Intrusion Detection in Smart Grid Distribution Domain Using Deep Ruptures Detection

Sarah Chahine (MSc. Computer Engineering Graduate)
Faculty of Engineering
University of Balamand
Balamand, El Koura, Lebanon
E-mail: sarah.chahine@std.balamand.edu.lb

Authors: Sarah Chahine
Dr. Chafic Mokbel

Sarah Chahine grew up in Kaftoun Lebanon. She received her Bachelor and Masters Degree in Computer Engineering from the University of Balamand. She is now working with JobDiva Tech Labs. Her research interests include learning algorithms.

Overview

- **Introduction to Smart Grids**
- Distribution Domain
- Smart Grid Challenges
- Intrusion Detection System
- The Simulated System
- Suggested IDS
- Results and Analysis
- Conclusion

What is Smart Grid?

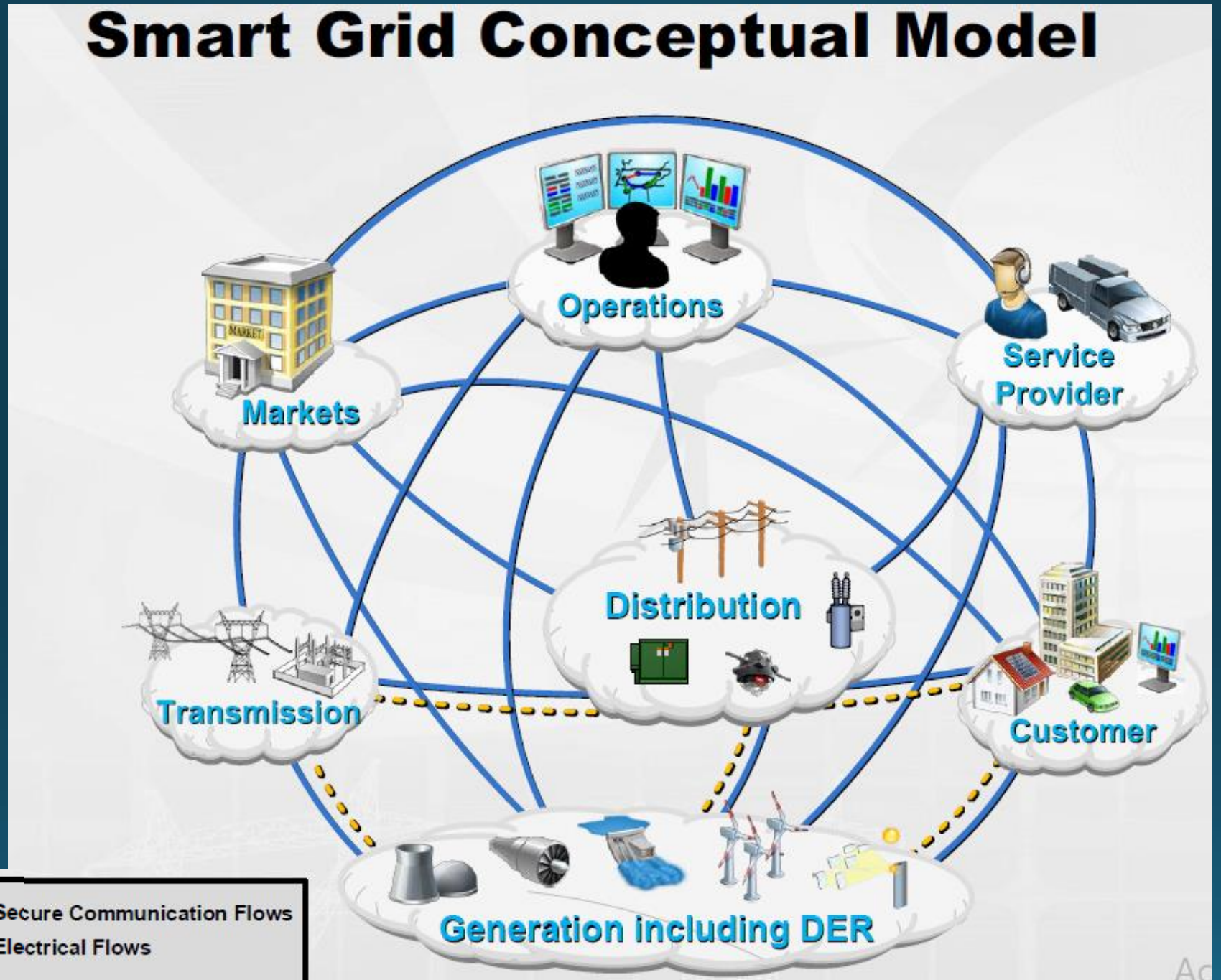
Smart grid is an intelligent power network that aims to provide a reliable and economic system that handles power supply and consumption.

