Assessing the Impacts of False Data Injection Attacks on Power System Dynamic Security

Dr Junhua Zhao

1. Introduction

False data injection attack (FDIA) can bias power system state estimation by compromising meters and injecting malicious data. Most existing studies focus on investigating the impacts of FDIA on the steady state performance of the system. In this research, we study how FDIA will influence the dynamic security of the system. We will demonstrate that, even by altering the reading of a single meter, the biased state estimate can cause the system to be unstable. A novel methodology is proposed to evaluate how vulnerable a meter is under FDIA. We propose to use the marginal reading of a meter, which makes the largest eigenvalue of the system equals zero, as a vulnerability index with respect to system small disturbance instability. The effectiveness of the proposed method is validated with the IEEE 14 bus test system.

2. Procedure for Assessing the Impacts of False Data Injection Attack

1) Given an initial system state and a compromised meter (If we are interested in determining how vulnerable a sensor S is, we will then choose it to be the compromised meter), randomly generate a set of meter readings for the uncompromised meters as discussed in Section II.B, and set the reading of the compromised meter to a false value.

2) Obtain a system state estimate using a particular state estimation algorithm based on the false meter readings; this state estimate is referred to as a false system state.

3) Solve an OPF model to obtain a dispatch plan based on the false system state.

4) Employing eigenvalue analysis to calculate the system dynamic security index based on the dispatch plan and true system state. A smaller security index indicates that the system is more secure. Repeat steps 1) - 3) for N times to obtain the expected value of the security index.

5) Change the compromised meter reading and repeat steps 1) – 4) until the expected security index is sufficiently close to 0; we define the reading, which makes the security index equals 0, as the marginal reading. It measures the vulnerability of a meter under FDIA.

3. Power System State Estimation

The objective of state estimation is to estimate the system state based on a set of meter measurements. Based on the state estimation theory, the control centre will receive meter readings:

$$Z = \bar{H}\cdot Y + e$$

Where Z denotes the vector of meter readings, Y represents the system state, $\bar{H}$ is the measurement matrix, and e is a vector of Gaussian measurement noise with zero mean and diagonal covariance matrix $\bar{\Sigma}$. In step 1) of our method, given the initial system state Y_0 , all meter readings $z_j, j \neq i$ except the compromised meter i are randomly generated based on above equation.

4. Optimal Power Flow

Based on the false system state, the system operator will solve the optimal power flow problem to determine the system operation plan (e.g. the output of each generator). The OPF model usually takes the following general form:

$$\begin{array}{ll} \text{Min} & f(Y) \\ \text{Subject to} & g(Y) = 0 \\ & h(Y) > 0 \end{array}$$

where $f(Y)$ denotes the optimization objective (e.g. overall generation cost). $g(Y) = 0$ and $h(Y) > 0$ denote the system operation constraints such as the power flow equations and generator capacities.

