On Reliability Analysis of Smart Grids under Topology Attacks: A Stochastic Petri Net Approach

Beibei Li (Visiting Student), Rongxing Lu*, Raymond Choo, Wei Wang, and Sheng Luo

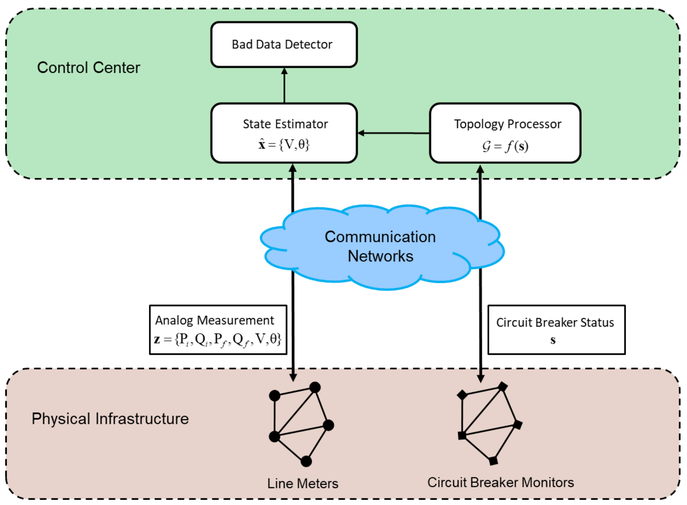
Contact Email: rlu1@unb.ca

Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB)

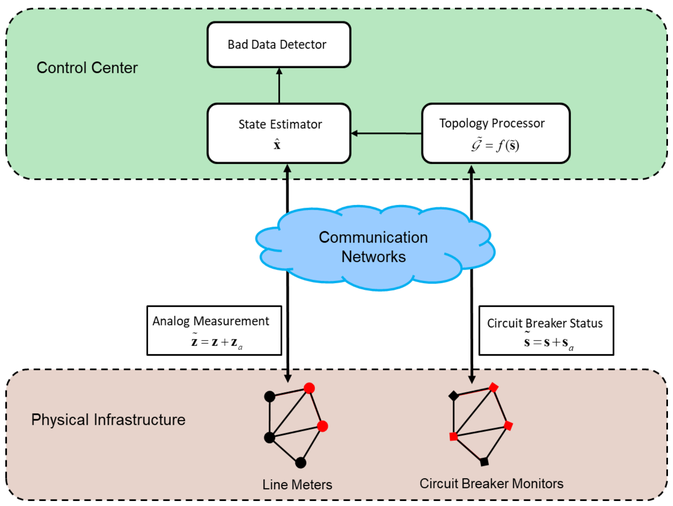
ABSTRACT

Building an efficient, smart, and multifunctional power grid while maintaining high reliability and security is an extremely challenging task, particularly in the ever-evolving cyber threat landscape. The challenge is also compounded by the increasing complexity of power grids in both cyber and physical domains. In this article, we develop a stochastic Petri net based analytical model to assess and analyze the system reliability of smart grids, specifically against topology attacks and system countermeasures (i.e., intrusion detection systems and malfunction recovery techniques). Topology attacks, evolving from false data injection attacks, are growing security threats to smart grids. In our analytical model, we define and consider both conservative and aggressive topology attacks, and two types of unreliable consequences (i.e., system disturbances and failures). The IEEE 14-bus power system is employed as a case study to clearly explain the model construction and parameterization process. The benefit of having this analytical model is the capability to measure the system reliability from both transient and steady-state analysis. Finally, intensive simulation experiments are conducted to demonstrate the feasibility and effectiveness of our proposed model.