It faces many challenges whether in the electric domain or the network domain.

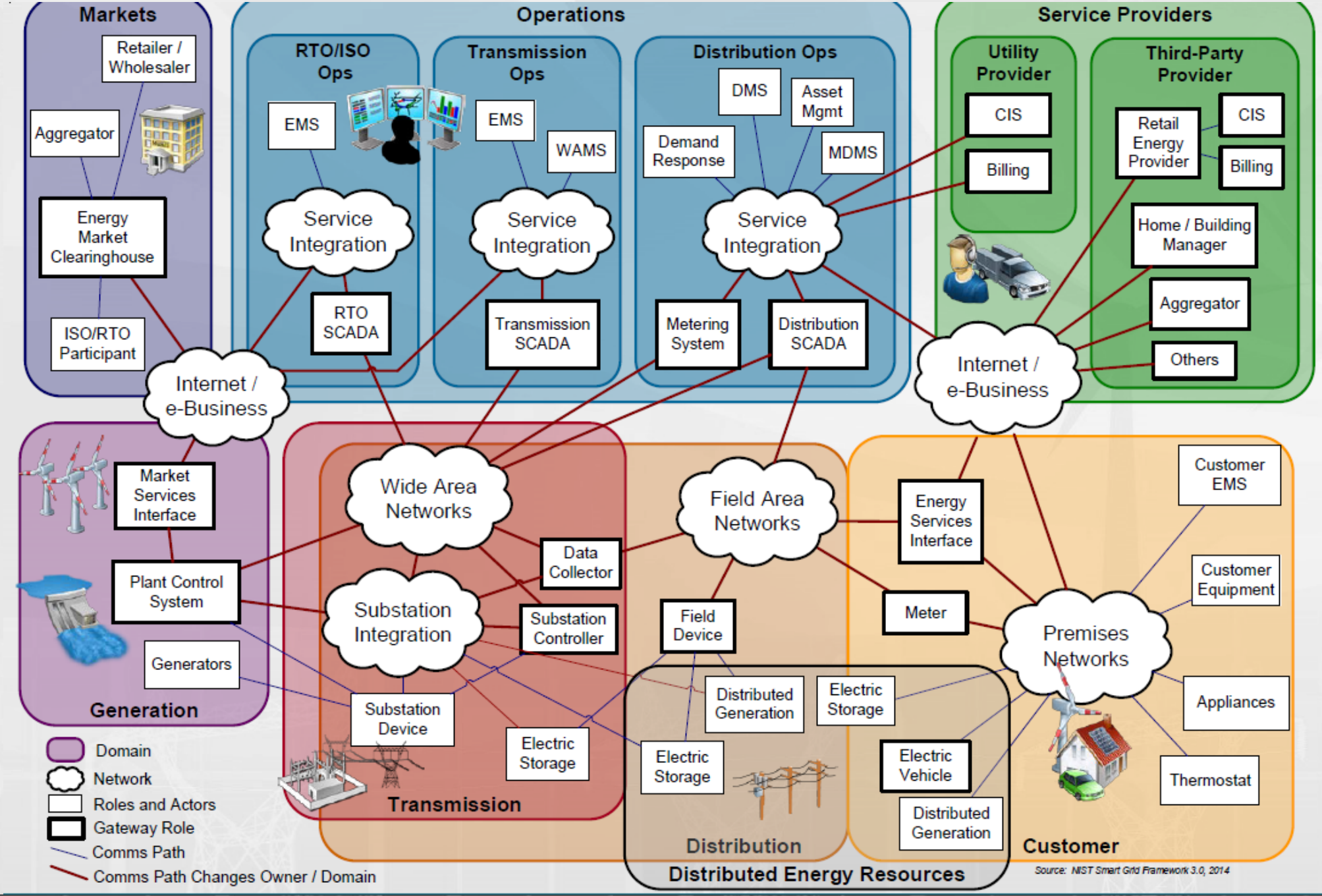
Overview

- Introduction to Smart Grids
- **Distribution Domain**
- Smart Grid Challenges
- Intrusion Detection System
- The Simulated System
- Suggested IDS
- Results and Analysis
- Conclusion

