

[信息安全]

基于报文特征的SMV信息安全检测技术

文/南京南瑞继保电气有限公司 曹少珂
国网江苏省电力有限公司邳州市供电分公司 徐 贝
中国长江电力股份有限公司三峡水力发电厂 李 琛
南京南瑞继保电气有限公司 齐 岩

IEC 61850通信协议作为智能变电站国际通用的通信标准，极大地方便了智能变电站内的站域通信。然而，标准化和开放化的通信协议也给变电站网络安全带来了极大的威胁。详细介绍了当前智能变电站所面临的网络安全威胁及常用的安全策略，提出了一种基于智能变电站过程层SMV报文信息的入侵检测技术并进行了仿真验证。仿真结果表明该方法能够有效地检测出报文是否遭到入侵，并且能够定位遭遇入侵的字段。

随着电力行业与网络通信技术的不断融合发展，原本人们印象中非常安全的电力系统也面临着网络安全威胁。2015年乌克兰电力网络遭遇黑客入侵，造成大面积停电事故；2018年黑客通过网络窃取了法国某电力公司大量的文件，造成机密信息泄露。上述针对电力网络的恶意入侵事件只是近年来电力系统网络攻击事件的冰山一角。这些电力系统网络入侵案例说明通信技术的发展给电力系统带来进步的同时，给电力系统网络安全带来的问题也不容忽视，探究提升电力系统网络安全的方法，对电网的安全稳定运行具有重要意义。

智能变电站网络信息安全分析

1. 智能变电站网络结构

根据IEC 61850标准体系的描述，典型的智能变电站可分为三层：站控层、间隔层及过程层。其中站控层位于变电站的顶层，包括主机与操作员站、远动通信系统和对时系统等。间隔层位于站控层与过程层的中间，包括保护、测量、控制和录波等二次装置。过程层位于智能变电站的最底层，典型设备包括常规/电子式互感器、智能终端（执行单元）和合并单元等。上述三个层级间以

及同一层级间存在着大量的信息交换，为了满足信息的实时传递，智能变电站使用了多种类型的通信协议来传递不同类型的信息。在IEC 61850通信协议的基础上，智能变电站使用三种不同协议来满足多种类型报文对于不同类型信息的传递，分别是SMV（Sample Measured Value）、GOOSE（Generic Object Oriented Substation Event）及MMS（Manufacturing Message Specification）。其中GOOSE报文负责传输站内电子设备的状态信息，SMV报文传输线路的采样值，MMS报文传输变电站工作人员发出的指令及文件。

2. 智能变电站网络安全现状

在智能变电站三层结构下，各个层级之间以及同一层级间的通信使用IEC 61850的标准化通信协议，IEC 61850是一个开放式的国际标准，它明文规范了变电站内的通信协议，但是没有对变电站的网络系统提供相关的安全规范，因此标准化的通信协议在带来便利的同时，也给智能变电站的通信安全带来了许多隐患，给开放式变电站信息系统的安全性和可靠性带来了许多不安全因素。威胁变电站网络信息安全的因素可以分为人为因素与外部干扰两部分，下面对其进行详细介绍。

(1) 人为因素

人为因素可以细分为外部人员与内部人员。来自外部人员的网络安全威胁包括非法截获、中断、篡改、伪造、恶意程序、权限管理不当及Internet的安全漏洞等,这些来自外部的攻击往往针对报文的个别字段,具有无序性和随机性,会对智能变电站的正常运行造成破坏。内部人员对网络安全带来的隐患也是威胁网络安全运行的不可忽视的一部分。

(2) 外部干扰

智能变电站处于复杂多变的外部环境,特别是变电站需要与各种外部设备进行对接,外部环境中的电磁波、噪声等因素会不可避免地对外部环境中的信息传输过程造成干扰,导致信息在传输过程中发生畸变、丢失或者传输状态的改变,从而威胁变电站的网络安全。

智能变电站网络安全策略分析

原则上,应用于其他网络的安全策略都可以应用到智能变电站网络中,但是由于电力行业对于信息传输实时性的要求,所以针对智能变电站网络安全的策略需要进行具体分析。当前针对智能变电站网络安全的研究主要是增强网络自身的防护能力,通过加密或数字签名进行验证,可防止对传输数据的窃听、诱骗和监测,利用IEC 61850标准的变电站配置语言可生成防火墙、入侵检测系统和入侵预防系统的安全措施。以下是几类常见的提升变电站网络安全性的措施。