5. Eigenvalue Analysis

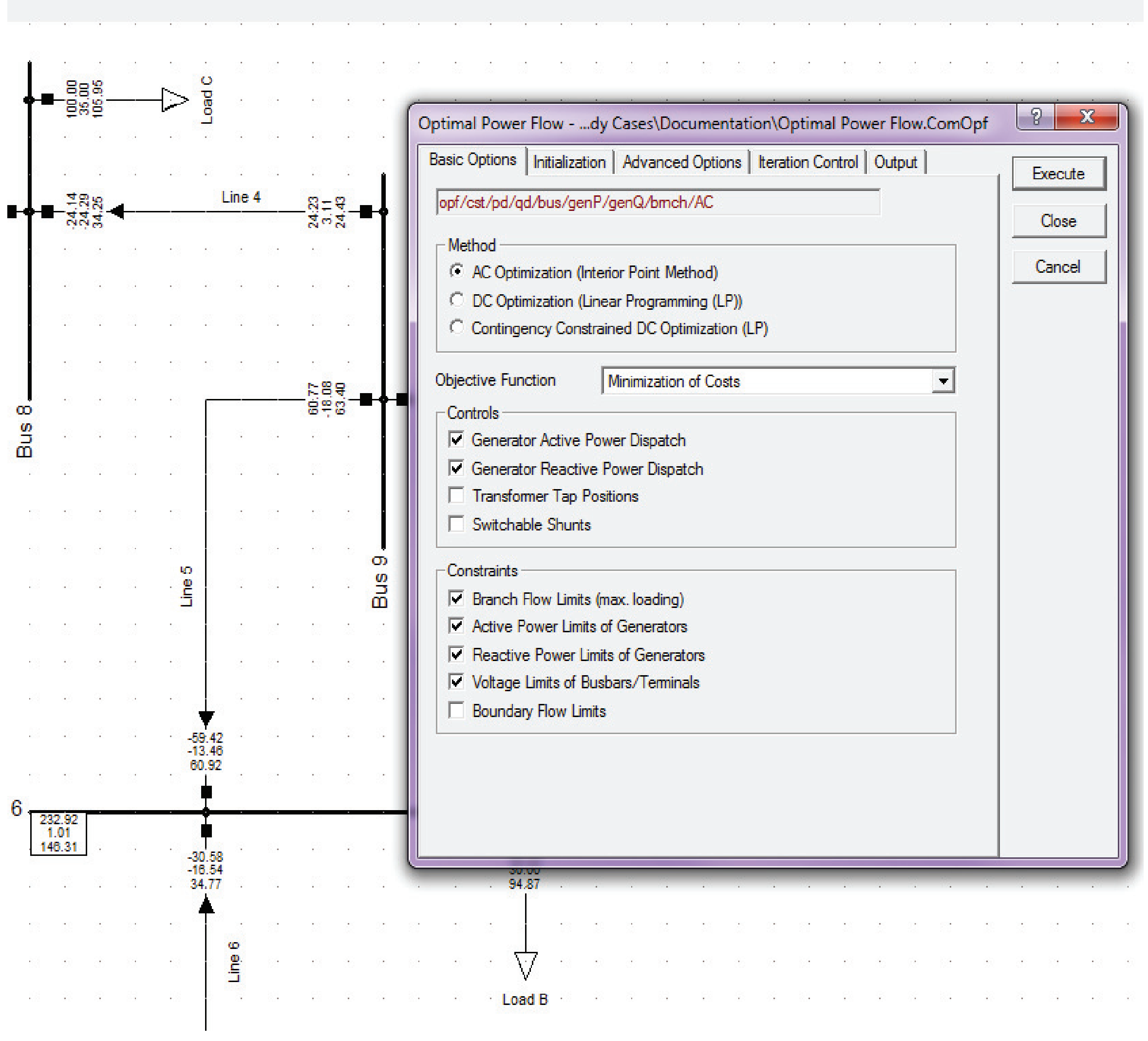
The small disturbance dynamic security index of the power system can be obtained by performing the eigenvalue analysis. Consider the following linearized model of the system:

$$\frac{dX}{dt} = \bar{A}\cdot X + \bar{B}\cdot Y$$
$$0 = \bar{C}\cdot X + \bar{D}\cdot Y$$

Here X represents the vector of system dynamic states (e.g. generator rotor angle and angular speed). $\bar{A}, \bar{B}, \bar{C}, \bar{D}$ are parameter matrices. We can assess the dynamic security of the system by calculating the eigenvalues of the following matrix:

$$\bar{A}' = \bar{A} - \bar{B}\bar{D}^{-1}\bar{C}$$

OPF Calculation in DigSilent Power Factory



Optimal Power Flow - ...dy Cases\Documentation\Optimal Power Flow.ComOpf

opf/cst/pd/qd/bus/genP/genQ/brnch/AC

Method
- ● AC Optimization (Interior Point Method)
- ○ DC Optimization (Linear Programming (LP))
- ○ Contingency Constrained DC Optimization (LP)

Objective Function: Minimization of Costs

Controls
- ☑ Generator Active Power Dispatch
- ☑ Generator Reactive Power Dispatch
- ☐ Transformer Tap Positions
- ☐ Switchable Shunts

Constraints
- ☑ Branch Flow Limits (max. loading)
- ☑ Active Power Limits of Generators
- ☑ Reactive Power Limits of Generators
- ☑ Voltage Limits of Busbars/Terminals
- ☐ Boundary Flow Limits

