

VSC-HVDC 系统恶意数据注入攻击演示与分析软件说明书

2017 年 06 月 01 日

目录

1 软件概况.....	2
2 软件程序步骤说明.....	4
3 软件流程图.....	11
3 软件程序数据说明.....	11
3.1. 系统数据	11
3.2. 外部程序数据	13
3.3. 恶意数据注入攻击数据	13
4 软件程序主要类和函数说明.....	13
4.1 系统数据导入函数	13
4.2 状态估计数据生成类	13
4.3 系统单线图绘制函数	14
4.4 生成量测数据函数	14
4.5 含 VSC-HVDC 交直流系统状态估计类.....	14
4.6 攻击前残差分析函数	14
4.7 攻击前 P-Q 运行极限和运行点分析函数.....	14
4.8 VSC-HVDC 系统恶意数据注入攻击策略模型求解类	14
4.9 批量分析函数	14
5 附图.....	14
5.1 修改的 IEEE-14 节点系统单线图.....	15

1 软件概况

随着信息技术的大量渗入,现代电力系统已经发展成为由电力及其监控系统构成的复杂信息-物理系统(Cyber-Physical System, CPS)。由于信息系统与物理系统的高度耦合,信息系统遭受的故障或网络攻击不仅会影响其自身的正常运行,更有可能传导至物理系统从而威胁电力系统的安全、稳定和经济运行。这类新的安全问题被称为电力系统信息物理安全问题。其中,恶意数据注入攻击,即通过篡改量测数据进而影响 SE 结果的网络攻击,是电力 CPS 所面临的信息物理安全问题的一种重要形式。基于电压源型换流器的高压直流输电(Voltage Source Converter based High Voltage Direct Current Transmission, VSC-HVDC)技术在电网中得到了广泛的应用,其在提高系统稳定性以及促进新能源消纳等诸多方面发挥着重要作用。如果攻击者对 VSC-HVDC 系统实施 FDI 攻击,必将会对 VSC-HVDC 系统自身甚至整个交直流系统的安全稳定运行造成极大影响。因此对 VSC-HVDC 系统的 FDI 攻击问题的研究具有重要意义。

VSC-HVDC 系统恶意数据注入攻击演示与分析软件基于含 VSC-HVDC 交直流系统的状态估计模型和电力系统恶意数据注入攻击的一般形式,通过求解以破坏 VSC-HVDC 系统换流器运行安全为目标的恶意数据注入攻击策略模型,演示 VSC-HVDC 系统所面临的恶意数据注入攻击问题,并能够批量分析该攻击对状态估计最大标准化残差的影响,以帮助电网运行人员认识和理解 VSC-HVDC 系统所面临的恶意数据注入攻击风险。软件主要具有以下特点:

1. 代码结构性强。程序的编写过程参照结构化编程方法,将大段复杂代码按照功能模块进行分类。每个功能只完成自己的计算目的,只与调用它的主体程序交互信息而不与其他功能模块交互,这使得程序的测试、排错、维护、升级工作能够顺序进行。
2. 数据格式清晰规范。用户文档中给出了各数据文件的格式要求,对于数据量较大的交流系统数据,用户还可使用电力系统中广泛使用的中国版 BPA 软件格式数据,从而保证了数据的规范性。
3. 应用灵活。软件提供了攻击参数的修改功能,用户可设置不同的被攻击换流器、攻击参数以及批量分析次数,对恶意数据注入攻击的效果及分析结果进行观察。
4. 可视化程度高。软件运行中的主要结果均由图形显示,如恶意数据注入攻击前后状态估计中各量测量的标准化残差,恶意数据注入攻击前后换流器的 P-Q 运行极限和运行点,以及批量分析中状态估计中的最大标准化残差变化情况。

程序以 Windows 7 + Python2.7+ Qt Designer 为开发环境。

2 软件程序步骤说明

步骤 1: 导入系统数据文件;

步骤 2: 根据步骤 1 中输入的交流系统数据、VSC-HVDC 系统数据和节点地理位置数据绘制系统的单线图;

步骤 3: 生成的攻击前的量测数据以表格的形式显示在软件界面中;

步骤 4: 设置恶意数据注入攻击参数, 包括被攻击换流器、攻击参数 r_1 、攻击参数 r_2 以及批量分析次数 (仅进行批量分析计算时需要设置);

步骤 5: 基于恶意数据注入攻击前的量测数据进行状态估计, 进行残差分析以及 P-Q 运行极限和运行点分析;

步骤 6: 对 VSC-HVDC 系统中选择的换流器实施恶意数据注入攻击;

步骤 7: 基于恶意数据注入攻击后的量测数据进行状态估计, 进行残差分析以及 P-Q 运行极限和运行点分析, 并将分析结果以图形的形式显示在软件界面中;

