

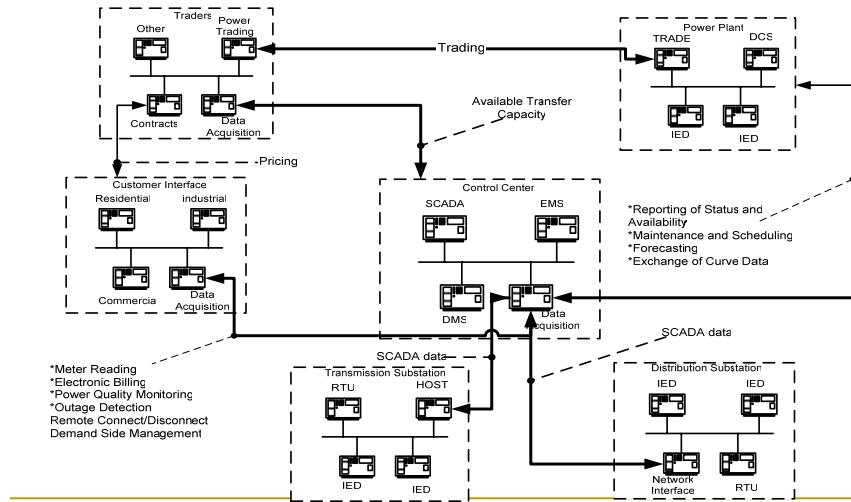
Improving a Methodology to Extract Rules to Identify Attacks in Power System Critical Infrastructure: New Results

Maurílio Pereira Coutinho, Germano Lambert-Torres, Luiz Eduardo Borges da Silva, and Jonas Guedes Borges da Silva –
Federal University of Itajuba - Brazil
José Cabral Neto –Rondonia Power Company – Brazil
Horst Lazarek – Technical University of Dresden - Germany

Critical Infrastructures



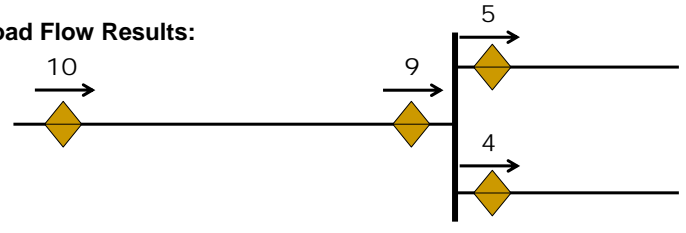
Electrical Power Systems Critical Infrastructures



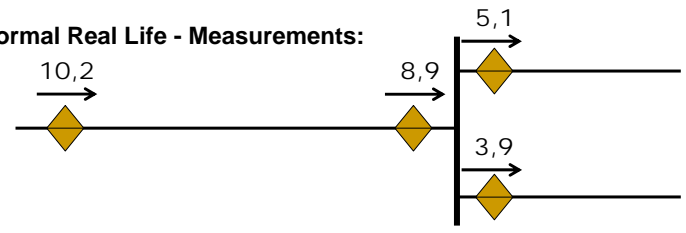
Bose, A., et al. "Flexible and Robust Status Dissemination Middleware for the Electric Power Grid", WSU, 2002

The Main Problem

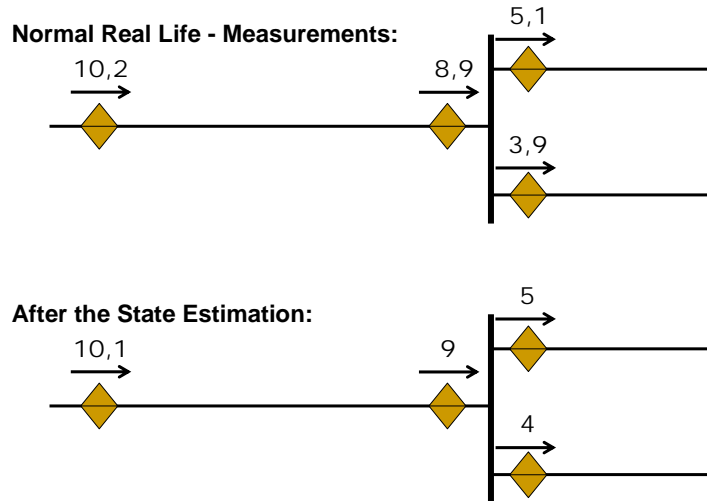
Load Flow Results:



Normal Real Life - Measurements:

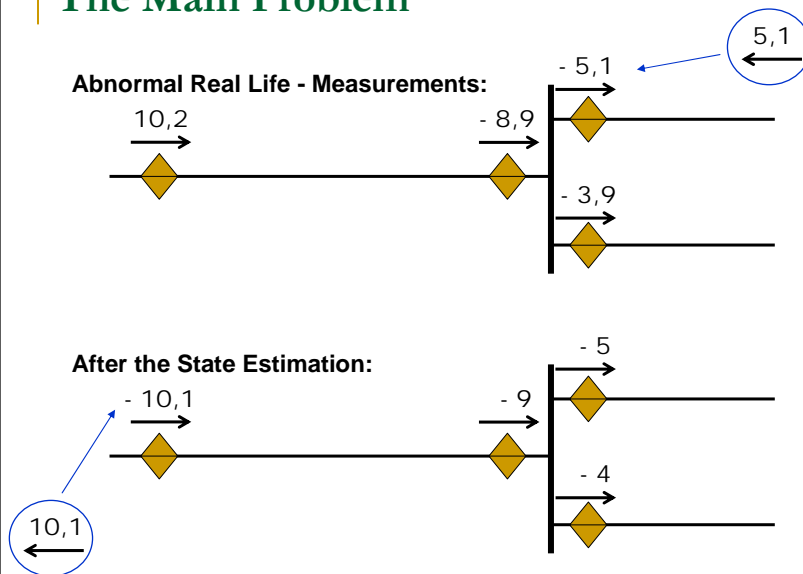


The Main Problem



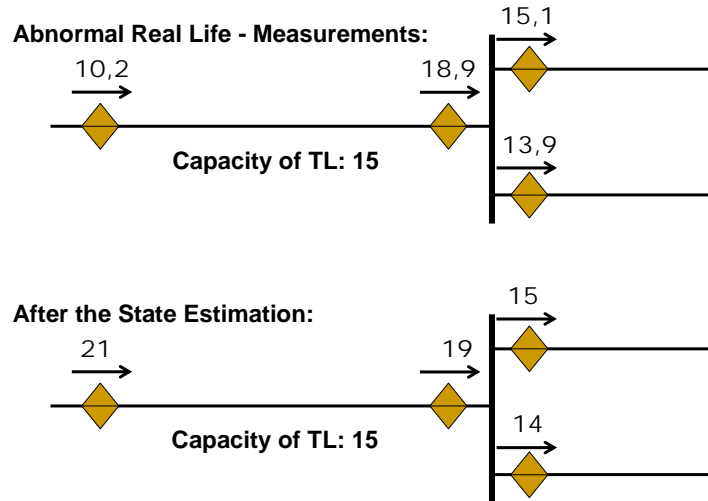
5

The Main Problem



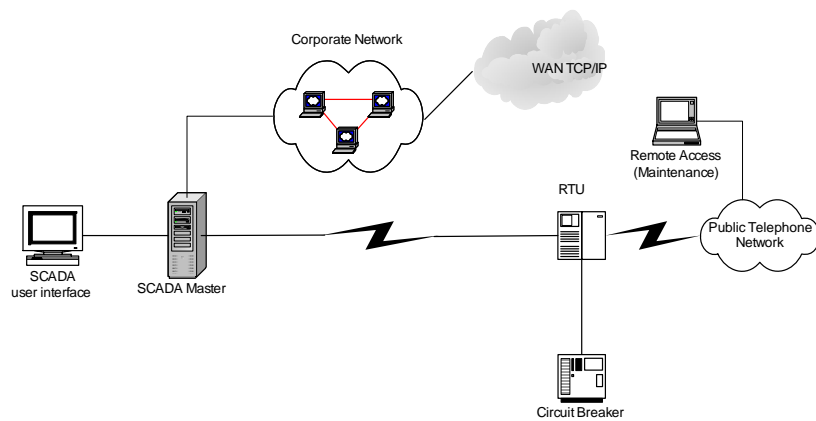
6

Another Problem



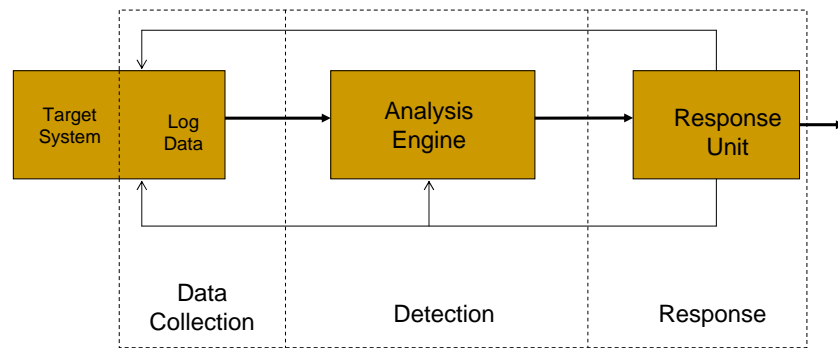
7

SCADA System Communication Model



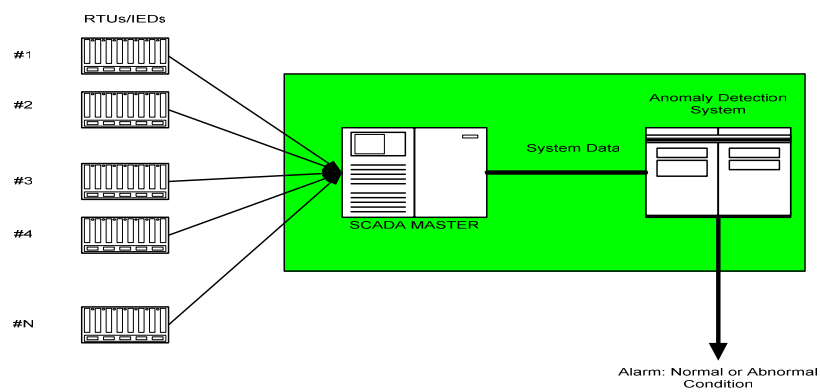
8

Generic Model of Intrusion Detection System



9

Proposed Anomaly Detection Architecture



10

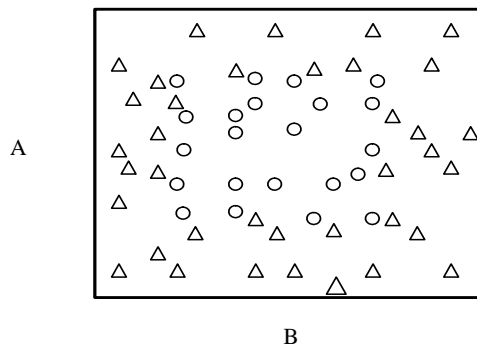
Rough Sets Theory

- Proposed by Z. Pawlak in 1982
- Uses lower and upper approximations of a set
- Reduces the upper set and expands the lower set using the knowledge available in the Original Set of Examples and defining a set of rules that maintain the same inductive classification.

