PARIS 2022

Study Committee D2

Information Systems and Telecommunication

Paper 10503_2022

AI BASED SECURITY MECHANISM TO FALSE DATA INJECTION ATTACK – A CASE STUDY OF NORTHERN REGION OF INDIAN GRID

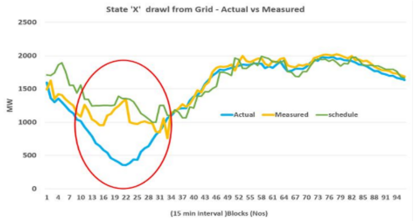
S Naresh RAM*, P KARTHIK, N S SODHA [2] , N M L SACHDEVA [3] ,S LAKRA, M K AGARWAL, N NALLARSAN

Power System Operation Corporation ltd (NRLDC), Former Power Grid [2] , Former Central Electric Authority[3]

INDIA

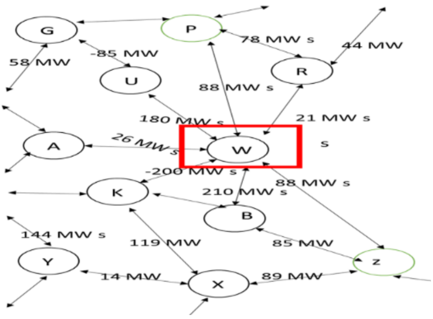
Motivation

- Recently, real time drawl data of State X of Northern Region is calculated incorrectly, due to erroneous telemetry. Which led to deviation of around 800MW w.r.t to Scheduled drawl.



Such erroneous data was due to failure of a major fiber optic link , resulted complete suspect of the pooling Station 'W' and stations connected to it .

Approx layout of the region



- The same situation may be created by false data injection attack also.

Why State estimator failed here?

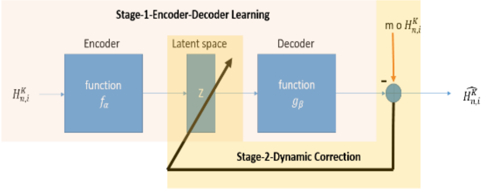
Ans: State estimator works on least square minimization principle, under both Topology and measurement missing. Recursively estimating topology(s) and Line (L) becomes biased and non convergent solutions.

$$\min_{s,L} \|F - h(s,\ L)\|_2 \text{ where } s \in 0, 1$$

To defend from such false data/ suspect cases ,there is a need for the special tool which estimates the individual feeder(F) data even under suspect measurement (L) and topology (S).

Tool: INTELLIGENT STATE ESTIMATOR

A Novel Model is proposed based on two ideas where one is learning auto-encoder through the Gated Recurrent Unit and the other is adjusting/ generating the data through latent dimensions to match the real time data.



Here " $H^K{}_{n,i}$ " represents the SCADA/meter data for time step K, n_{th} feeder and i_{th} data sample.

Here "m" represents data of the feeders which are not affected by FDI attack

stage 1 : Auto encoder :

In this stage the model learns inter temporal correlation between parallel feeders and non-parallel feeders through latent space/compressed space (Z).

Such learning be done through below objective functions

$$\alpha^*, \beta^* = \arg \min_{(\alpha,\beta)} \frac{1}{n} \sum_{i=1}^{n} L(H^K_{N,i},\ g_\beta(f_\alpha(H^K_{N,i})))$$

Stage 2: Dynamic correction :

Stage 1 captures the inter temporal correlation but, an extra correction is needed for the model to understand the actual dynamics.

