文/南京工程学院电力工程学院　胡文明　张惠刚　胡　煜

目前的智能变电站在信息安全方面的防护十分薄弱，通信协议普遍缺乏安全措施。由于网络化通信方式的大量应用以及通信协议的标准化，智能变电站很难对蓄意攻击做出有效的防护。基于IEC 62351提出了增强智能变电站信息安全的设计，并制作了原型系统进行实现。

近年来国家大力发展智能电网，变电站的智能化已成为电网发展的方向。智能变电站的主要特点是：全站信息数字化、通信平台网络化、信息共享标准化。相较于传统变电站，智能变电站极大地提高了传输效率，解决了传统变电站调试复杂、互操作性差等问题。然而网络化的通信与标准化的协议也带来了传统变电站所没有的通信安全方面的隐患。智能化变电站一旦遭受网络攻击，会对电网的安全稳定运行造成极大威胁。因此，智能变电站的通信安全问题备受国内外关注。

本文根据数据和通信安全规约 IEC 62351搭建了有安全措施的智能变电站通信系统。

关于IEC 62351标准

IEC 62351标准是由国际电工委员会IEC制定的，针对当前电力系统中广泛使用的计算机、通信和网络技术带来的安全隐患，旨在提高和增强电力系统的数据和通信安全。IEC 62351的核心内容是认证和加密。认证即认证访问者与通信对象的身份，以防止无关人士接触机密信息或取得控制权限；加密即对数据通信进行加密处理，以防止黑客截获或篡改通信数据威胁电网安全。

IEC 62351标准与其他相关标准的关系如图1所示。

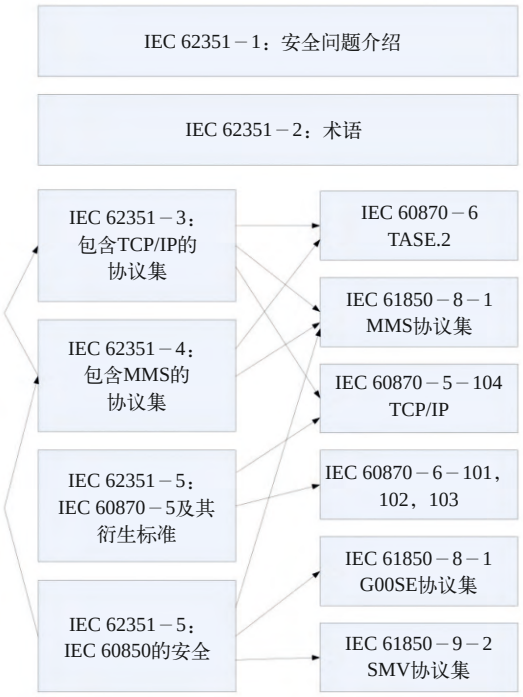

图1　IEC 62351标准与相关标准的关系

变电站通信安全体系的主要内容

1．TCP/IP协议集安全

TCP/IP部分的安全规范针对通信的传输层，其核心内容是在TCP握手协议中添加TLS握手协议以建立安全的TCP连接。

TLS协议全称为安全传输层协议，主要为数据传输提供保密性和数据完整性。协议本身基于TCP，在TCP连接的基础上实现协议版本协商、身份认证、秘钥交换及数据加密解密等功能。

在TCP连接中添加TLS协议时，仍需以socket接口建立TCP握手连接，而后在TCP连接的接口上进行TLS握手连接，完成TLS的秘钥交换和证书认证。并且按照IEC 62351－4的要求，带TLS连接的TCP连接应使用TCP的3782端口代替传统非安全连接时的102端口，以区别安全与非安全的TCP连接。

2．MMS协议集安全

MMS部分的通信安全分为两部分考虑，即应用协议集（A－Profile）和传输协议集（T－Profile）。

T－Profile规定了OSI参考模型中1～4层的协议和要求，这部分与IEC 62351－3中的TCP/IP协议集部分重叠，在此不多做介绍。

A-Profile规定了应用层中的安全要求，引入OSI模型应用层中的关联控制服务单元（ACSE），使用ACSE请求（ARRQ）和ACSE响应（ARRE）来确立和维持Client与Server之间的MMS连接。

ACSE的关联建立时应有对等实体的认证，该认证信息分别在ARRQ与ARRE的协议数据单元（PDU）的认证功能单元（认证FU）中携带，其中认证的签名证书的内容使用按照基本编码规则编码的X.509证书，证书的交换为双向。证书中的签名值为RSA签名算法签署，秘钥长度为1024位。

ARRQ和ARRE的验证规则相同。即解码后的签名值必须与time字段（ARRQ与ARRE报文中的时间参数）的值相同、time字段值与当地时间的差值不得大于10 min、接收者在10 min内没有收到过包含相同签名值的报文，以上三点任意一点不符合，则接收者发出P－About原语（表示层异常终止命令），终止此次连接。

若无P－About原语则报文验证通过，即将安全参数传递给MMS处理。

3．GOOSE与SMV

对于IEC 61850中的GOOSE（面向变电站事件的通用对象）与SMV（采样值），可以将报文的PDU进行扩展，并将原PDU的保留字部分与扩展PDU的扩展部分一起利用，改造成安全报文。扩展后的PDU格式如图2所示。