11

Rough Sets Theory

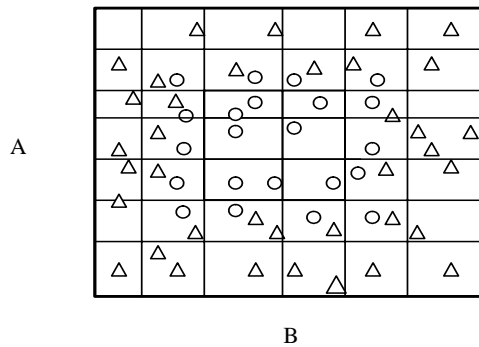
- The main idea: find a discernable set



12

Rough Sets Theory

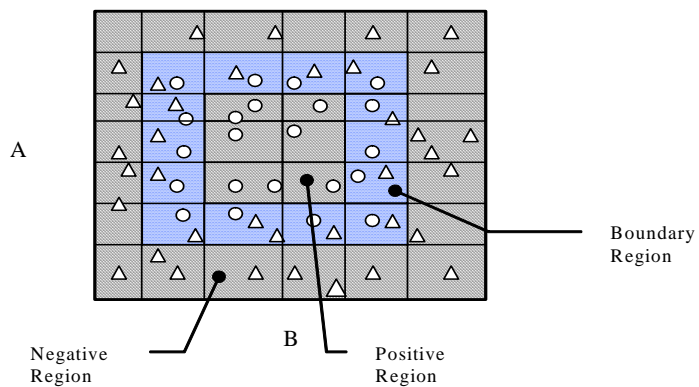
- Division of the space using the attributes