The updating/correcting the latent space vector $\widehat{Z^k_{M,i}}$ through the **equation b** and the data estimation after dynamic correction through **equation c is** $\widehat{H^k_{M,i}}$

$$\widehat{Z^k_{M,i}} = \arg \min_{(Z^k_{M,i})} ||g_\beta(Z^k_{M,i}) - H^k_{N,i} \circ m|| \tag{b}$$

$$\widehat{H^k_{M,i}} = m \circ g_\beta(\widehat{Z^K_{M,i}}) + (1 - m) \circ H^k_{N,i} \tag{c}$$

Estimated data Of the attacked/suspected feeder

http://www.cigre.org

Study Committee D2

Information systems and telecommunication

Paper 10503_2022

AI BASED SECURITY MECHANISM TO FALSE DATA INJECTION ATTACK – A CASE STUDY OF NORTHERN REGION OF INDIAN GRID continued

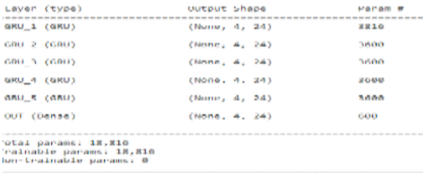
Experimental setup & test results

Dataset:-

Indian Grid SCADA and Meter data of State X (27 nos ISTS feeders) of Northern Region is collected for a period of **3 months at 15-minute interval** for estimating the corrupt data.

Training- Network Architecture:-

Network comprises of **5 layer GRU cells** with encoder parameters of **18,816** .Whereas decoder has **18,675** parameters and the latent space Z dimension is **4x20.**



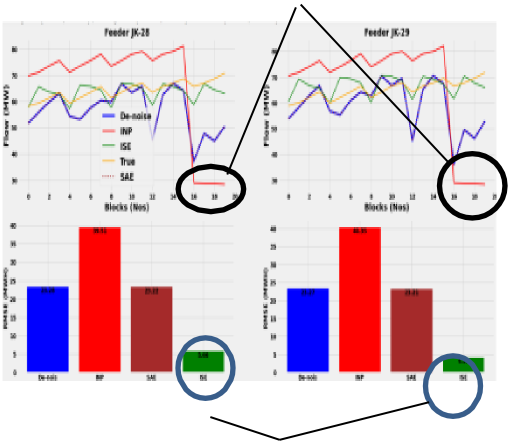
```
Layer (type)                 Output Shape              Param #
=================================================================
GRU_1 (GRU)                  (None, 4, 24)             3816
GRU_2 (GRU)                  (None, 4, 24)             3600
GRU_3 (GRU)                  (None, 4, 24)             3600
GRU_4 (GRU)                  (None, 4, 24)             3600
GRU_5 (GRU)                  (None, 4, 24)             3600
OUT (Dense)                  (None, 4, 24)             600
=================================================================
otal params: 18,816
rainable params: 18,816
Non-trainable params: 0
_________________________________________________________________
```

Results:

Proposed tool tested on four different case and to demonstrate its effectiveness, the model compared with SAE, De noising Auto encoder models which were State of the art models in this filed.

Case-1 Parallel feeder data suspect case

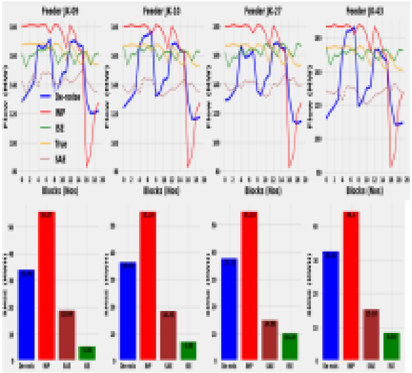
Stuck at value 30 MW



Through ISE tool, the estimated error is lowest (~4MW)

Case 2 : FDI attack on Station "W“

False data injected - four ICTs



Discussion

- The proposed tool applied on different datasets and attained better results.
- This tool not only estimates the false data, but can also be used to identify the outliers i.e (FDIA attack) through simple addition of threshold logic to stage 1.
- For cases like false generation injection and false generation outage the proposed tool effectively identified and the results of such cases are properly explained in the paper.

Conclusion

- Elucidates the importance of defense mechanism to avert the adverse impact of cyber-attacks or data suspect cases of Power system.
- The proposed tool **ISE** outperformed other ML models with an average RMSE of **15%** which is quite good to apply in real time conditions.
- The proposed tool is flexible and not subject to specific conditions such as distribution, environment etc. i.e can be adopted to any national /regional/state Grid for reliable operations.