WIDE AREA MONITORING PROTECTION AND CONTROL (WAMPAC) CYBERSECURITY FOR HVDC APPLICATIONS

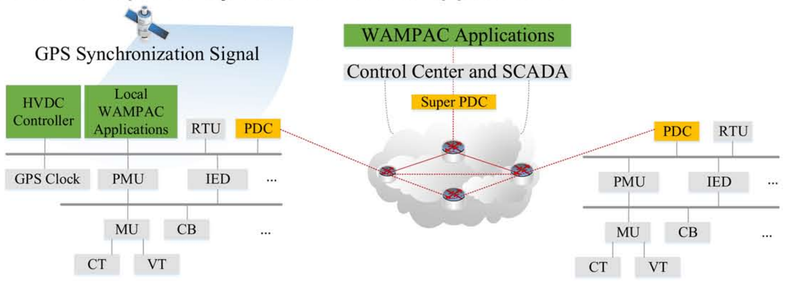
Model-Based Detection and Mitigation Toward Real-Time Protection

Bo Chen (bo.chen@anl.gov) , **Sang-il Yim** (yim@anl.gov), **Hyekyung (Clarisse) Kim** (clarisse@anl.gov)
Center for Energy, Environmental, and Economic Systems Analysis (CEEESA)
Argonne National Laboratory

ABSTRACT

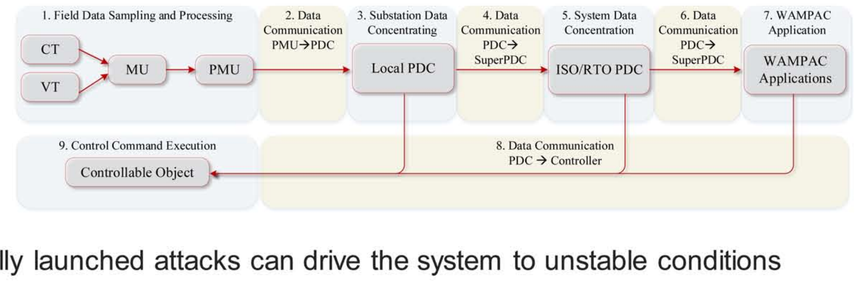
Wide Area Measurement, Protection, and Control (WAMPAC) system enables high voltage direct current (HVDC) systems to provide advanced grid applications in many areas such as transient stability improvement, wide area damping control, and maximum power transfer improvement. However, the WAMPAC system inevitably introduces an enlarged attack surface. We have developed a model-based detection and mitigation method for real-time protection of WAMPAC-based HVDC applications against False Data Injection (FDI) that enables:

- Cross-validation based on physical principles using local and remote data
- Compromised data are replaced with accurate data generated by the algorithm
- Real-time protection performance required by various HVDC applications
- Easy implementation

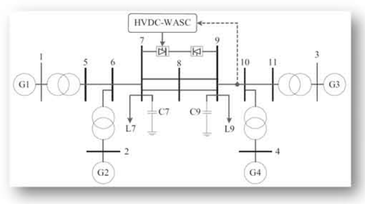


MOTIVATION

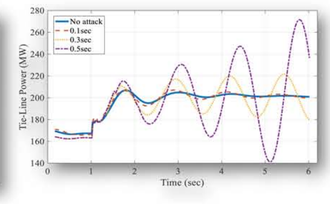
- HVDC are critical assets that must be protected.
- WAMPAC data processing involves multiple cyber vulnerabilities



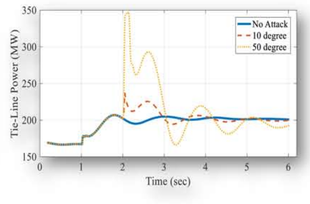
- Successfully launched attacks can drive the system to unstable conditions



