A Computational Intelligence System for Identification Cyber-Attacks on Smart Energy Grids

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

Democritus University of Thrace
Dep. of Forestry & Management of the Environment & Natural Resources
Lab of Forest-Environmental Informatics & Computational Intelligence

Konstantinos Demertzis – Lazaros Iliadis

Cryptography, Cybersecurity & Information Warfare…

What Is the Smart Grid?

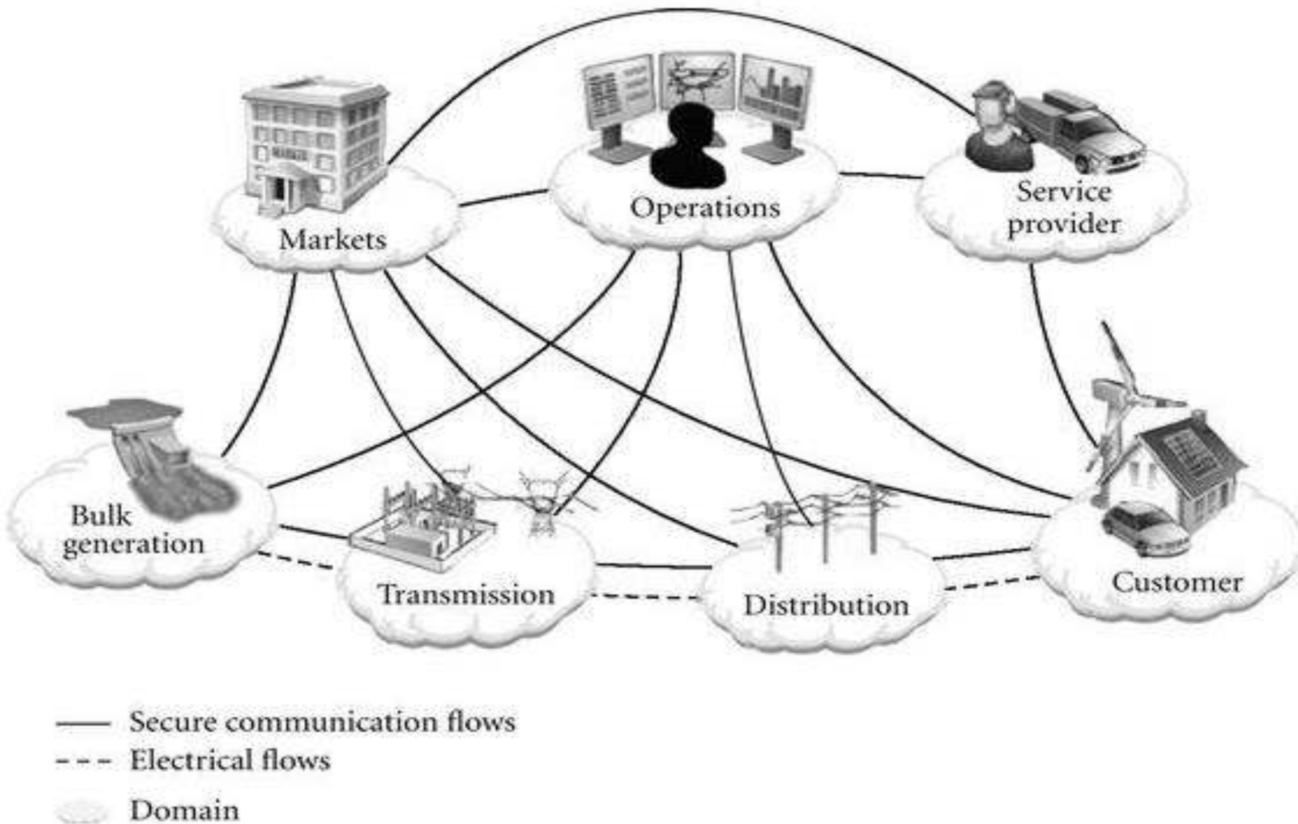
- ✓ A smart grid is an energy transmission and distribution network enhanced through digital control, monitoring and telecommunications capabilities.
- ✓ It provides a real-time, two-way flow of energy and information to all stakeholders in the electricity chain, from the generation plant to the commercial, industrial and residential end user.