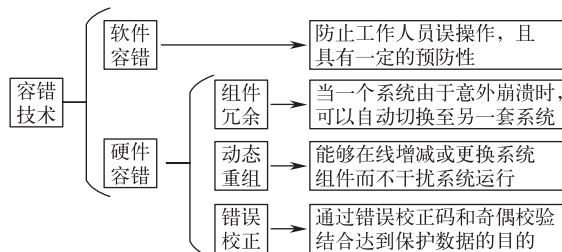
1. 采用独立组网结构

独立组网结构是独立组建智能变电站站内的通信网络,确保其他变电站遭到攻击时本站不会受到影响。独立组网技术可以与5G技术结合起来,如今5G独立组网模式已正式推出,将其应用到智能变电站的通信网络中,可以不借助外部网络就实现用户的无线接入及互联网的接入和相应的管理功能等,实现网络的独立工作。

2. 容错技术

智能变电站在智能电网的建设中承担着承上启下的作用,涉及电能输送的各个方面,其安全运行意义重大。为了提高变电站运行可靠性,变电站的通信系统需要采用容错技术,即允许变电站通信网

络中存在故障,但是这些故障发生时不会对网络的通信造成影响。容错技术应用的目的是使整个智能变电站的通信网络不会因为发生入侵而整个瘫痪,避免灾难性事故的发生。容错技术的一些重要功能如图1所示。



3. 加密技术

加密技术是最基本、最常用而又最有效的信息安全技术,可以有效地降低网络遭到截获、中断、篡改及伪造的概率,从而达到保证信息安全的目的。加密技术在一定程度上可以防止信息泄露及监听等恶意入侵事件,但是由于IEC 61850标准规定了智能变电站端到端之间的通信最大延迟为4 ms,在变电站过程层网络上加密措施并不能全部有效。

4. 虚拟专网技术

虚拟专用网是指借助公共互联网的数据传输能力,建立专用的数据通道,使通信数据能够可靠、安全及保密的传送。虚拟专网技术具有运行成本低、网络移动性强和可灵活扩充等优点,适用于独立构建的变电所通信网络。

5. 深度防御理论的网络保护策略

深度防御理论可以从实时防御和日常防御两方面来展开。实时防御包括网络防火墙的实时更新、恶意入侵的实时检测、遭遇入侵后的实时预警及拥有完备的应急响应预案,必要时还可以启动反攻击系统进行反攻。日常防御包括对安全隐患的检测分析及对外部数据的长期预警,以抵御可能会发生的未知攻击。

在构思或解决网络中的关键问题时深度防御理论应用是全方位的、综合考虑,使得网络中的各个层面的管理与应用处于最佳状态,受到威胁的概率最小。此外,深度防御理论还保证了每一层面的各个系统之间的独立性,限制了内部用户的权限,一定程度上减小了内部人员对网络安全的威胁。

面向SMV报文的信息安全检测技术

1. SMV报文特征

由于智能变电站对实时性要求非常高，上述的许多安全措施很难在不影响实时性的情况下应用于变电站网络，因此许多研究者又展开了针对智能变电站入侵技术的研究，可以建立一套包括智能变电站、电力系统网络等在内的网络安全测试台和基于主机和网络的集成异常检测方法，也可以通过监控并分析网络信息流量和网络状态的方法来检测异常事件。在此基础上，本文提出了一种利用SMV报文信息的智能变电站入侵检测技术。

智能变电站过程层网络中的报文使用明文传输智能变电站中设备的关键控制信息和重要遥测信号，且不采取任何防护措施，安全性非常差。因此研究智能变电站过程层的入侵检测意义重大，对比传统网络的各种入侵检测方法，发现基于协议特征的入侵方法能够在时间开销最小的情况下为网络提供有效的安全检测。

每条SMV报文都由以太网头部、IEC 61850 SMV头部以及协议数据单元（PDU）三个层次构成。其中协议数据单元（PDU）采用抽象语法标记（ASN.1）语法对采样值进行编码，一个协议数据单元（PDU）由多个应用数据服务单元（ASDU）链接而成。SMV报文中的关键字段及其含义见表1，这些关键字段的值会根据变电站状态的不同而发生变化，无论变电站正常运行还是遭到入侵，除这几个字段以外的其他字段都不应该发生变化。