Smart Grid Conceptual Model



Source: DRAFT NIST Smart Grid Framework 4.0


Markets
Retailer / Wholesaler
Aggregator
Energy Market Clearinghouse
ISO/RTO Participant
Operations
RTO/ISO Ops
EMS
RTO SCADA
Transmission Ops
EMS
WAMS
Transmission SCADA
Distribution Ops
DMS
Asset Mgmt
Demand Response
MDMS
Metering System
Distribution SCADA
Service Integration
Service Integration
Service Integration
Service Providers
Utility Provider
CIS
Billing
Third-Party Provider
Retail Energy Provider
CIS
Billing
Home / Building Manager
Aggregator
Others
Internet / e-Business
Internet / e-Business
Market Services Interface
Plant Control System
Generators
Generation
Wide Area Networks
Substation Integration
Data Collector
Substation Controller
Substation Device
Electric Storage
Transmission
Field Area Networks
Field Device
Distributed Generation
Electric Storage
Distribution
Energy Services Interface
Meter
Electric Vehicle
Distributed Generation
Customer EMS
Customer Equipment
Premises Networks
Appliances
Thermostat
Customer
Distributed Energy Resources
Domain
Network
Roles and Actors
Gateway Role
Comms Path
Comms Path Changes Owner / Domain
Source: NIST Smart Grid Framework 3.0, 2014

Overview

- Introduction to Smart Grids
- Distribution Domain
- **Smart Grid Challenges**
- Intrusion Detection System
- The Simulated System
- Suggested IDS
- Results and Analysis
- Conclusion

Smart Grid Challenges

- Grid architectures are not mutually exclusive.
- Grid operation is highly interdependent with market structure, which in turn is limited by the nature of grid operations.
- Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways.
- Trustworthiness
  - Privacy
  - Reliability
  - Resilience
  - Safety
  - Security

Overview

- Introduction to Smart Grids
- Distribution Domain
- Smart Grid Challenges
- **Intrusion Detection System**
- The Simulated System
- Suggested IDS
- Results and Analysis
- Conclusion