步骤 8: 批量分析计算。

步骤 1 中, 导入的系统数据包括交流系统数据文件、VSC-HVDC 系统数据文件、量测配置数据文件以及节点地理位置数据文件; 各数据文件需遵守一定的格式规范, 其中数据量较大的交流系统数据即可选择本软件给定的格式规范, 也可选择 BPA 潮流数据格式; 导入的数据文件以表格的形式显示在软件界面中。

步骤 2 中, 系统中交流节点在单线图中显示为圆形, VSC-HVDC 系统的换流站在单线图中显示为方形。

步骤 3 中, 根据系统潮流计算的结果计算各量测量的真实值, 然后在量测量真实值的基础上添加服从正态分布的量测误差以模拟真实的量测量。

步骤 4 中, 攻击参数 r_1 、攻击参数 r_2 设置范围为 0~1.5, 批量分析次数的设置的最大值为 1000。

步骤 5 中, 状态估计算法为基于加权最小二乘法的含 VSC-HVDC 交直流系统状态估计算法, 残差分析中对各量测量的标准化残差进行计算, P-Q 运行极限图中给出反映流入换流器的交流侧电流幅值限制的实线圆和反映换流器交流侧电压幅值限制的虚线圆, 换流器的安全运行区间用灰色阴影标出, 根据状态估计结果计算得到的换流器的运行点用红色圆点标出。另外, 残差分析的结果也以图形的形式显示在软件界面中。

步骤 6 中, 求解以被篡改量测量数目最小为目标的恶意数据注入攻击策略模型, 求解过程中利用 IPOPT 求解器求解非线性优化模型; 被攻击的换流器在系统单线图中用红色圆形标出, 攻击后的量测数据以表格的数据显示在软件界面中, 其中被篡改的量测数据用红色标出;

步骤 8 中, 随机生成多组量测数据, 且每组量测数据满足使状态估计后量测量的最大标准化残差小于 3, 在各组生成的量测数据下进行恶意数据注入攻击, 并进行残差分析, 各次恶意数据注入攻击前后状态估计中最大标准化残差的变化情况同时以图形和表格的形式显示在软件界面中。

现以修改的 IEEE-14 节点系统为算例, 对软件程序步骤进行说明。

步骤 1, 导入系统数据文件, 共包含 4 个.txt 文件, 各文件内容如下:

交流系统数据文件: case_ac.txt

```
case_ac.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

START-BASEMVA
100:
END-BASEMVA

START-BUS
1 3 0 0 0 0 1 1.06 0 0 1 1.06 0.94;
2 2 21.7 12.7 0 0 1 1.045 -4.98 0 1 1.06 0.94;
3 2 94.2 19 0 0 1 1.01 -12.72 0 1 1.06 0.94;
4 1 47.8 -3.9 0 0 1 1.019 -10.33 0 1 1.06 0.94;
5 1 7.6 1.6 0 0 1 1.02 -8.78 0 1 1.06 0.94;
6 2 11.2 7.5 0 0 1 1.07 -14.22 0 1 1.06 0.94;
7 1 0 0 0 0 1 1.062 -13.37 0 1 1.06 0.94;
8 2 0 0 0 0 1 1.09 -13.36 0 1 1.06 0.94;
9 1 29.5 16.6 0 19 1 1.056 -14.94 0 1 1.06 0.94;
10 1 9 5.8 0 0 1 1.051 -15.1 0 1 1.06 0.94;
11 1 3.5 1.8 0 0 1 1.057 -14.79 0 1 1.06 0.94;
12 1 6.1 1.6 0 0 1 1.055 -15.07 0 1 1.06 0.94;
13 1 13.5 5.8 0 0 1 1.05 -15.16 0 1 1.06 0.94;
14 1 14.9 5 0 0 1 1.036 -16.04 0 1 1.06 0.94;
END-BUS

START-GENERATOR
1 232.4 -16.9 10 0 1.06 100 1 332.4 0 0 0 0 0 0 0 0 0 0 0;
2 40 42.4 50 -40 1.045 100 1 140 0 0 0 0 0 0 0 0 0 0;
3 0 23.4 40 0 1.01 100 1 100 0 0 0 0 0 0 0 0 0 0;
6 0 12.2 24 -6 1.07 100 1 100 0 0 0 0 0 0 0 0 0 0;
8 0 17.4 24 -6 1.09 100 1 100 0 0 0 0 0 0 0 0 0 0;
END-GENERATOR

START-BRANCH
1 2 0.01938 0.05917 0.0528 9900 0 0 0 0 1 -360 360;
1 5 0.05403 0.22304 0.0492 9900 0 0 0 0 1 -360 360;
2 3 0.04699 0.19797 0.0438 9900 0 0 0 0 1 -360 360;
2 4 0.05811 0.17632 0.034 9900 0 0 0 0 1 -360 360;
2 5 0.05695 0.17388 0.0346 9900 0 0 0 0 1 -360 360;
3 4 0.06701 0.17103 0.0128 9900 0 0 0 0 1 -360 360;
4 5 0.01335 0.04211 0 9900 0 0 0 0 1 -360 360;
4 7 0.20912 0 9900 0 0 0.978 0 1 -360 360;
4 9 0 0.55618 0 9900 0 0 0.969 0 1 -360 360;
5 6 0 0.25202 0 9900 0 0 0.932 0 1 -360 360;
6 11 0.09498 0.1989 0 9900 0 0 0 0 1 -360 360;
6 12 0.12291 0.25581 0 9900 0 0 0 0 1 -360 360;
6 13 0.05615 0.13027 0 9900 0 0 0 0 1 -360 360;
7 8 0 0.17615 0 9900 0 0 0 0 1 -360 360;
7 9 0 0.11001 0 9900 0 0 0 0 1 -360 360;
7 10 0.03181 0.0845 0 9900 0 0 0 0 1 -360 360;
9 14 0.12711 0.27038 0 9900 0 0 0 0 1 -360 360;
10 11 0.08205 0.19207 0 9900 0 0 0 0 1 -360 360;
12 13 0.22092 0.19988 0 9900 0 0 0 0 1 -360 360;
13 14 0.17093 0.34802 0 9900 0 0 0 0 1 -360 360;
END-BRANCH
```