表1 SMV报文关键字段及其含义

SMV报文关键字段	所属层次	描述
Application Length	IEC 61850 SMV头部	从应用标识（Appid）开始的字节数
PDU Length		协议数据单元长度
Number of Asdu		ASDU数量
Sample Count	协议数据单元（PDU）	采样帧计数，该值累加，下一帧加1，达到3 999后归零，重新计数

2. SMV报文异常检测技术

在具体检测时，根据智能变电站网络是否划分虚拟局域网（VLAN），可以分成两种情况讨论：在网络未划分VLAN时，应检测报文头部的12、13字节，当报文为0x88或0xba时可确定该报文为SMV报文；在网络未划分VLAN的情况下，检测报文头部的16、17字节，当报文为0x88或0xba时可确定该报文为SMV报文。

在判断所检测报文为SMV报文之后，为了更好地检测SMV报文是否遭到入侵及被入侵的程度，建立与SMV报文有关的函数 $f(x_1, x_2, x_3) = x_1 + x_2 + x_3$ ，自变量的含义见表2。

表2 各自变量具体含义

自变量	包含字段	正常运行时 字段状态	遭到入侵时字段 状态
x_1	Application Length PDU Length	不变	改变
x_2	Number of ASDU	不变	改变
x_3	Sample Count	前一条+1	0

为了更直观地展示函数发生的变化，假设报文正常运行时 $x_1 = x_2 = x_3 = 1$ ，此时 $f(x_1, x_2, x_3) = 3$ ，也称为期望值。自变量 x_1 中包含着与字段长度有关信息，利用公式1来判断字段长度是否发生变化

$$\begin{cases} Z = \left\{ \underbrace{z_1, z_2, \dots, z_m}_{L_{\text{Appid}}}, \underbrace{z_{m+1}, \dots, z_n}_{L_{\text{PDU}}} \right\} \\ x_1 = \frac{z_1 + z_2 + \dots + z_n}{L_{\text{Appid}} + L_{\text{PDU}}} \end{cases} \quad (1)$$

式中，Z为方便计算引入的与字段长度有关的函数； $z_1, z_2, \dots, z_m$ 为从Appid字段开始的所有字节； $z_{m+1}, \dots, z_n$ 为PDU中包含的所有字节，正常情况下这些字节记为1，遭受攻击时变为0； L_{Appid} 为从Appid开始的字节长度； L_{PDU} 为协议数据单元包含的字节长度。从式（1）可以看出， x_1 的值在0~1区间内浮动，当 $x_1 = 1$ 时代表无入侵发生， $x_1 < 1$ 时代表有入侵发生。

自变量 x_2 代表与应用数据服务单元（ASDU）数量有关的信息，假定当智能变电站正常运行时，一个协议数据单元由n个ASDU单元链接而成，用 $x_2 = 1$ 来表示。当ASDU数量发生改变时，代表着通信网络遭到了较为严重的入侵，例如发生报文丢失等情况，此时报文将会被弃用，用 $x_2 = 0$ 来表示。利用式（2）来判断Number of ASDU字段的安全状况

$$\begin{cases} x_2 = 1 & \text{ASDU数量为} n \\ x_2 = 0 & \text{ASDU数量不为} n \end{cases} \quad (2)$$

自变量 x_3 代表与采样计数有关的信息，在智能变电站正常运行时，Sample Count报文所在字段与上一条报文相同，字段值为前一条报文字段值+1。当Sample Count报文所在字段遭到入侵时，采样帧计数被打乱，此时后续报文字段值恒等于1，计数功能丢失。用 $m_0, m_1, m_2, \dots, m_{3999}$ 来表示4 000个采样帧计数，当其满足式（3）时，记 $x_3 = 1$ ，否则记 $x_3 = 0$