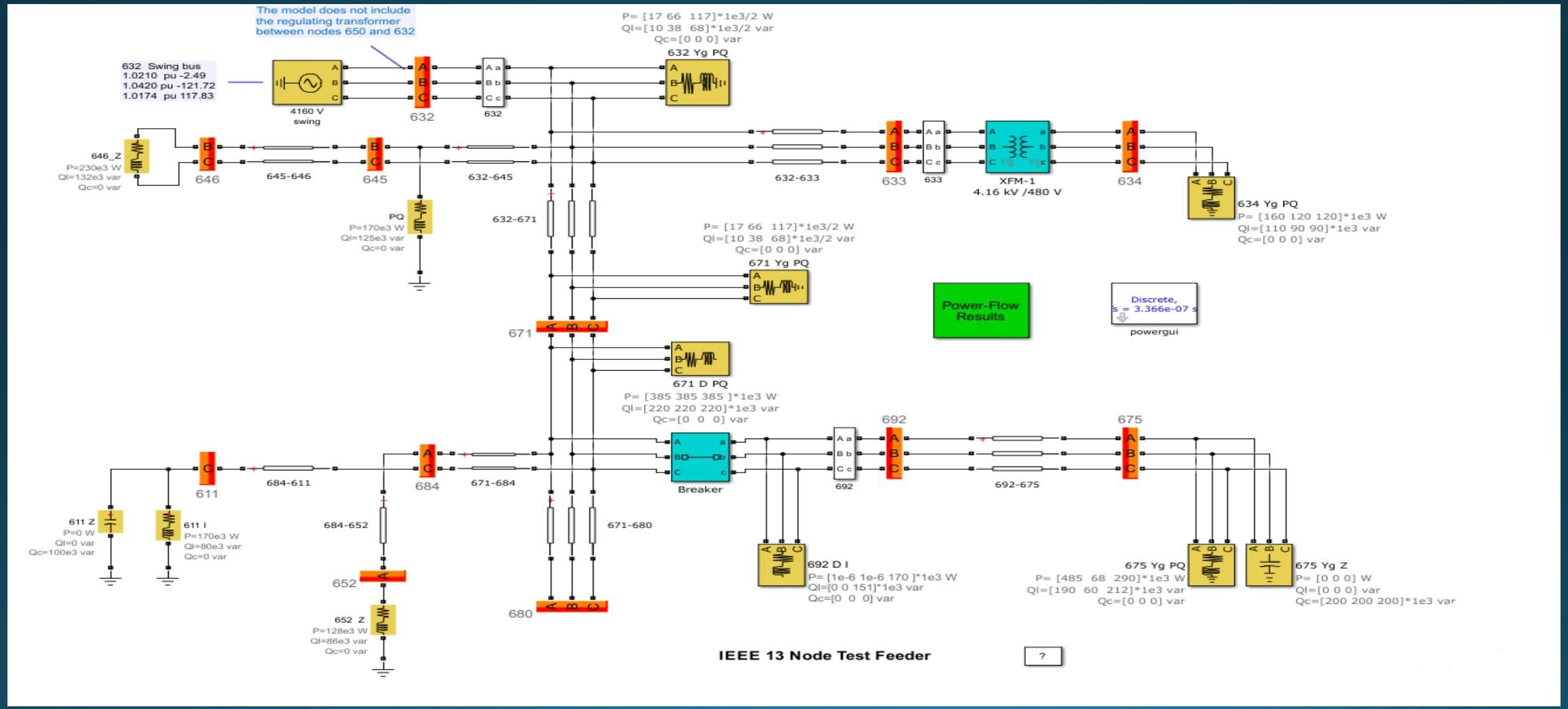
Intrusion Detection System

- An **Intrusion Detection System (IDS)** is a system that observes **network traffic** for suspicious action and produces alerts when such activity is discovered.
- The methodologies of intrusion detection are categorized as :
  - "Anomaly-based Detection" (AD)
  - "Signature-based Detection" (SD)
  - "Stateful Protocol Analysis" (SPA)
- For industries, IDS helps protecting Industrial Control Systems from cyberattacks.
- Online vs. Offline Detection

Overview

- Introduction to Smart Grids
- Distribution Domain
- Smart Grid Challenges
- Intrusion Detection System
- **The Simulated System**
- Suggested IDS
- Results and Analysis
- Conclusion

IEEE 13-Bus Test Feeder



Simulation System

- The simulation system is made up from open-source components:
  - HELICS
  - NS-3
  - GridDyn
  - Gridlab-d
  - In addition to MATLAB

Simulation System

- The HELICS acts as the main connector between all the different parts.
- The NS-3 is used as the network of the system that connects the various parts.
- The GridDyn is used for creating and simulating the transmission grid.
- The Gridlab-d and the MATLAB are used for the creation and the simulation of the distribution grid.
- System setup:
  - Server Side (Control Center)
  - Client Side (Where all the action will be taken)

Simulation System

- The creation of a system to be able to simulate a smart grid takes many steps even if it does not include all the seven domains.
- Several tests are run where a simulation is created as if the hacker is going into the system.
- The attack creates a glitch for a fraction of time.

Overview

- Introduction to Smart Grids
- Distribution Domain
- Smart Grid Challenges
- Intrusion Detection System
- The Simulated System
- **Suggested IDS**
- Results and Analysis
- Conclusion

Suggested IDS

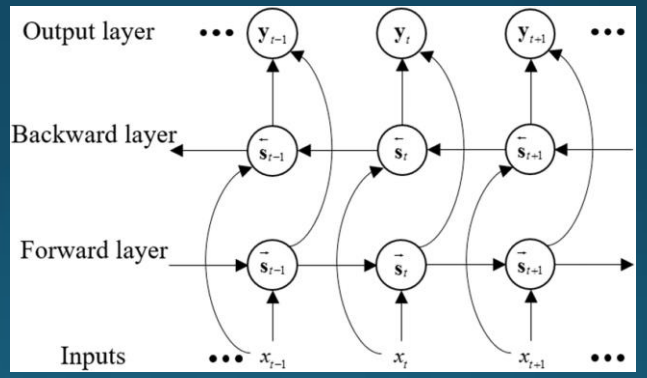
- Assumption
  - A cyberattack shall induce a change in the properties of the electrical signals
- Key idea for IDS
  - Detect changes in the properties of the electrical signals => detection of ruptures
- Detection of ruptures:
  - Cost Function
  - Search Method
  - Limitations