Two-Area Test System



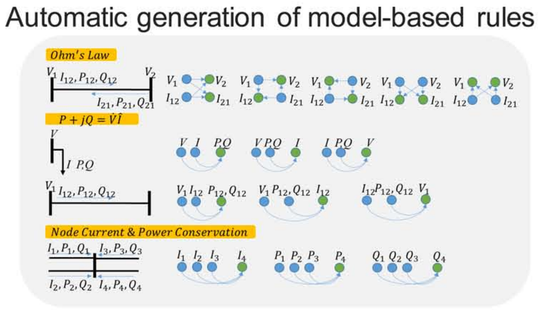
Denial-of-Service Attack

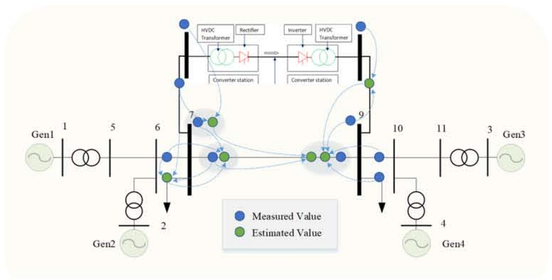


False Data Injection Attack

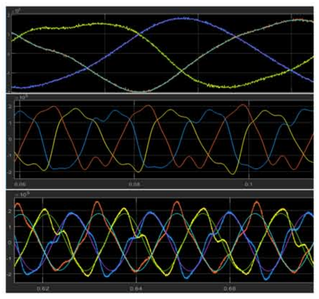
MODEL-BASED DETECTION

- Automatic generation of model-based rules



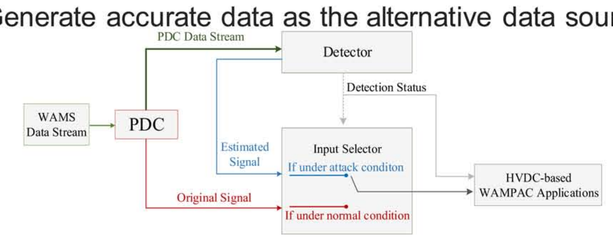


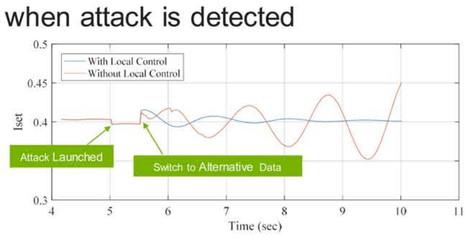
- Self-checking and cross-checking for data integrity
  - Robust to high-level harmonics and noises
  - Exhaustive case studies: various operation conditions



Case No.	Operation Condition: Normal Condition	Load Shedding Condition	Swing Condition	Fault Condition	Location	Accuracy	Results: Missed Positive?	False Positive?	First Malicious Data Detected?
1	x				N/A	100%	No	No	√
2	x				N/A	100%	No	No	√
3	x				N/A	100%	No	No	√
4	x				N/A	100%	No	No	√
5	x				N/A	100%	No	No	√
6	x				N/A	100%	No	No	√
7	x				N/A	100%	No	No	√
8	x				N/A	100%	No	No	√
9	x				N/A	100%	No	No	√
10	x				N/A	100%	No	No	√
11		x			Bus7, 100 MW	100%	No	No	√
12		x			Bus7, 100 MW	100%	No	No	√
13		x			Bus7, 100 MW	100%	No	No	√
14		x			Bus7, 100 MW	100%	No	No	√
15		x			Bus9, 100 MW	100%	No	No	√
16		x			Bus9, 100 MW	100%	No	No	√
17		x			Bus9, 100 MW	100%	No	No	√
18		x			Bus8, 100 MW	100%	No	No	√
19		x			Bus7, 200 MW	100%	No	No	√
20		x			Bus7, 200 MW	100%	No	No	√