Smart Grid Architecture

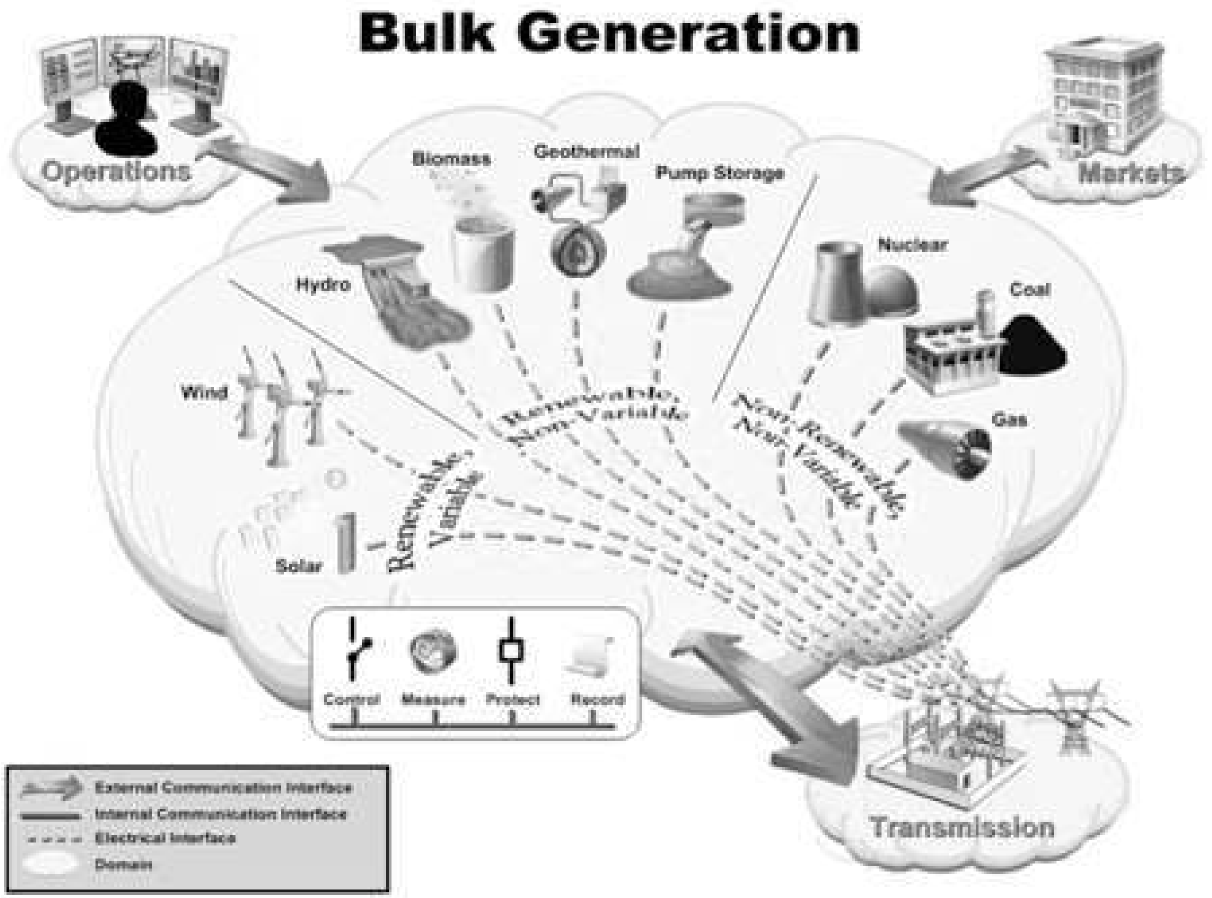
- ✓ Smart grid layers require a system of systems approach with differentiated security needs.
- ✓ The smart grid includes different domains (***Smart Grid Conceptual Model***):
  1. ***Bulk generation***
  2. ***Transmission***
  3. ***Distribution***
  4. ***Markets***
  5. ***Operations***
  6. ***Service Provider***
  7. ***Customer - Distributed energy resources - Electric Vehicles***