System Model



Adversary Model



State Estimation & Bad Data Detection

$$\mathbf{z}=\mathbf{H}_{\mathcal{G}}\mathbf{x}+\boldsymbol{\eta}$$

- $\mathbf{z}\in\mathbb{R}^{m\times 1}$: measurement data
- $\mathbf{x}\in\mathbb{R}^{n\times 1}$: real system status data
- $\mathbf{H}_{\mathcal{G}}\in\mathbb{R}^{m\times n}$: measurement Jacobian matrix
- $\eta\in\mathbb{R}^{m\times 1}$: measurement noise
- $\mathcal{G}$: system topology

$$\hat{\mathbf{x}}=[\mathbf{H}_{\mathcal{G}}{}^{T}\mathbf{C}^{-1}\mathbf{H}_{\mathcal{G}}]^{-1}\mathbf{H}_{\mathcal{G}}{}^{T}\mathbf{C}^{-1}\mathbf{z}\triangleq\mathbf{\Lambda}\mathbf{z}$$

$$\mathbf{r}=\mathbf{z}-\hat{\mathbf{z}}=\mathbf{z}-\mathbf{H}_{\mathcal{G}}\mathbf{\Lambda}\mathbf{z}=(\mathbf{I}-\mathbf{H}_{\mathcal{G}}\mathbf{\Lambda})\mathbf{z}$$

$$\begin{cases}\text{Bad data detected, if } \|\mathbf{r}\|_2\geq\tau\\ \text{No bad data detected, if } \|\mathbf{r}\|_2<\tau\end{cases}$$

$$\tilde{\mathbf{z}}=\mathbf{z}+\mathbf{z}_a$$

$$\tilde{\mathbf{s}}=\mathbf{s}+\mathbf{s}_a$$

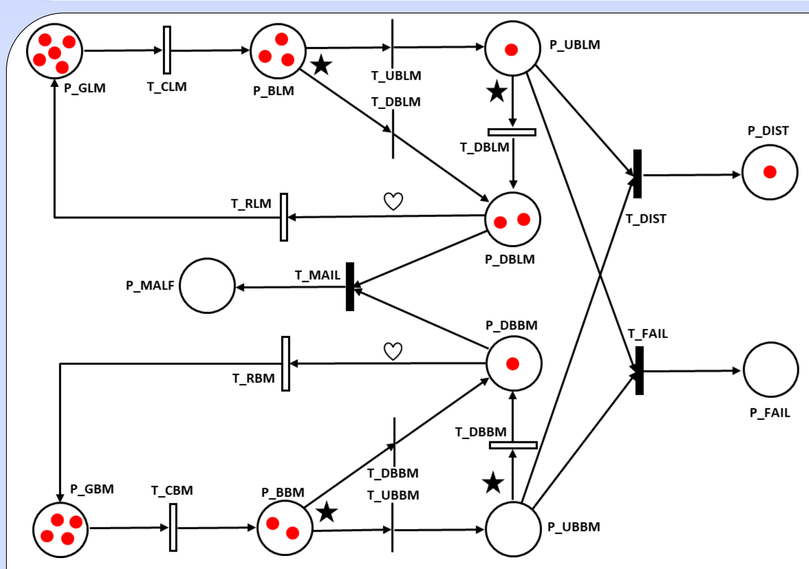
$$\tilde{\mathcal{G}}=f(\tilde{\mathbf{s}})=f(\mathbf{s}+\mathbf{s}_a)$$

$$\tilde{\mathbf{z}}=\mathbf{H}_{\tilde{\mathcal{G}}}\mathbf{x}+\boldsymbol{\eta}$$

$$\hat{\mathbf{x}}=\arg\min_{\mathbf{x}}[\tilde{\mathbf{z}}-\mathbf{H}_{\tilde{\mathcal{G}}}\mathbf{x}]^{T}\mathbf{C}^{-1}[\tilde{\mathbf{z}}-\mathbf{H}_{\tilde{\mathcal{G}}})\mathbf{x}]\triangleq\tilde{\mathbf{\Lambda}}\tilde{\mathbf{z}}$$

$$\tilde{\mathbf{r}}=\tilde{\mathbf{z}}-\hat{\mathbf{z}}=(\mathbf{I}-\mathbf{H}_{\tilde{\mathcal{G}}}\tilde{\mathbf{\Lambda}})\tilde{\mathbf{z}}$$

$$\begin{cases}\text{Bad data detected, if } \|\tilde{\mathbf{r}}\|_2\geq\tau\\ \text{No bad data detected, if } \|\tilde{\mathbf{r}}\|_2<\tau\end{cases}$$