VSC-HVDC 系统数据文件: case_dc.txt

```
case_dc.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

START-BASEMVAac
100:
END-BASEMVAac

START-BASEMVAdc
100:
END-BASEMVAdc

START-POL
1:
END-POL

START-BUS
1 6 1 0 1 345 1.1 0 0;
2 4 1 0 1 345 1.1 0 0;
END-BUS

START-CONVERTER
1 1 -100 80 1 0.0015 0.1121 0.0000 0.0001 0.16428 345 1.1 0 1.2 1 1.103 0.887 2.885 4.371;
2 2 0 0 1 0.0015 0.1121 0.0000 0.0001 0.16428 345 1.1 0 1.2 1 1.103 0.887 2.885 4.371;
END-CONVERTER

START-BRANCH
1 2 0.052 0 0 100 100 100 1;
END-BRANCH
```

量测配置数据文件: case_mc.txt

```
case_mc.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

START-BUS
1 1 1e-3 0 1e-3 0 1e-3;
2 1 1e-3 1 1e-3 1 1e-3;
3 1 1e-3 1 1e-3 1 1e-3;
4 1 1e-3 0 1e-3 0 1e-3;
5 0 1e-3 0 1e-3 0 1e-3;
6 1 1e-3 0 1e-3 0 1e-3;
7 0 1e-3 2 1e-3 2 1e-3;
8 1 1e-3 0 1e-3 0 1e-3;
9 0 1e-3 0 1e-3 0 1e-3;
10 0 1e-3 1 1e-3 1 1e-3;
11 0 1e-3 0 1e-3 0 1e-3;
12 0 1e-3 0 1e-3 0 1e-3;
13 0 1e-3 1 1e-3 1 1e-3;
14 0 1e-3 1 1e-3 1 1e-3;
END-BUS

START-BRANCH
1 2 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
1 5 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
2 3 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
2 4 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
2 5 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
3 4 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
4 5 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
4 7 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
4 9 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
5 6 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
6 11 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
6 12 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
6 13 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
7 8 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
7 9 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
9 10 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
9 14 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
10 11 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
12 13 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
13 14 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
END-BRANCH

START-BUSDC
1 6 1 1e-3 1 1e-3 0 1e-3 1 1e-3 2 1e-3 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
2 4 1 1e-3 1 1e-3 0 1e-3 1 1e-3 2 1e-3 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
END-BUSDC
```

节点地理位置数据: case_bl.txt

```
case_mc.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

START-BUS
1 1 1e-3 0 1e-3 0 1e-3;
2 1 1e-3 1 1e-3 1 1e-3;
3 1 1e-3 1 1e-3 1 1e-3;
4 1 1e-3 0 1e-3 0 1e-3;
5 0 1e-3 0 1e-3 0 1e-3;
6 1 1e-3 0 1e-3 0 1e-3;
7 0 1e-3 2 1e-3 2 1e-3;
8 1 1e-3 0 1e-3 0 1e-3;
9 0 1e-3 0 1e-3 0 1e-3;
10 0 1e-3 1 1e-3 1 1e-3;
11 0 1e-3 0 1e-3 0 1e-3;
12 0 1e-3 0 1e-3 0 1e-3;
13 0 1e-3 1 1e-3 1 1e-3;
14 0 1e-3 1 1e-3 1 1e-3;
END-BUS

START-BRANCH
1 2 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
1 5 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
2 3 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
2 4 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
2 5 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
3 4 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
4 5 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
4 7 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
4 9 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
5 6 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
6 11 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
6 12 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
6 13 0 1e-3 0 1e-3 0 1e-3 0 1e-3;
7 8 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
7 9 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
9 10 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
9 14 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
10 11 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
12 13 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
13 14 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
END-BRANCH

START-BUSDC
1 6 1 1e-3 1 1e-3 0 1e-3 1 1e-3 2 1e-3 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
2 4 1 1e-3 1 1e-3 0 1e-3 1 1e-3 2 1e-3 1 1e-3 1 1e-3 0 1e-3 0 1e-3;
END-BUSDC
```