13

Rough Sets Theory

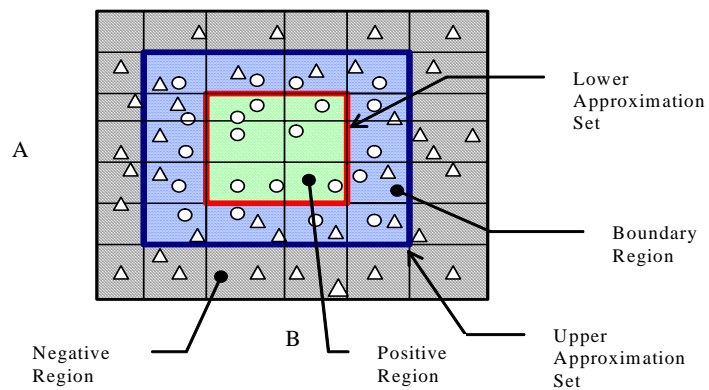
- Three Discernable Regions



14

Rough Sets Theory

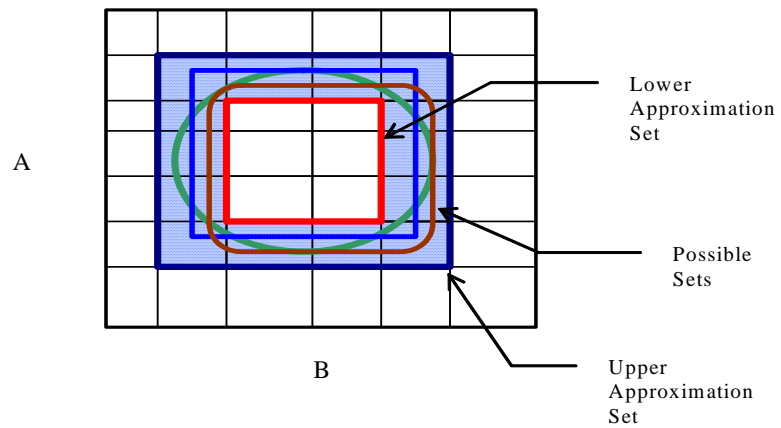
■ Lower and Upper Approximation Sets



15

Rough Sets Theory

■ Possible Sets

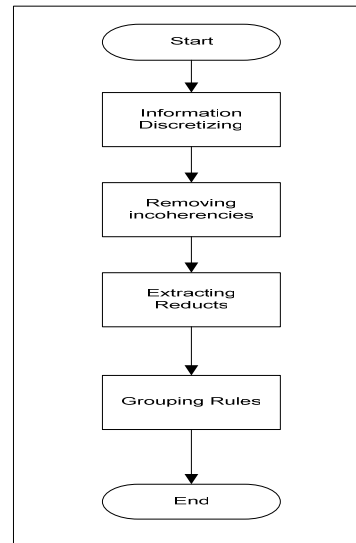


16

Rough Sets Theory Proposed Algorithm

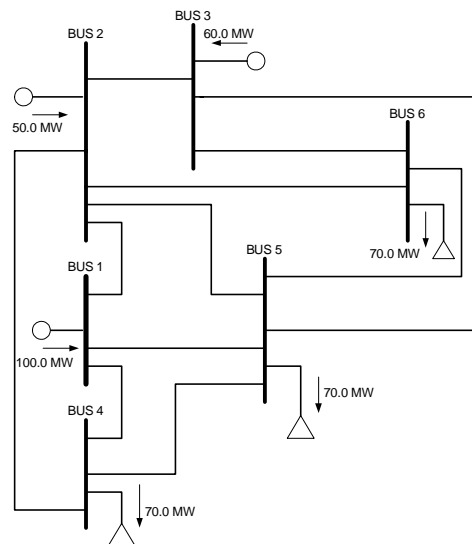
Set of Rules

- If Active Power on Bus 4 ≥ -0.77 and Active Power on Bus 4 < -0.2567 and Active Power on Bus 6 ≥ -0.77 and Active Power on Bus 6 < -0.5133 then output condition is Normal.
- If Active Power on Bus 4 ≥ 0.4667 and Active Power on Bus 4 < 0.71 then output condition is Abnormal.
- If Active Power on Bus 6 ≥ 0.4667 and Active Power on Bus 6 < 0.71 then output condition is Abnormal.



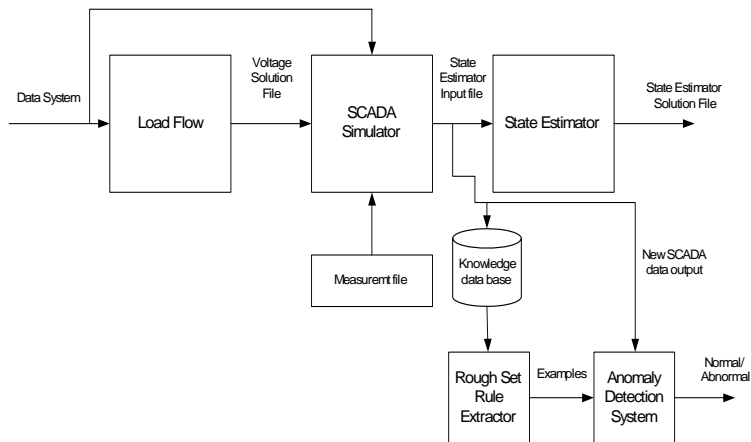
17

Illustrative Example



18

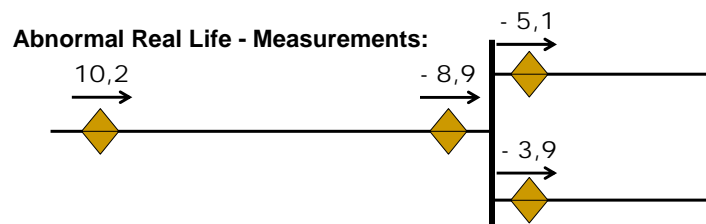
Test Environment Diagram



19

Database Generation

- 45 examples containing the 57 measurements (2565 original data samples) provided by the SCADA simulator program with some sort of errors introduced
- For sake of clarity, the errors were applied only on **Bus 4** and **Bus 6** of the Six Bus Power System and included only sign switch error type.