Analytical SPN Model

Table II. Places in the SPN model

Place	Meaning
P_GLM	Place of good line meters
P_BLM	Place of bad line meters
P_GBM	Place of good breaker monitors
P_BBM	Place of bad breaker monitors
P_DBLM	Place of detected bad line meters
P_UBLM	Place of undetected bad line meters
P_DBBM	Place of detected bad breaker monitors
P_UBBM	Place of undetected bad breaker monitors
P_DIST	Place of system disturbance: 0 before and 1 after
P_FAIL	Place of system failure: 0 before and 1 after
P_MALF	Place of system malfunction: 0 before and 1 after

Table III. Transitions in the SPN model

Transition	Meaning
T_CLM	Transition that the attacker compromises a line meter
T_CBM	Transition that the attacker compromises a breaker monitor
T_DBLM	Transition that the intrusion detection system detects a bad line meter
T_UBLM	Transition that the intrusion detection system fails to detect a bad line meter
T_DBBM	Transition that the intrusion detection system detects a bad breaker monitor
T_UBBM	Transition that the intrusion detection system fails to detect a bad breaker monitor
T_RLM	Transition that the system operator recovers a line meter
T_RBM	Transition that the system operator recovers a breaker monitor
T_DIST	Transition that the power grid encounters a system disturbance
T_FAIL	Transition that the power grid encounters a system failure
T_MALF	Transition that the power grid encounters a system malfunction

The MxST of IEEE 14-bus System

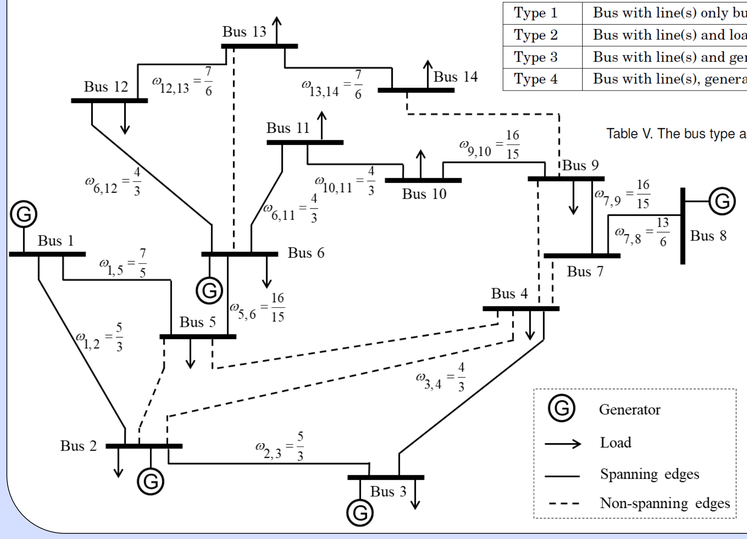


Table IV. Weights assigned to each bus

Bus type	Description	Weight assigned
Type 1	Bus with line(s) only but no generator or load	1 unit
Type 2	Bus with line(s) and load(s) but no generator	2 units
Type 3	Bus with line(s) and generator but no load	3 units
Type 4	Bus with line(s), generator and load(s)	4 units

Table V. The bus type and total weight assigned in IEEE 14-bus system

Bus index	Bus type	Weight assigned
#1	Type 3	3 units
#2	Type 4	4 units
#3	Type 4	4 units
#4	Type 2	2 units
#5	Type 2	2 units
#6	Type 4	4 units
#7	Type 1	1 unit
#8	Type 3	3 units
#9	Type 2	2 units
#10	Type 2	2 units
#11	Type 2	2 units
#12	Type 2	2 units
#13	Type 2	2 units
#14	Type 2	2 units

Numerical Results

Transient Analysis

$$\text{MTTD}=\int_0^{\infty}t[1-Q_D(t)]dt$$

$$\text{MTTF}=\int_0^{\infty}t[1-Q_F(t)]dt$$

Steady-State Analysis

$$R=(1-p_{malf})*(1-\frac{\alpha*p_{dist}+\beta*p_{fail}}{\alpha+\beta})^k$$

$$=(1-\frac{\alpha*\overline{N}_S/N+\beta*N_S/N}{\alpha+\beta})^k$$