步骤 2, 绘制系统单线图, 如图 1 所示。

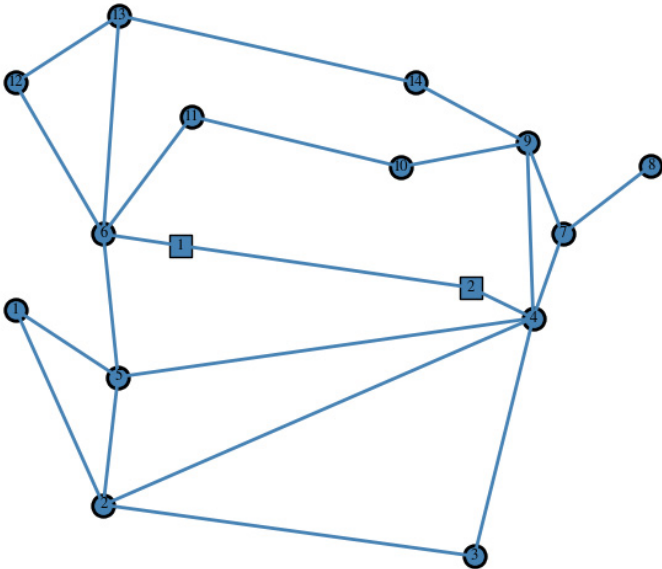


图 1 系统单线图

步骤 3 生成量测数据，结果如图 2 至图 4 所示。

	交流节点名称	电压幅值量测 (p.u.)	注入有功量测 (p.u.)	注入无功量测 (p.u.)
1	1	1.0593	-	-
2	2	1.0467	0.219	-0.1116
3	3	1.0086	0.2563	0.2701
4	4	0.9997	-	-
5	5	-	-	-
6	6	1.0683	-	-
7	7	-	-0.0001	0.0015
8	8	1.0896	-	-
9	9	-	-	-
10	10	-	-0.0144	0.0443
11	11	-	-	-
12	12	-	-	-
13	13	-	-0.0201	0.0838
14	14	-	-0.001	0.0942

图 2 攻击前的量测数据（部分 1）

	支路首端节点	支路末端节点	有功潮流量测	无功潮流量测	有功潮流量测	无功潮流量测
1	1	2	-	-	-	-
2	1	5	0.818	0.1226	-	-
3	2	3	0.7192	0.0376	-	-
4	2	4	-	-	-	-
5	2	5	0.5002	0.106	-	-
6	3	4	-0.2439	0.1553	-	-
7	4	5	-0.093	0.0293	-	-
8	4	7	-	-	-	-
9	4	9	0.2889	-0.0268	-	-
10	5	6	-	-	-	-
11	6	11	-	-	-	-
12	6	12	0.0541	0.0403	-	-
13	6	13	-	-	-	-
14	7	8	0.0002	-0.1984	-	-

图 3 攻击前的量测数据（部分 2）

直流节点名称	交流节点名称	有功潮流量测 (p.u.)	无功潮流量测 (p.u.)	有功功率量测 (p.u.)	无功功率量测 (p.u.)	有功平衡量测 (p.u.)	电压量测 (p.u.)	电流量测 (p.u.)	调制比量测	移相角量测
1 1	6	-0.9999	0.7997	-	1.1958	-0.0002	1.0501	0.9375	-	-
2 2	4	0.9224	-0.4251	-	-0.1385	0.0024	0.9999	-0.9378	-	-

图 4 攻击前的量测数据（部分 3）

步骤 4 设置攻击参数，其中被攻击换流器选择换流器 1，批量分析次数设置为 100，攻击参数 r_1 和攻击参数 r_2 均设置为 0.95。

步骤 5，运行状态估计程序，并进行残差分析，分析结果如图 5 所示；然后进行 P-Q 运行极限和运行点分析，分析结果如图 6 所示。从图 6 中可以看出，恶意数据注入攻击前换流器的运行点已经超出了其安全运行区间，控制系统应做出相应多做将其运行点拉回安全运行区间。