6. Simulation Results

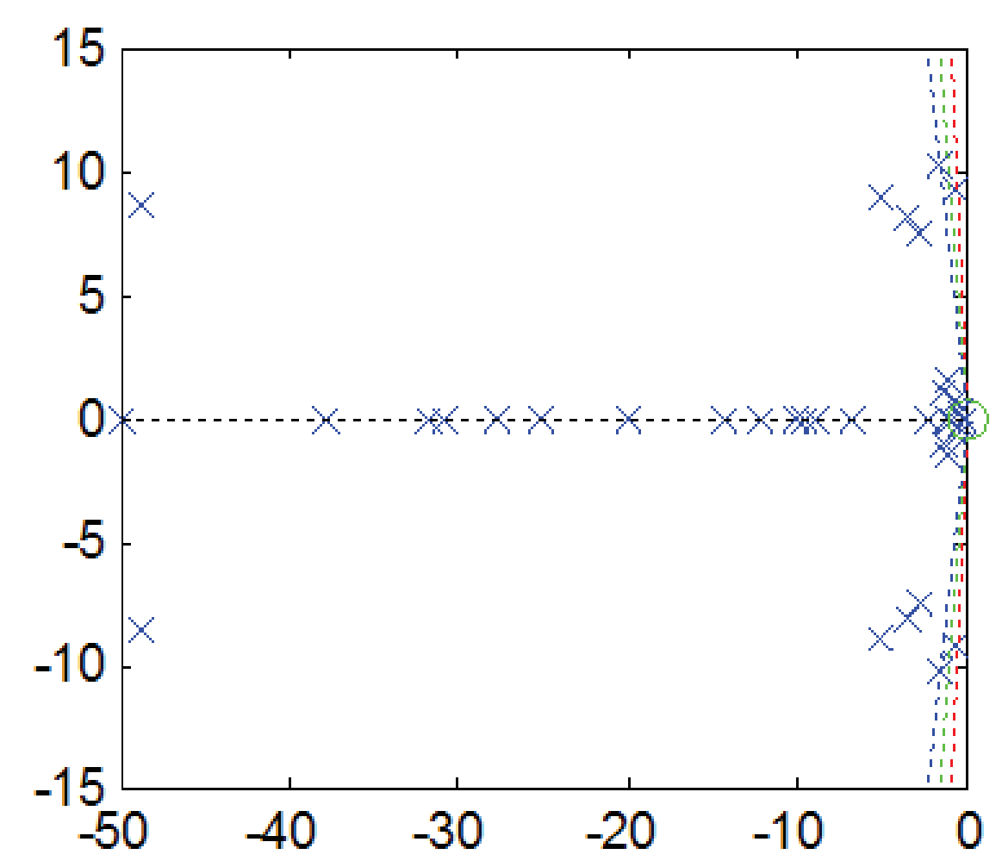


Fig.1 Eigenvalues (stable)