Rupture Detection of Glitches

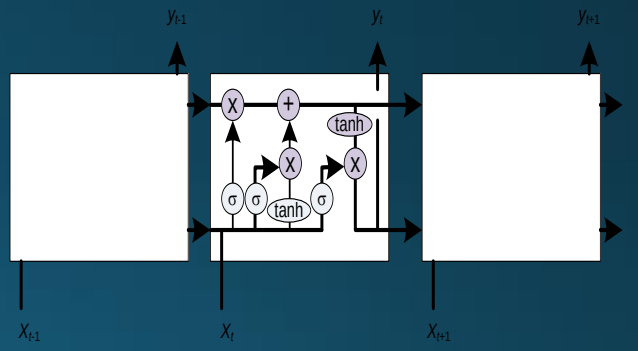
- AR Order 4
- AR Order 10
- Gaussian Process Change
- Least Absolute Deviation
- Least Squared Deviation
- Linear Model Change
- Square Root of Square Sum
- Normalized Square Root of Square Sum

Suggested IDS

- Detection of ruptures
  - Model-based
    - E.g. a model of the background signal and the cost of fitting the model on local segment of the signal
  - Statistical
    - Hypotheses testing
- Non linear deep detection
  - Non linear predictive CNN filter
  - LSTM model

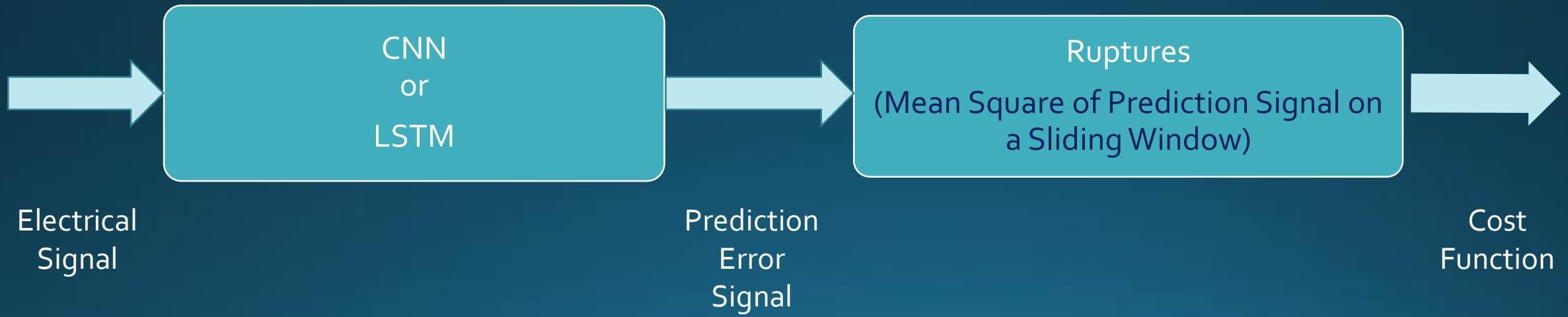


Multivariate Predictive Filter

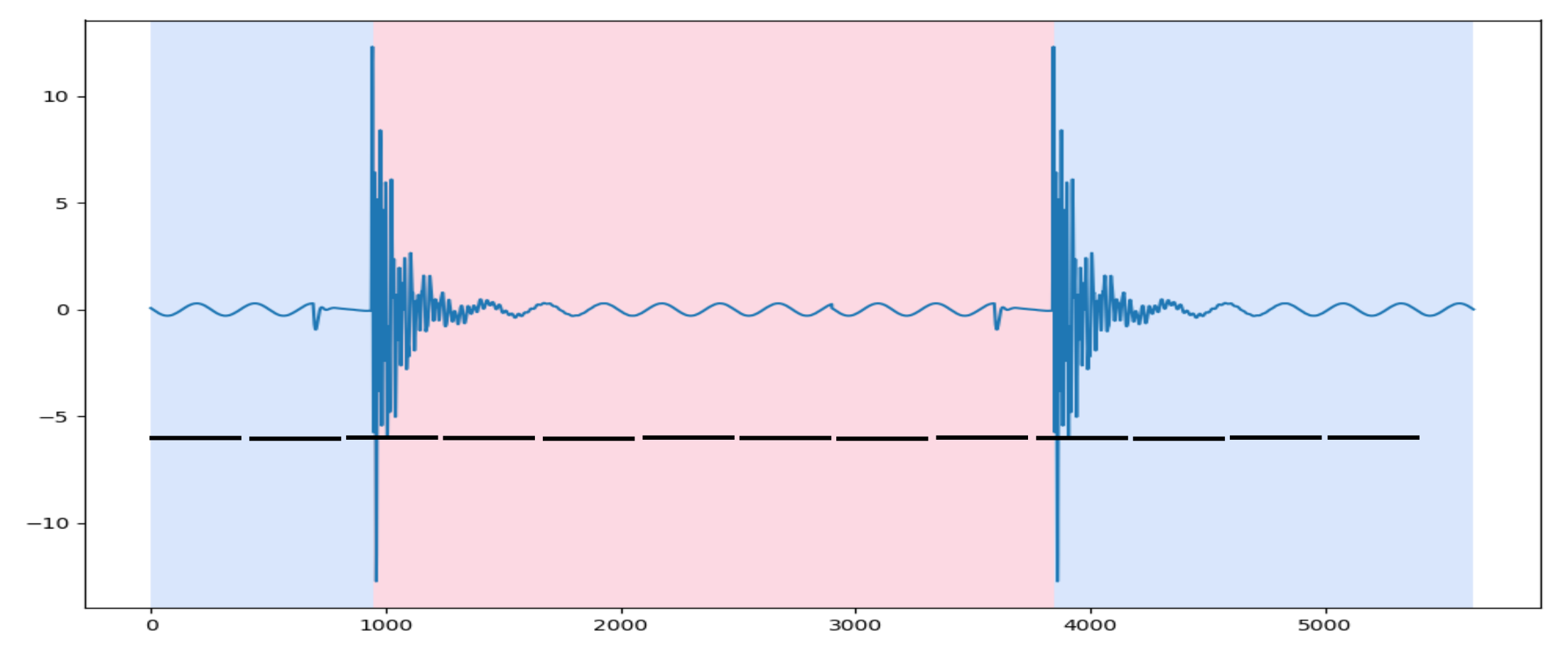


LSTM Predictive Filter

Suggested IDS



Suggested IDS



Overview

- Introduction to Smart Grids
- Distribution Domain
- Smart Grid Challenges
- Intrusion Detection System
- The Simulated System
- Suggested IDS
- **Results and Analysis**
- Conclusion

Results and Analysis

The following tables will show the False Accept (FA) vs. the False Reject (FR) for:

Known Points	Unknown Points (epsilon=0)	Unknown Points (epsilon=5)	Unknown Points of Glitches LSTM	Unknown Points of Glitches Multivariate	Unknown Points of Glitches LSTM Epsilon Variation	Unknown Points of Glitches Multivariate Epsilon Variation

They have been tried on over 40 simulations and the Hausdroff distance have been calculated along with the FA and the FR.

Known Points

		FA (%)	FR (%)
AR Order 4	Current	18.24	18.24
	Power	28.33	28.33
	Voltage	37.37	37.37
Gaussian Process Change	Current	33.33	33.33
	Power	49.88	49.88
	Voltage	54.14	54.14
Least Absolute Deviation	Current	16.04	16.04
	Power	16.40	16.40
	Voltage	14.43	14.43
Least Squared Deviation	Current	20.68	20.68
	Power	20.33	20.33
	Voltage	17.83	17.83
Linear Model Change	Current	11.04	11.04
	Power	21.16	21.16
	Voltage	12.29	12.29

		FA (%)	FR (%)
AR Order 4	Current	18.24	18.24
	Power	28.33	28.33
	Voltage	37.37	37.37
AR Order 10	Current	10	10
	Power	9.04	9.04
	Voltage	10.71	10.71

Unknown Points (Epsilon=0 and Epsilon=5)