$$\{m_k = m_{k-1} + 1 \quad k \in Z \text{ 且 } k \in [0, 3999]\} \quad (3)$$

3. SMV报文异常检测流程

综合上述情况，可以得到完整的检测流程图，如图2所示。

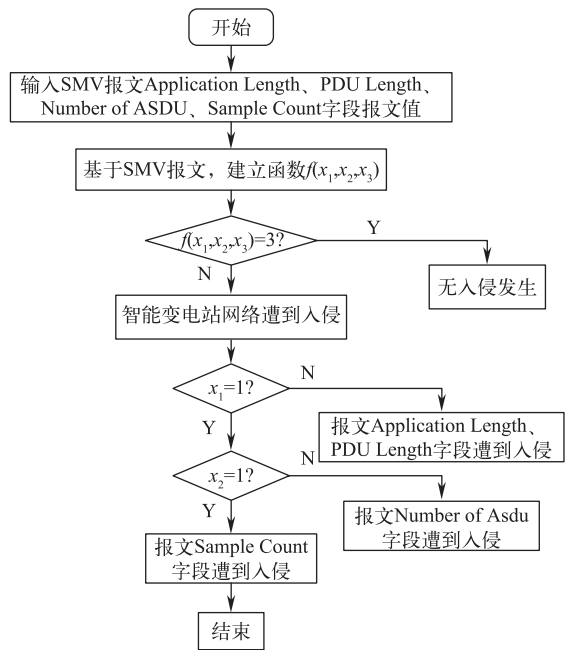


图2 SMV协议异常检测流程图

仿真验证与结果分析

本文的仿真实验模拟SMV报文发送和接收过程，借助试验平台选取1 000条试验用的SMV报文，并设置下列三种类型攻击。①向报文注入无效代码；②加强外部网络对SMV报文的干扰；③随机篡改报文。利用上文提出的SMV检测方法对每条报文进行安全监测。

1. 入侵正确率验证

设置攻击类型分为上述三种单一攻击类型以及混合攻击，即入侵行为中包含所有三种攻击类型，共四种攻击类型分别在相同的时间内入侵SMV报文，入侵次数为50次，采用文中提出的SMV报文检测方法对接以到的1 000条报文进行入侵次数检测，检测结果见表3。

表3 入侵次数验证结果

入侵类型	设置入侵次数	检测到入侵次数	检测正确率(%)
向报文注入无效代码	50	49	98
加强外部网络对SMV报文的干扰		48	96
随机篡改报文		50	100

试验结果显示上文所提报文检测方法能够较为准确地检测出SMV报文是否遭到入侵。

2. 入侵字段检测验证

本试验在3天时间内对所有接收的报文进行检测，设置在3天内随机对SMV报文进行入侵，入侵次数为50次，利用上文的检测技术对报文遭遇入侵字段进行检测。入侵字段验证结果见表4。

表4 入侵字段验证结果

SMV报文字段	是否遭到入侵	检测到入侵次数	总次数
PDU Length Application Length	是	21	50
Number of Asdu		18	
Sample Count		11	

试验结果表明上文提出的SMV报文检测技术可以对发生入侵字段进行定位。

结束语

本文分析了当前智能变电站的网络信息安全现状，并介绍了常见的提升网络安全的手段。本文在满足智能变电站对于实时性要求的基础上，提出了一种基于智能变电站过程层SMV报文信息的入侵检测技术，并通过仿真对该项技术进行了验证，仿真结果表明：该方法能够有效地检测出报文是否遭到入侵，并且能够定位报文遭遇入侵的字段。

参考文献

- [1] 谭文恕. 变电站通信网络和系统协议IEC 61850介绍[J]. 电网技术, 2001, 25(9): 8-11.
- [2] 莫峻, 谭建成. 基于IEC 61850的变电站网络安全分析[J]. 电力系统通信, 2009, 30(4): 12-16.
- [3] 高卓. 变电站的计算机网络安全分析[J]. 电力系统自动化, 2002, 26(1): 53-57.
- [4] 骆钊, 谢吉华, 顾伟, 等. SM2加密体系在智能变电站站内通信中的应用[J]. 电力系统自动化, 2015, 39(13): 116-123.
- [5] 王保义, 王民安, 张少敏. 一种基于GCM的智能变电站报文安全传输方法[J]. 电力系统自动化, 2013, 37(3): 87-92.
- [6] 田宇, 赵恒阳, 柯艳国, 等. 智能变电站智能控制柜散热策略研究[J]. 电气应用, 2020, 39(6): 40-45.

(收稿日期: 2021-09-28)