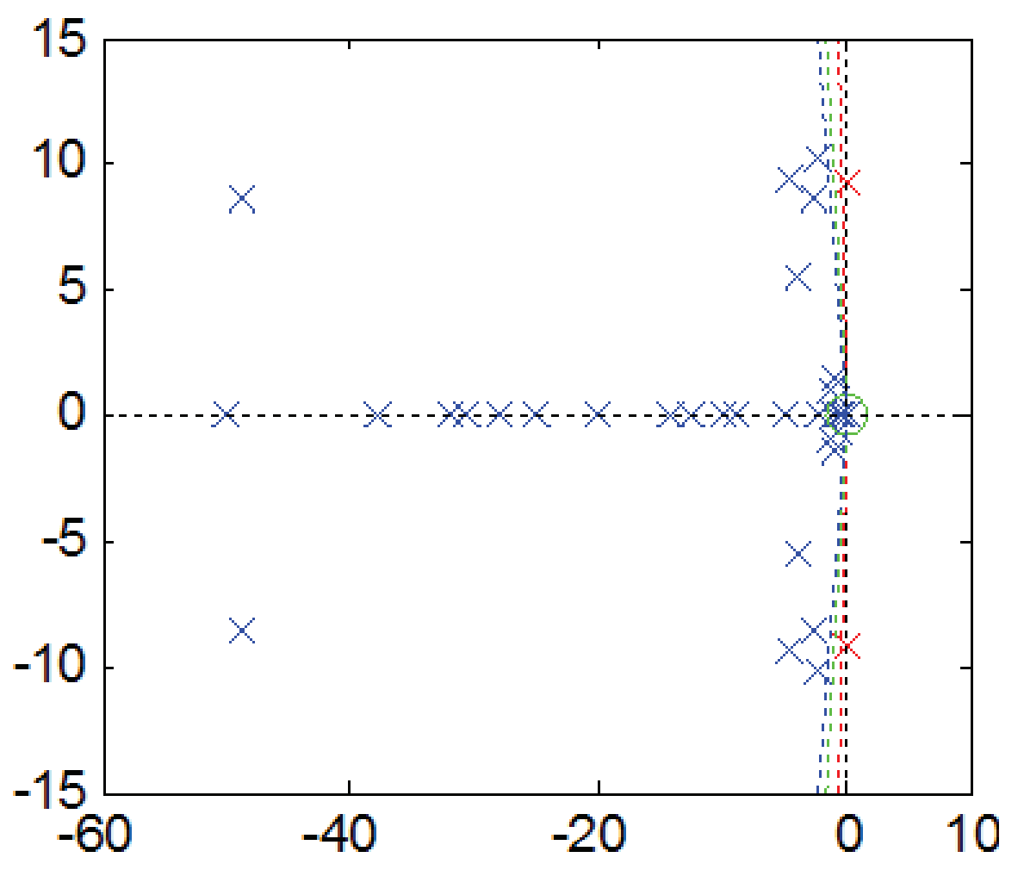
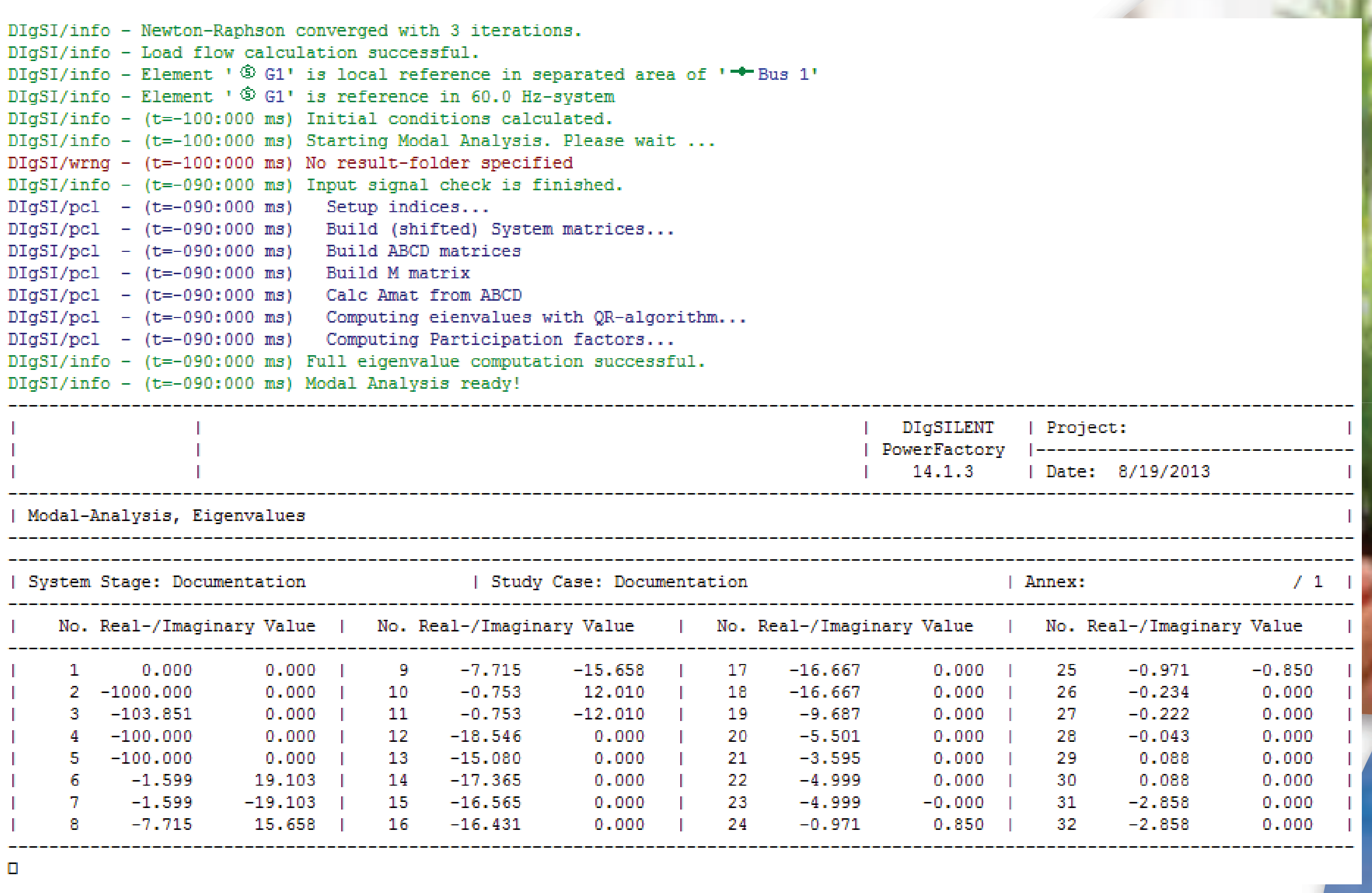