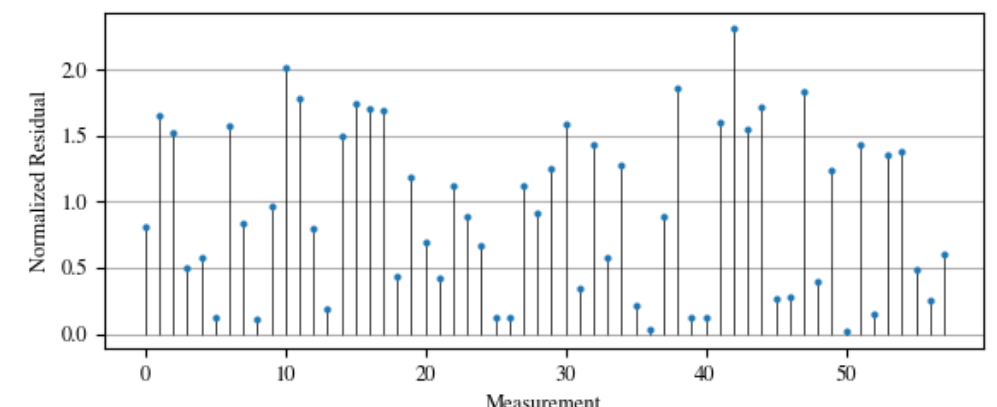


图 5 恶意数据注入攻击前各量测量的标准化残差

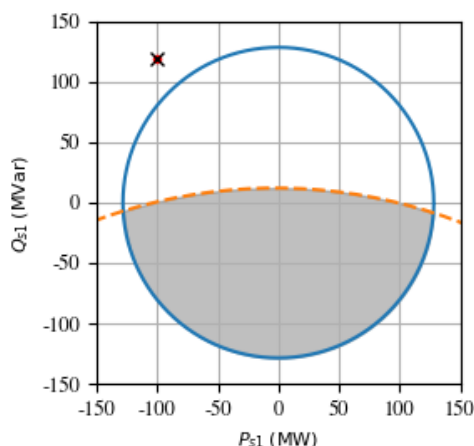


图 6 恶意数据攻击前换流器的 P-Q 运行极限与运行点

步骤 6 对换流器 1 进行恶意数据注入攻击，如图 7 所示，被攻击的换流器用红色圆形标出；进一步通过求解攻击策略模型，得到篡改后的量测数据如图 8 所示。显示红色的量测数据为被篡改的量测数据，图中未标红色量测数据和未给出的量测数据均保持与攻击前相同的值。

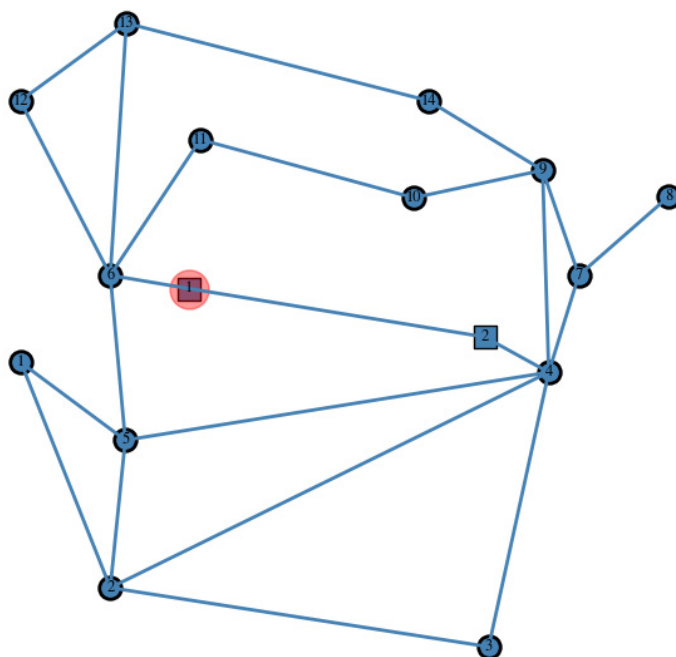


图 7 被攻击换流器标记示意图

	直流节点名称	交流节点名称	注入有功潮流量测 (p.u.)	注入无功潮流量测 (p.u.)	i功率量	换流器无功功率量测 (p.u.)
1	1	6	-0.9991	-0.5173	-	-0.2111
2	2	4	0.9224	-0.4251	-	-0.1385

图 8 篡改后的量测数据

步骤 7，换流器 1 受到恶意数据注入攻击后，运行状态估计程序，并进行残差分析以及 P-Q 运行极限和运行点分析，结果分别如图 9 和图 10 所示。从图中可以看出，恶意数据注入攻击并没有使各量测量的标准化残差大于阈值，即恶意数据注入攻击躲过了不良数据检测环节。进一步根据状态估计结果分析得到的换

流器 1 运行点位于安全运行区间内，不会引起控制系统的相应动作。但换流器的真实运行状态已经位于安全运行区间以外，可见恶意数据注入攻击达到了威胁 VSC-HVDC 系统安全稳定运行的目的。