20

Some Results

```

V 1 1 1.0500000000E+00 1.000E-04
A 1 1 0.0000000000E+00 1.000E-04
I 1 1 1.0787184633E+00 1.000E-02 2.0661845005E-01 1.000E-02
I 2 4.9999997656E-01 1.000E-02 1.0000000975E+00 1.000E-02
I 3 5.9999998883E-01 1.000E-02 5.9999999970E-01 1.000E-02
I 4 -6.9999998098E-01 1.000E-02 -7.000000159E-01 1.000E-02
I 5 -6.9999998542E-01 1.000E-02 -6.9999999861E-01 1.000E-02
I 6 -6.9999998569E-01 1.000E-02 -6.9999999599E-01 1.000E-02
F 1 2 2.8692958228E-01 1.000E-02 -1.5370907928E-01 1.000E-02
F 1 4 4.3642327197E-01 1.000E-02 2.0994987978E-01 1.000E-02
F 1 5 3.5536560905E-01 1.000E-02 1.5037764955E-01 1.000E-02
F 2 1 -2.7788988175E-01 1.000E-02 1.2769252903E-01 1.000E-02
F 2 3 1.6235984678E-02 1.000E-02 -6.8377435467E-03 1.000E-02
F 2 4 3.3625310381E-01 1.000E-02 4.7475533518E-01 1.000E-02
F 2 5 1.5913964959E-01 1.000E-02 1.9011396616E-01 1.000E-02
F 2 6 2.6626112023E-01 1.000E-02 2.1427601073E-01 1.000E-02
F 3 2 -1.6192816562E-02 1.000E-02 -5.8643777656E-02 1.000E-02
F 3 5 1.8031588028E-01 1.000E-02 1.6516547798E-01 1.000E-02
F 3 6 4.3587692511E-01 1.000E-02 4.9347829938E-01 1.000E-02
F 4 1 -4.2534439593E-01 1.000E-02 -2.0719387096E-01 1.000E-02
F 4 2 -3.2042041362E-01 1.000E-02 -4.6386767811E-01 1.000E-02
F 4 5 4.5764828567E-02 1.000E-02 -2.8938452525E-02 1.000E-02
F 5 1 -3.4376001516E-01 1.000E-02 -1.6841831208E-01 1.000E-02
F 5 2 -1.5275868126E-01 1.000E-02 -2.1200810552E-01 1.000E-02
F 5 3 -1.7264611276E-01 1.000E-02 -1.9947687704E-01 1.000E-02
F 5 4 -4.5314578728E-02 1.000E-02 -4.7162224557E-02 1.000E-02
F 5 6 1.4479402488E-02 1.000E-02 -7.2934479413E-02 1.000E-02
F 6 2 -2.5804510996E-01 1.000E-02 -2.4269807513E-01 1.000E-02
F 6 3 -4.2770560886E-01 1.000E-02 -4.7323343918E-01 1.000E-02
F 6 5 -1.4249266860E-02 1.000E-02 1.5931518320E-02 1.000E-02

```

21

Rough Sets Rules

- If Active Power on $-0.77 \leq \text{Bus 4} < -0.2567$ and Active Power on $-0.77 \leq \text{Bus 6} < -0.5133$ then output condition is Normal.
- If Active Power on $0.4667 \leq \text{Bus 4} < 0.71$ then output condition is Abnormal.
- If Active Power on $0.4667 \leq \text{Bus 6} < 0.71$ then output condition is Abnormal.

22

Some Results

TABLE I
LOAD FLOW AND STATE ESTIMATION OUTPUTS FOR BASE CASE

LINES	LOAD FLOW [MW]	STATE ESTIMATION OUTPUT [MW]
FROM 4 TO 1	-42.53	-42.53
FROM 4 TO 2	-32.04	-32.04
FROM 4 TO 5	4.58	4.58
FROM 6 TO 2	-25.0	-25.80
FROM 6 TO 3	-42.77	-42.77
FROM 6 TO 5	-1.42	-1.42

```
» rules
Enter Input File Name: 'Scada_out.txt'
Enter Number of Inputs: 6
Input: 1 RESULT: ABNORMAL
Input: 2 RESULT: ABNORMAL
Input: 3 RESULT: ABNORMAL
Input: 4 RESULT: ABNORMAL
Input: 5 RESULT: ABNORMAL
Input: 6 RESULT: ABNORMAL
```

23

Some Conclusions and Future Work

- Validation Tests using the “QMUL Electricity Test Data” for the “IEEE Test Systems”.
- The “QMUL Electricity Test Data” was filtered and corrupted with noise and a set of outages and induced attacks.
- Introduce this technology in a real Control Center
- Establish the type of attack (classification system)

24