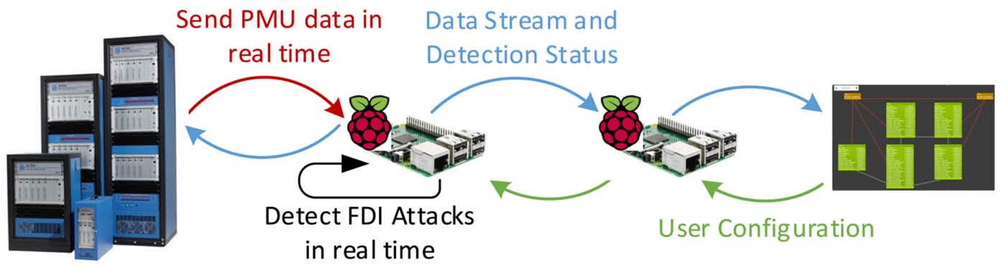
- Generate accurate data as the alternative data source when attack is detected



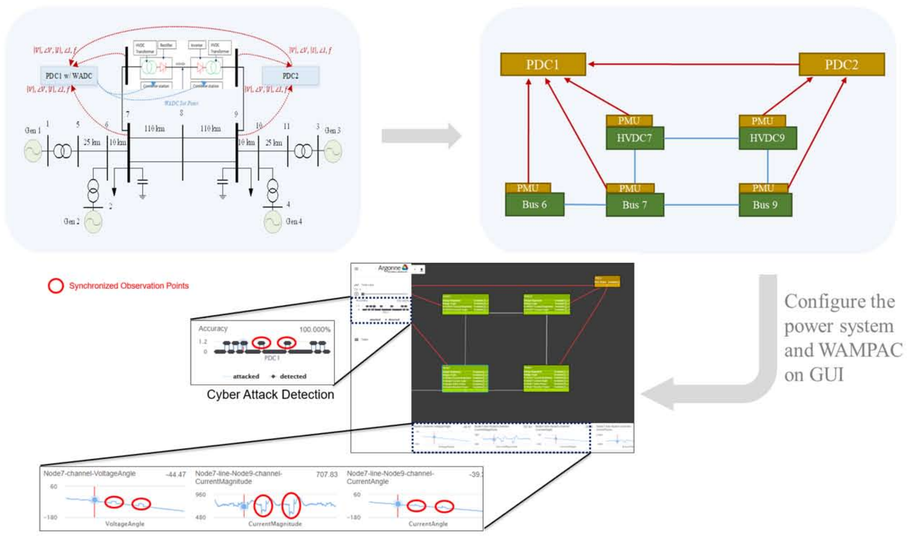


HARDWARE-IN-THE-LOOP VALIDATION

- Hardware-In-The-Loop
  - Various tests performed
  - Slow-injection attack performed



- Interactive User Interface



CONCLUSIONS

- Rule-based method requires minimal computational memory and capacity. Rapid execution time allows real-time evaluation of data samples (30 samples/s) without introducing delays.
- Triggers alarm accurately when thresholds are violated
- Not sensitive to randomly changing load demand or noise/harmonics
- Currently, the threshold parameter for attack detection is set manually using historical data of the user's system. Method can be made more generally applicable by developing a way to automatically set the threshold parameter.
- Since method is not functionally dependent on the WADC controller model, future work can easily adapt this method to other HVDC applications.

REFERENCES

- "Improving Grid Resilience Using High-Voltage dc: Strengthening the Security of Power System Stability," in IEEE Power and Energy Magazine, vol. 17, no. 3, pp. 38-47, May-June 2019.
- "Wide Area Monitoring Protection and Control Cybersecurity for HVDC Applications", presented in IEEE Power and Energy General Meeting, August, 2019.
- "Cyber Attack Detection for WAMPAC-based HVDC Applications," 2020 IEEE PES T&D Conference (submitted).
- "Cyber security of wide-area monitoring, protection and control systems for HVDC applications," IEEE Transactions on Power Systems (abstract accepted).

ACKNOWLEDGMENTS

- This project is led by ABB, Inc., with support from the US Department of Energy's division of Cybersecurity for Energy Delivery Systems (CEDS).
- This work was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily state or reflect those of the United States Government or any agency thereof.