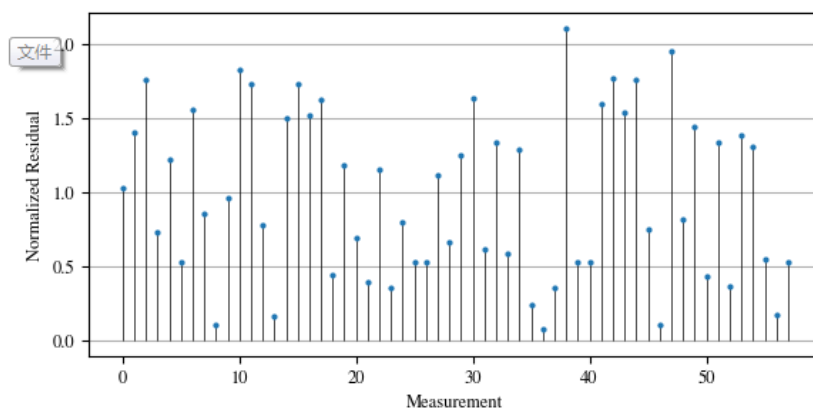


图 9 恶意数据注入攻击后各量测量的标准化残差

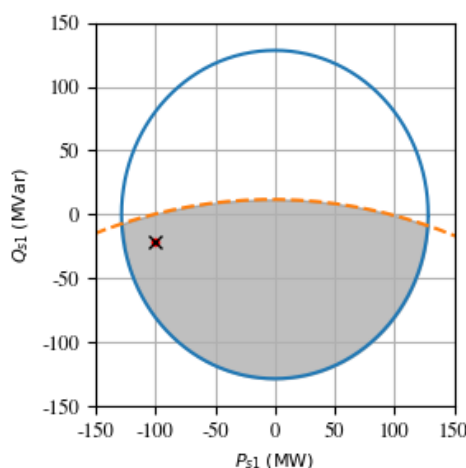


图 10 恶意数据攻击后换流器的 P-Q 运行极限与运行点

步骤 8，随机生成 100 组量测数据，并重复上述的恶意数据注入攻击，攻击后状态估计中最大标准化残差变化情况如图 11 所示。从图中可以看出，100 组恶意数据注入攻击中，大多数攻击并未引起最大标准化残差的明显增大，攻击后的最大标准化残差大部分并未超过安全阈值，因此，针对 VSC-HVDC 系统的恶意数据注入攻击具有很高的成功率。

