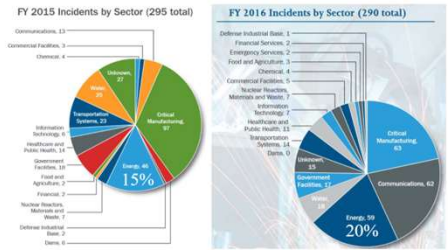
Machine Learning Framework for Packet Anomaly Detection in Smart Grid Substation Networks

Sowmya Bandari, Sai Lamba Karanam, Dr. Byrav Ramamurthy
School of Computing

Why Smart Grid Security?

A Smart Grid (SG) is an advanced electrical network that integrates digital communication, automation, and real-time monitoring to enhance efficiency, reliability, and security. With this advent, Grid has been exposed to the Internet not only to the Service providers but also the Cyber attackers can access this data and modify any data that can cause severe damage to the Grid system.

- In 2015 a well-known Ukrainian power grid company was the subject of a cyber-attack which led to the indefinite end of its operation[1]
- A cyberattack on the substation at LaGuardia Airport in New York City in December 2018 resulted in a power transformer explosion, which caused a 45-minute disruption in airport operations and a 2-hour flight grounding. [2]



Motivation & Objective

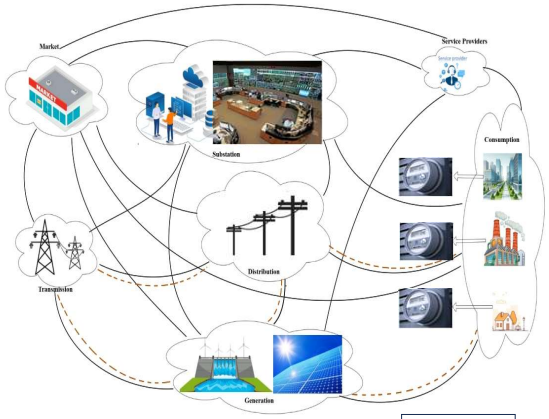
- IEC-60870-5-104 (IEC-104) lacks built-in security, making Smart Grids vulnerable to advanced cyberattacks undetectable by traditional IDS.
- To build an ML-based IDS for real-time, accurate detection of IEC-104 anomalies with low false positives.
- By leveraging the real-time dataset from UKPN Power Grid Dataset [5], from which realistic network traffic is emulated between Remote Terminal Units (RTUs) and Human-Machine Interfaces (HMIs).

Architecture and Threat Model

Recent research indicates that cyberattacks on SG infrastructure have targeted multiple points across the network. These attacks can occur on a single device or in a distributed fashion, leveraging vulnerabilities in communication protocols such as IEC104, and IEC 61850 of Supervisory Control and Data Acquisition(SCADA). Each domain within the Smart Grid faces unique security challenges.

Critical Points of Exploitation in the Smart Grid:

- SCADA & Control Systems
- Communication Network
- Field Devices & IoT
- Power Generation & Substations
- Enterprise IT & Cloud Systems

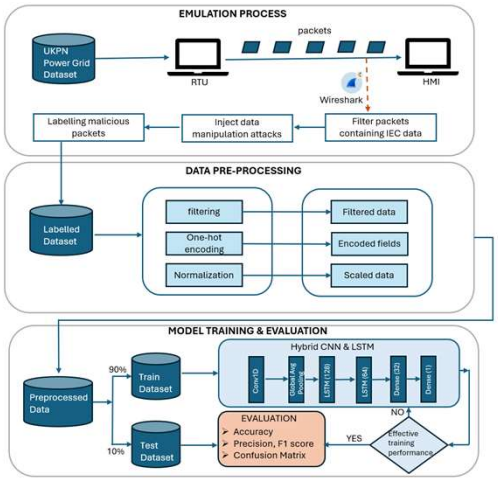


Smart Grid Conceptual Model

Below mentioned are the implementation details:

- **Dataset Preparation**: Preprocessed IEC-104 traffic and UKPN smart meter data, injecting anomalies such as False Data Injection (FDI) by modifying protocol-level features (TTL, TOS, Checksum, TCP Flags, etc.).
- **Feature Engineering:** Extracted critical packet-level features including sequence numbers, TCP flags, checksums, and raw byte data to capture both behavioral and structural changes caused by attacks.
- **Model Development & Evaluation:** build ML model and train using labeled dataset & evaluate its performance

System Architecture



Results

- Tree-based models like **Random Forest** are robust and offer strong classification performance for feature-rich packet data.
- **Deep learning models (Conv+LSTM)** are particularly promising when temporal patterns and packet sequences are considered.

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	92%	92%	88%	90%
XGBoost	87%	87%	79%	83%
Conv + LSTM Layers	86%	86%	77%	81%
MLP Classifier	86%	82%	83%	82%
Gradient Boosting	71%	92%	27%	41%
AdaBoost	68%	100%	17%	28%
Ridge Classifier	68%	68%	33%	44%
Bernoulli Naive Bayes	66%	57%	55%	56%

Conclusion and Future Work

- The Smart Grid consists of multiple layers of vulnerabilities that can be exploited.
- Even security mechanisms themselves can be targeted and bypassed by sophisticated attackers.
- Using an ICS emulator to simulate real-world cyberattacks and evaluate security defenses.
- This study demonstrated the effectiveness of machine learning, particularly deep learning models like Conv+LSTM, in detecting cyberattacks data integrity attacks on IEC-104.
- Extend the binary classification model to a multi-class classification framework to not only detect malicious traffic but also classify specific types of attacks

Acknowledgements

This work was supported by the Nebraska Public Power District through the Nebraska Center for Energy Sciences Research at the University of Nebraska-Lincoln.

References

1. "Analysis of the Cyber Attack on the Ukrainian Power Grid" Electricity Information Sharing and Analysis Center (E-ISAC)
2. https://www.cybersecurity-insiders.com/cyber-attacks-can-cause-transformer-explosions/
3. https://www.cisa.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_IR_Pie_Chart_S508C.pdf
4. "Study of Smart Grid Communication Network Architectures and Technologies" Journal of Computer and Communications > Vol.7 No.3
5. https://ukpowernetworks.opendatasoft.com/explore/dataset/ukpn-smart-meter-consumption-substation/information/