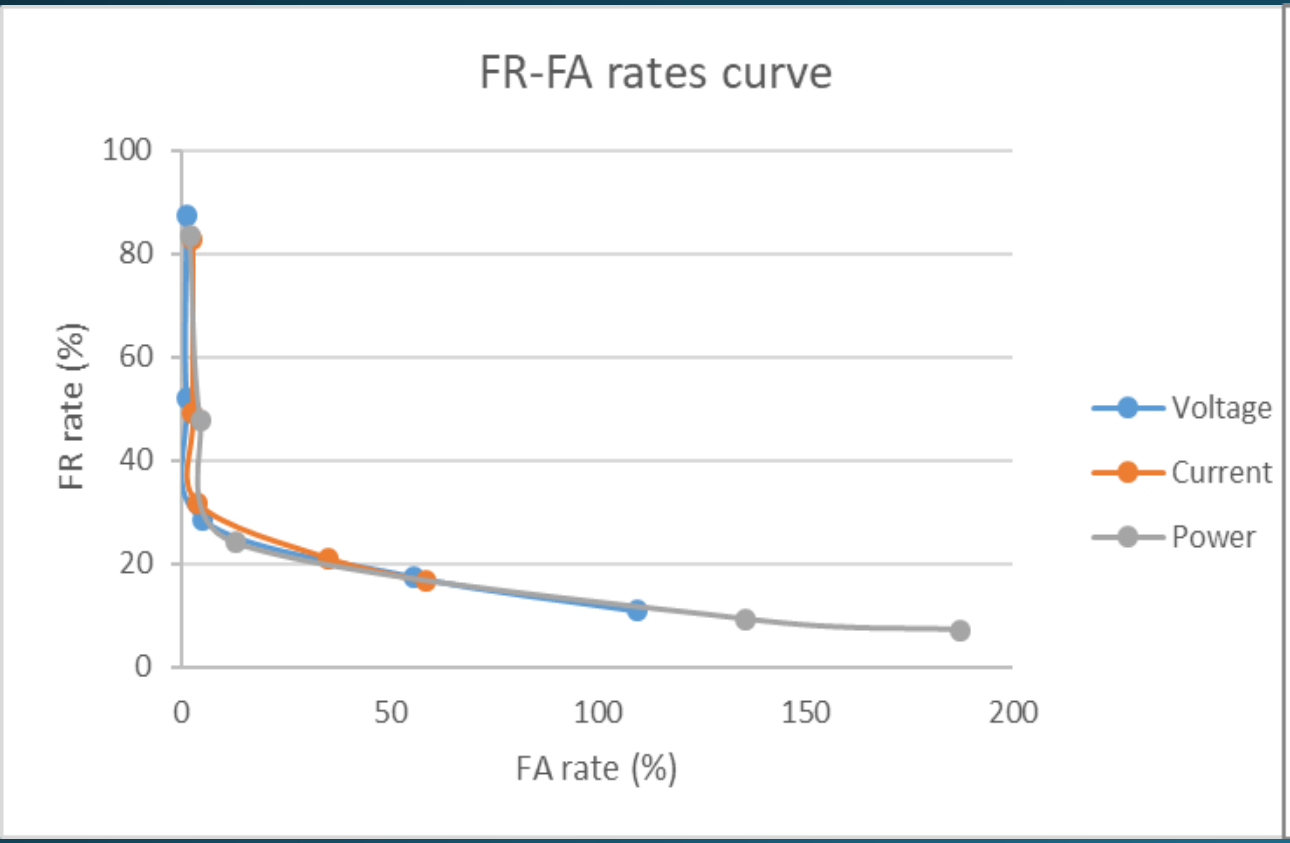
		FA (%)	FR (%)
AR Order 4	Current	25557.30	0
	Power	20377.67	0
	Voltage	19819.06	0
Least Absolute Deviation	Current	8063.17	290.36
	Power	8861.98	0
	Voltage	11433.17	0
Least Squared Deviation	Current	6851.54	0
	Power	7695.77	0
	Voltage	8374.67	0
Linear Model Change	Current	9195.32	37.5
	Power	16865.10	0
	Voltage	21716.36	22.5

Unknown Points of Glitches LSTM and Multivariate (Epsilon=0)