Fig.2 Eigenvalues (unstable)

TABLE I. VULNERABLE METERS AND MARGINAL READINGS

Meter	Marginal reading	Largest real part of eigenvalues
Bus 3	1.79	0.0036
Bus 4	2.23	0.0089
Bus 2	3.55	0.0024
Bus 6	5.75	0.0052
Bus 13	6.69	0.4428

Eigenvalue Analysis in DigSilent Power Factory



```
DIgSI/info - Newton-Raphson converged with 3 iterations.
DIgSI/info - Load flow calculation successful.
DIgSI/info - Element 'Ⓢ G1' is local reference in separated area of '-+-Bus 1'
DIgSI/info - Element 'Ⓢ G1' is reference in 60.0 Hz-system
DIgSI/info - (t=-100:000 ms) Initial conditions calculated.
DIgSI/info - (t=-100:000 ms) Starting Modal Analysis. Please wait ...
DIgSI/wrng - (t=-100:000 ms) No result-folder specified
DIgSI/info - (t=-090:000 ms) Input signal check is finished.
DIgSI/pcl  - (t=-090:000 ms)   Setup indices...
DIgSI/pcl  - (t=-090:000 ms)   Build (shifted) System matrices...
DIgSI/pcl  - (t=-090:000 ms)   Build ABCD matrices
DIgSI/pcl  - (t=-090:000 ms)   Build M matrix
DIgSI/pcl  - (t=-090:000 ms)   Calc Amat from ABCD
DIgSI/pcl  - (t=-090:000 ms)   Computing eienvalues with QR-algorithm...
DIgSI/pcl  - (t=-090:000 ms)   Computing Participation factors...
DIgSI/info - (t=-090:000 ms) Full eigenvalue computation successful.
DIgSI/info - (t=-090:000 ms) Modal Analysis ready!
--------------------------------------------------------------------------------------------------------------------------------
|                 |                                                                       |   DIgSILENT   | Project:                     |
|                 |                                                                       | PowerFactory  |------------------------------
|                 |                                                                       |    14.1.3     | Date:  8/19/2013             |
--------------------------------------------------------------------------------------------------------------------------------
| Modal-Analysis, Eigenvalues                                                                                                    |
--------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------
| System Stage: Documentation                | Study Case: Documentation                      | Annex:                    / 1  |
--------------------------------------------------------------------------------------------------------------------------------
|    No. Real-/Imaginary Value  |    No. Real-/Imaginary Value     |    No. Real-/Imaginary Value    |    No. Real-/Imaginary Value     |
--------------------------------------------------------------------------------------------------------------------------------
|     1       0.000       0.000 |     9      -7.715     -15.658    |    17    -16.667       0.000    |    25     -0.971      -0.850    |
|     2   -1000.000       0.000 |    10      -0.753      12.010    |    18    -16.667       0.000    |    26     -0.234       0.000    |
|     3    -103.851       0.000 |    11      -0.753     -12.010    |    19     -9.687       0.000    |    27     -0.222       0.000    |
|     4    -100.000       0.000 |    12     -18.546       0.000    |    20     -5.501       0.000    |    28     -0.043       0.000    |
|     5    -100.000       0.000 |    13     -15.080       0.000    |    21     -3.595       0.000    |    29      0.088       0.000    |
|     6      -1.599      19.103 |    14     -17.365       0.000    |    22     -4.999       0.000    |    30      0.088       0.000    |
|     7      -1.599     -19.103 |    15     -16.565       0.000    |    23     -4.999      -0.000    |    31     -2.858       0.000    |
|     8      -7.715      15.658 |    16     -16.431       0.000    |    24     -0.971       0.850    |    32     -2.858       0.000    |
--------------------------------------------------------------------------------------------------------------------------------
□
```

7. Conclusion

In this research, a novel method is proposed to quantify the impacts of false data injection attack on the dynamic security of power systems. We demonstrate that even by compromising a single meter, the attacker can cause the system to become small-signal unstable; and the concept of marginal reading is introduced as an index to measure the vulnerability of a meter.

Centre for Intelligent Electricity Networks
The University of Newcastle
Centre for Future Energy Networks
The University of Sydney