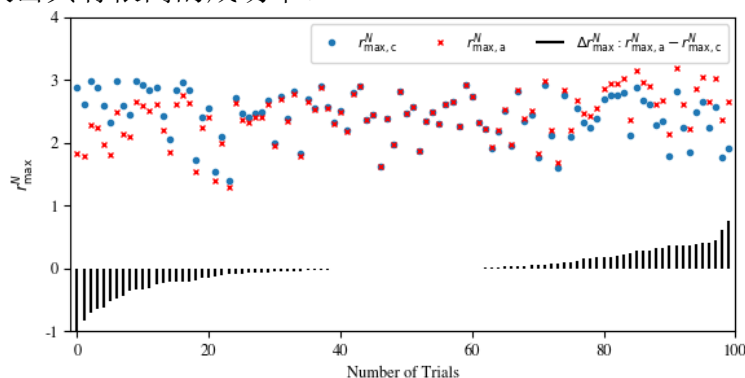


图 11 批量分析中最大标准化残差变化情况

3 软件流程图

本软件的流程图请见下图 12。

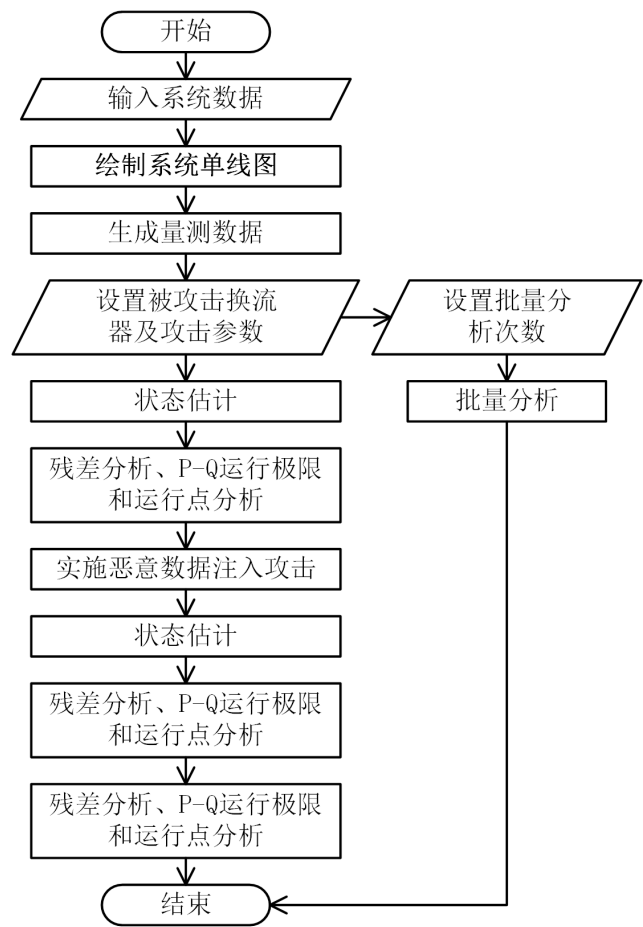


图 12 VSC-HVDC 系统恶意数据注入攻击演示与分析软件流程图

3 软件程序数据说明

3.1. 系统数据

交流系统数据	.TXT 格式文件或中国版 BPA 程序.DAT 格式文件。对于.TXT 格式文件，包括容量基准值数据、交流节点数据、发电机数据、交流支路数据，每一部分分别以 START-BASEMVA、START-BUS、START-GENERATOR、START-BRANCH 开头，以 END-BASEMVA、END-BUS、END-GENERATOR、END-BRANCH 结束；每一部分中，数据格式与电力系统分析程序程序包 MATPOWER 中相同，数据之间用制表符间隔，每一行数据以分号结尾。
	.TXT 格式文件，包括交流基准容量值数据、直流基准值容量数据、直流网络极数数据、直流节点数据、换流器数据、直流线路数据，

VSC-HVDC 系统数据	<p>每一部分分别以 START-BASEMVAac、START-BASEMVAac、START-POL、START-BUS、START-CONVERTER、START-BRANCH 开头，以 END-BASEMVAac、END-BASEMVAac、END-POL、END-BUS、END-CONVERTER、END-BRANCH 结束。</p> <p>直流节点数据中，每行表示一个直流节点，每一列数据含义依次为直流节点名称、交流节点名称、直流网络名称、直流有功功率 (MW)、直流电压幅值 (p.u.)、直流电压基准值 (Kv)、直流电压最大值 (p.u.)、直流电压最小值 (p.u.)、对地电容 (p.u.)。</p> <p>换流器数据中，每行表示一个换流器，每一列数据含义依次为直流节点名称、直流控制类型、交流控制类型、注入交流系统有功功率 (MW)、注入交流系统无功功率 (MVar)、交流节点电压整定值 (p.u.)、换流变压器电阻 (p.u.)、换流变压器电抗 (p.u.)、滤波器电纳 (p.u.)、移相器电阻 (p.u.)、移相器电抗 (p.u.)、交流电压基准值 (Kv)、交流电压最大值 (p.u.)、交流电压最小值 (p.u.)、交流电流最大值 (p.u.)、停运状态、损耗系统 A、损耗系统 B、损耗系统 C1、损耗系统 C2。</p> <p>直流线路参数中，每行表示一条直流，每一列数据含义依次为直流线路名称、首端直流节点、末端直流节点、直流线路电阻 (p.u.)、直流线路电感 (p.u.)、直流电路电容 (p.u.)、长期最大容量 (MVA)、短期最大容量 (MVA)、紧急最大容量 (MVA)、线路状态、线路首端注入功率 (MW)、线路末端注入功率 (MW)。</p> <p>每一行数据以分号结尾，一行中的不同数据用制表符间隔。</p>
量测配置数据	<p>.TXT 格式文件，包括交流节点量测配置、交流支路量测配置、换流站量测配置。每一部分分别以 START-BUS、START-BRANCH、START-BUSDC 开始，以 END-BUS、END-BRANCH、END-BUSDC 结束。</p> <p>交流节点量测配置数据中，每一行表示一个节点的量测配置，每一列数据含义依次为交流节点名称、电压幅值量测配置标识、电压幅值量测误差的标准差、节点注入有功量测配置标志、节点注入有功量测误差的标准差、节点注入无功量测配置标志、节点注入无功量测误差的标准差。</p> <p>交流支路量测配置数据中，每一行表示一条交流支路的量测配置，每一列数据含义依次为支路首端节点名称、支路末端节点名称、首端有功潮流量测配置标志、首端有功潮流量测误差的标准差、首端无功潮流量测配置标志、首端无功潮流量测误差的标准差、末端有功潮流量测配置标志、末端有功潮流量测误差的标准差、末端无功潮流量测配置标志、末端无功潮流量测误差的标准差。</p> <p>换流站量测配置数据中，每一行表示一个换流站的量测配置，每一列数据含义依次为直流节点名称、交流节点名称、注入有功潮流量测配置标志、注入有功潮流量测误差的标准差、注入无功潮流量测配置标志、注入无功潮流量测误差的标准差、换流器有功功率量测配置标志、换流器有功功率量测误差的标准差、换流器无功功率量测配置标志、换流器无功功率量测误差的标准差、换流器有功平衡量测配置标志、换流器有功平衡量测误差的标准差、直流电压量测配置标志、直流电压量测误差的标准差、直流电流量测配置标志、</p>

	直流电流量测误差的标准差、调制比量测配置标志、调制比量测误差的标准差、移相角量测配置标志、移相角量测误差的标准差。每一行数据以分号结尾，一行中的不同数据用制表符结尾。量测配置标志中，1 表示配置量测、0 表示未配置量测、2 表示为虚拟量测。
节点地理位置数据	.TXT 格式文件，包括交流节点地理位置数据、直流节点地理位置数据。每一部分分别以 START-ACBUS、START-DCBUS 开头，以 END-ACBUS、END-DCBUS 结尾，每一行表示一个交流（直流）节点地理位置，每一列数据含义依次为交流（直流）节点名称、节点经度、节点纬度。每一行数据以分号结尾，一行中的不同数据用制表符间隔。