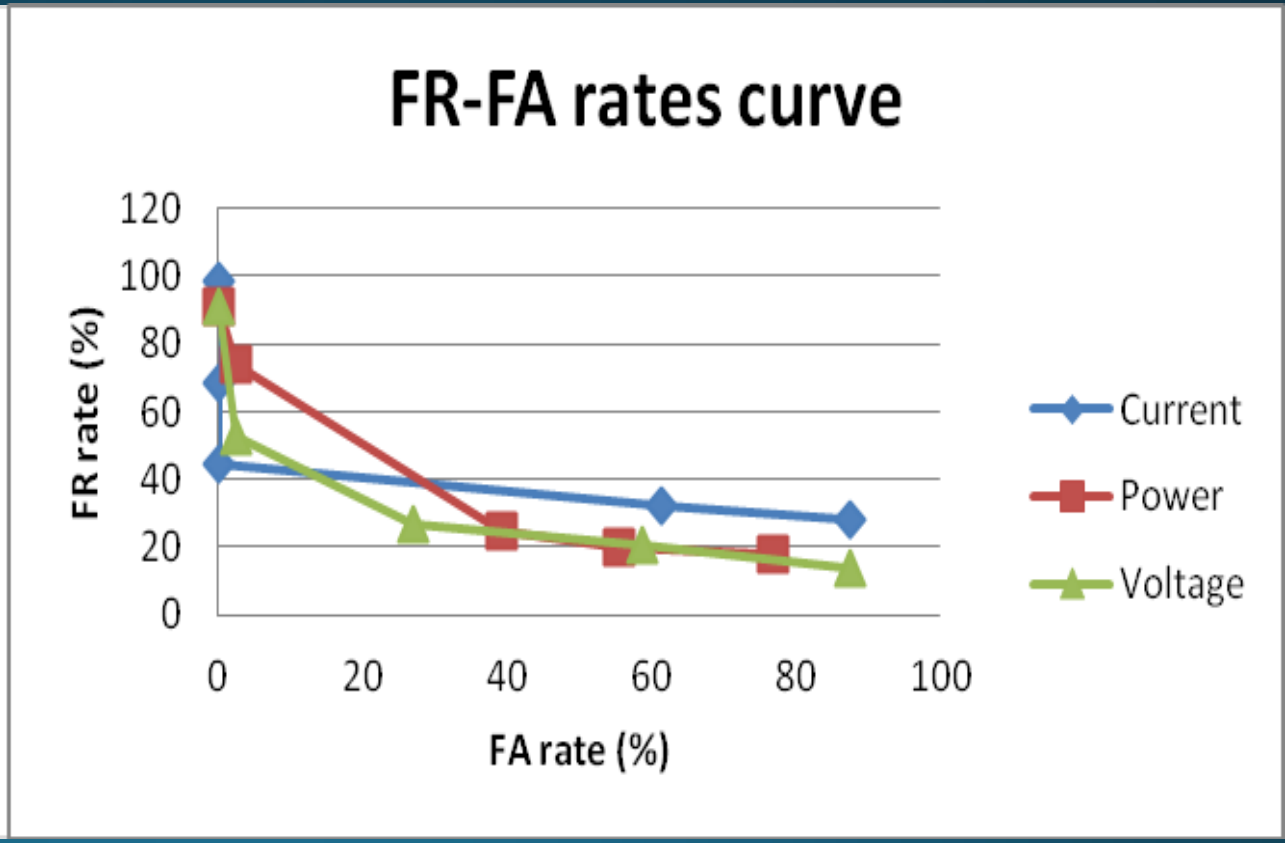
LSTM		FA (%)	FR (%)
AR Order 4	Current	263.11	3.4
	Power	189.23	5.46
	Voltage	190.82	6.98
Least Absolute Deviation	Current	234.61	1.03
	Power	297.20	3.05
	Voltage	256.15	0.313
Least Squared Deviation	Current	391.13	0.67
	Power	285.20	4.83
	Voltage	455.57	0.67
Custom Cost	Current	430.15	3.27
	Power	268.57	3.76
	Voltage	414.78	3.27
Normalized Custom Cost	Current	388.79	1.74
	Power	244.02	4.98
	Voltage	438.90	1.71
AR Order 10	Current	209.38	4.03
	Power	226.90	4.48
	Voltage	228.29	3.76

MSTM		FA(%)	FR(%)
AR Order 4	Current	234.17	4.74
	Power	165.72	6.23
	Voltage	267.07	5.5
Least Absolute Deviation	Current	217.39	4.07
	Power	263.01	4.12
	Voltage	328.85	4.12
Least Squared Deviation	Current	344.23	3.72
	Power	278.18	4.48
	Voltage	344.11	5.15
Custom Cost	Current	397.03	5.7
	Power	231.03	4.74
	Voltage	420.12	2.24
Normalized Custom Cost	Current	281.18	2.38
	Power	247.42	4.48
	Voltage	374.49	4.07

Unknown Points of Glitches LSTM and Multivariate Epsilon Variation



LSTM



Multivariate

Overview

- Introduction to Smart Grids
- Distribution Domain
- Smart Grid Challenges
- Intrusion Detection System
- The Simulated System
- Suggested IDS
- Results and Analysis
- **Conclusion**

Conclusions

- Intrusion Detection at the Distribution Domain is feasible
- The ability to try to identify the rupture (change in the signal properties) through glitches in the electrical signal
- Ruptures were generated through a co-simulation model in order to experiment and validate the results and efficiency of the newly proposed approach
- **Normalize the square root of the square sum** turned out to be the best after applying the LSTM method.
  - Lowest results at threshold 0.07
    - 5.19% FA and 28.49% FR
- The presented model needs to be studied practically before trying to apply it to the system for better precision and more accuracy.

Contributions

- A new simulation model
- Newly introduced models
- Deep nonlinear LSTM-based method is a viable solution to consider for intrusion detection for distribution domain in smart grid.

Thank you!