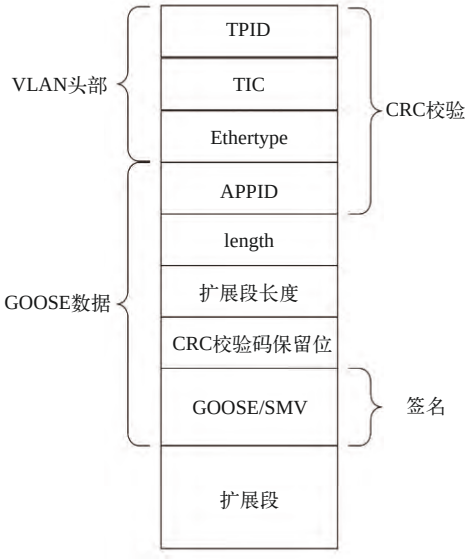

图2　扩展PDU

原PDU段的两个16位保留字段中，第一个字段前8位说明了扩展字段的长度，后8位依然保留作备用；第二个字段则存储了16位循环冗余校验码（CRC），由PDU字段中VLAN信息的前8位进行CRC计算得到。

扩展PDU段长度不定，格式分为三段。第一段为保留段，供以后PDU有除认证和加密以外的功能时使用，否则该字段不出现。第二段为厂商私有信息存储段，编码格式为ASN.1，为厂商需要预先协商的内容，此处也不做讨论。第三段为对GOOSE/SMV报文的摘要计算值进行签名所得到的签名值。

值得注意的是，GOOSE/SV报文由于对实时性要求很强，在选择算法的时候一定要考虑加密解密的效率，尽量不影响传输速度。

变电站通信安全系统的搭建及测试

1．系统平台介绍

Libiec61850是一个以C语言为基础的开源项目,它主要实现了IEC 61850中的通信模块。它拥有代码开源、可跨平台运行等诸多优点，适合作为智能变电站相关课题的学习与开发工具。本课题将以此为基础，参照通信安全规约IEC 62351标准要求，对通信模块进行改造，搭建一个安全的变电站通信系统。

2．加密套件介绍

加密套件采用的是开源套件OpenSSL。它是一个开放源代码的SSL协议的产品实现，其协议库完

全实现和封装了SSL协议的3个版本与TLS协议，这些协议在Windows中会编译在名为sslery32.lib的库中。此外OpenSSL的应用程序还自带了一个小型CA的功能，允许自己建立CA和签发证书。本文使用了OpenSSL的TLS1.0协议库与CA。

3．系统软件流程

软件主要框架参照IEC 61850搭建，以一台PC充当MMS客户端兼具有GOOSE/SMV报文接收等功能，另一台PC用于实现终端模拟MMS服务器通信、GOOSE/SV报文发送等功能。

MMS通信部分：建立双向证书验证，对于证书验证或证书超期的访问者拒绝访问。且参照IEC 62351-4的建议建立了更加可靠的双边表认证，即将通信设备的MAC地址记录在本地建立的认证表中并与证书绑定，进一步防止未经授权的连接与访问。通信部分在TCP握手之后增加TLS握手连接并交换密钥。MMS报文段添加ARRE与ARRQ验证。

GOOSE/SMV部分：对GOOSE/SMV的报文头进行CRC计算，然后按照扩展PDU格式组装报文并加密发送。由于GOOSE/SMV报文对实时性要求很高，要求发送/接收的时间必须在4 ms以内，综合考虑安全性与实时性，该部分的加密采用SHA1，密钥长度100位。

4．测试结果

对通信端数据进行截取，可以看出，改造后的通信数据已是加密过的数据，即使被黑客截获，也无法获得任何有用的信息，网络通信的安全性大大提高。

如图3所示，原本的MMS通信数据包完全依照IEC 61850标准格式建立，截取数据后轻易就可以获取通信报文内容。

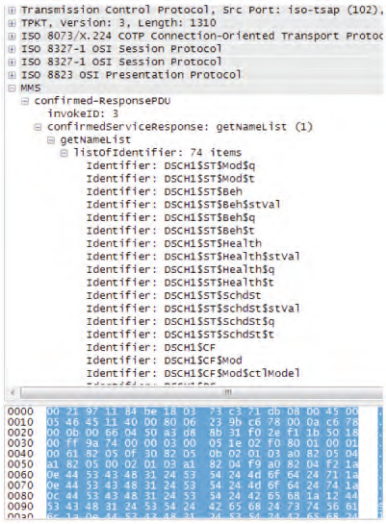

图3　传统MMS通信数据包

改造后的MMS报文如图4所示，加密数据无法解析。

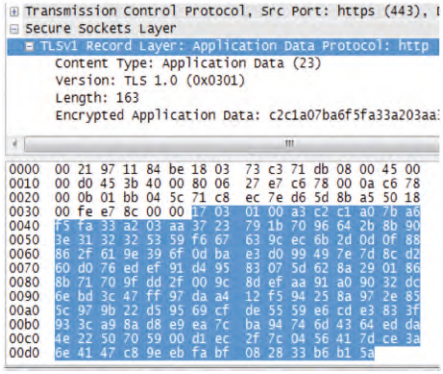

图4　改造后的MMS报文

对于GOOSE/SMV加密后，可以看到，发送接收的处理时间变长，但是仍满足4 ms的实时性要求，对性能并未产生影响。数据如表1所示。

表1　GOOSE报文用时

原报文用时/μs		加密后报文用时/μs	
发送	接收	发送	接收
24	9	39	64
26	13	43	70
33	12	47	68
31	10	48	69
32	9	53	63
31	11	52	63

结束语

本文对IEC 62351标准下的智能变电站通信系统做了探讨，并以开源平台实现了一个由IEC 61850改造的安全通信系统，探讨了其在变电站中的可行性。经测试该系统的信息安全性较原系统有了大幅提高。随着国家对智能变电站的推广，IEC 62351标准必定会得到应用。EA

（收稿日期：2016.05.23）

（编辑：杨得润）