3.2. 外部程序数据

非线性优化问题求解程序	IPOPT 非线性优化求解器，版本为 3.12.4
-------------	---------------------------

3.3. 恶意数据注入攻击数据

被攻击换流器	通过选择直流节点指定相应的被攻击的换流器
攻击参数 r_1	攻击后的换流器运行点距 P-Q 极限图中实线圆的圆心的距离与实线圆半径的比例，参数范围为 0~1.5。
攻击参数 r_2	攻击后的换流器运行点距 P-Q 极限图中虚线圆的圆心的距离与虚线圆半径的比例，参数范围为 0~1.5。
批量分析次数	参数范围为 0~1000。

4 软件程序主要类和函数说明

4.1 系统数据导入函数

声明：`def cache_data(path_ac, path_dc, path_mc, path_bl);`

说明：将选择的交流系统数据文件、VSC-HVDC系统数据文件、量测配置数据文件和节点地理位置数据文件合成转化为一个pf_result.mat文件，并保存至软件的缓存数据文件夹中。

4.2 状态估计数据生成类

声明：`class NetworkData;`

说明：从软件缓存数据文件夹中导入系统数据，并进一步形成状态估计计算所需要的数据，除以有的系统数据外，还包括交流系统节点导纳矩阵、量测误差的方

差矩阵、系统状态变量的真实值等。

4.3 系统单线图绘制函数

声明: `def pushButton_2_click(self);`

说明: 根据节点的地理位置数据绘制系统单线图, 交流节点用圆圈表示, 直流节点用方框表示。

4.4 生成量测数据函数

声明: `def pushButton_3_click(self);`

说明: 通过在量测量真实值上叠加满足正态分布的量测误差模拟生成真实的量测量。

4.5 含 VSC-HVDC 交直流系统状态估计类

声明: `class WlsSe(NetworkData);`

说明: 利用加权最小二乘法对含 VSC-HVDC 交直流系统进行状态估计。

4.6 攻击前残差分析函数

声明: `def pushButton_5_click(self);`

说明: 对攻击前状态估计后各量测量标准化残差进行计算, 并将计算结果绘制为条形图显示。

4.7 攻击前 P-Q 运行极限和运行点分析函数

声明: `def pushButton_6_click(self);`

说明: 计算攻击前被攻击换流器的 P-Q 运行圆图和运行点, 并绘制计算结果。

4.8 VSC-HVDC 系统恶意数据注入攻击策略模型求解类

声明: `class Attack;`

说明: 求解 VSC-HVDC 系统恶意数据注入攻击策略模型, 得到攻击后的量测量。

4.9 批量分析函数

声明: `def batch_main(self);`

说明: 生成多组量测数据, 在各组量测数据下, 求解恶意数据注入攻击策略模型, 并基于攻击后的量测数据进行状态估计, 最后计算各组量测数据对应的攻击前后的最大标准化残差。

5 附图

5.1 修改的 IEEE-14 节点系统单线图

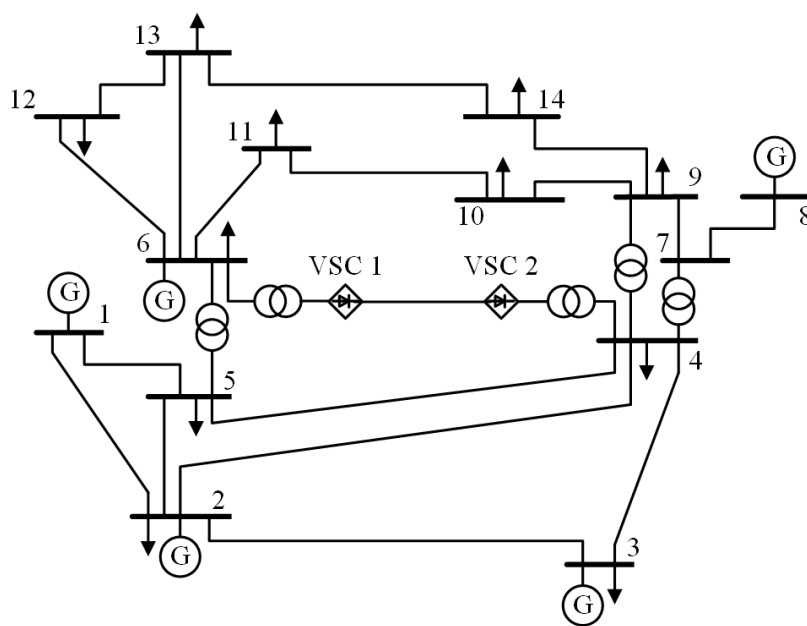


图 13 修改的 IEEE-14 节点系统单线图