Smart Grid Conceptual Model

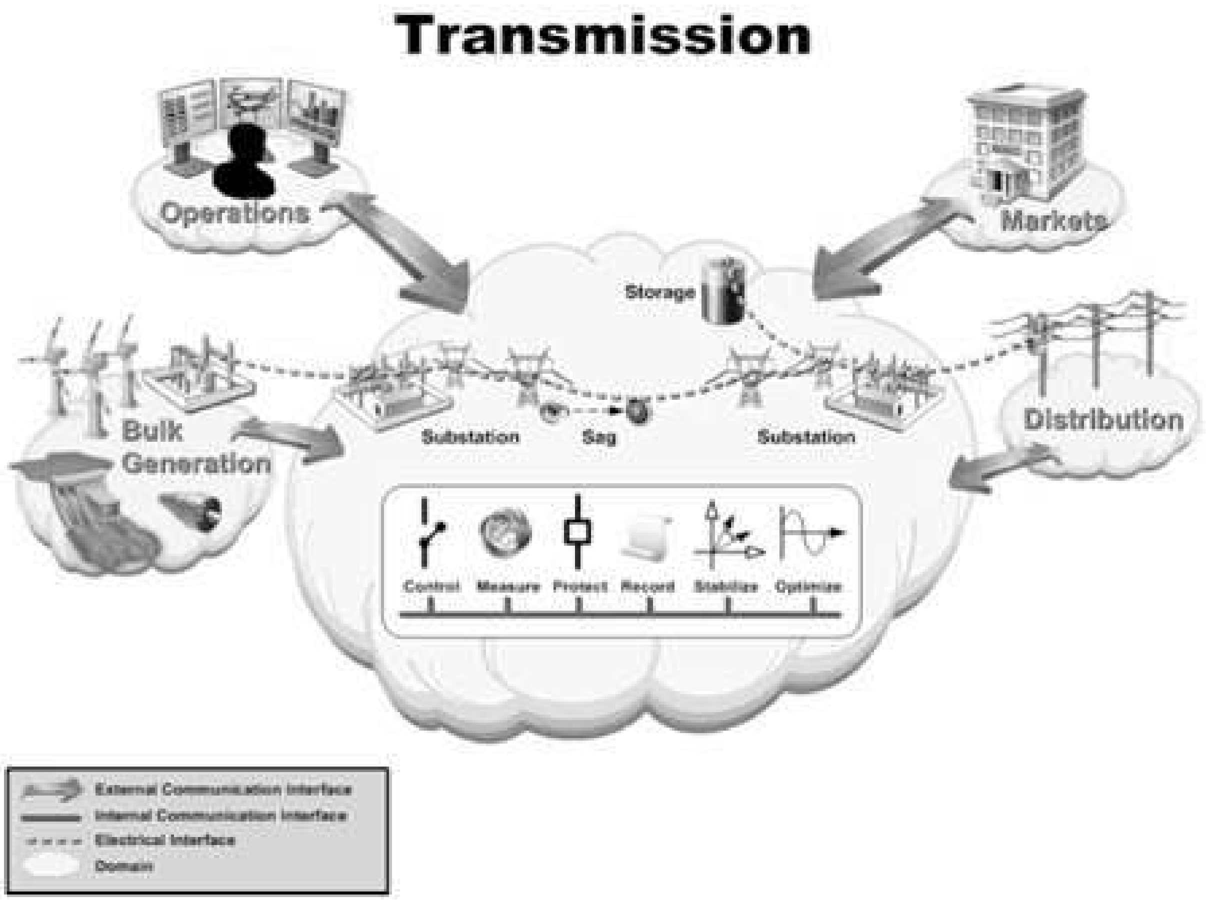
- ✓ It relies on a multitude of stakeholders, each with its own specific role and activity within a given domain.



Smart Grid Conceptual Model

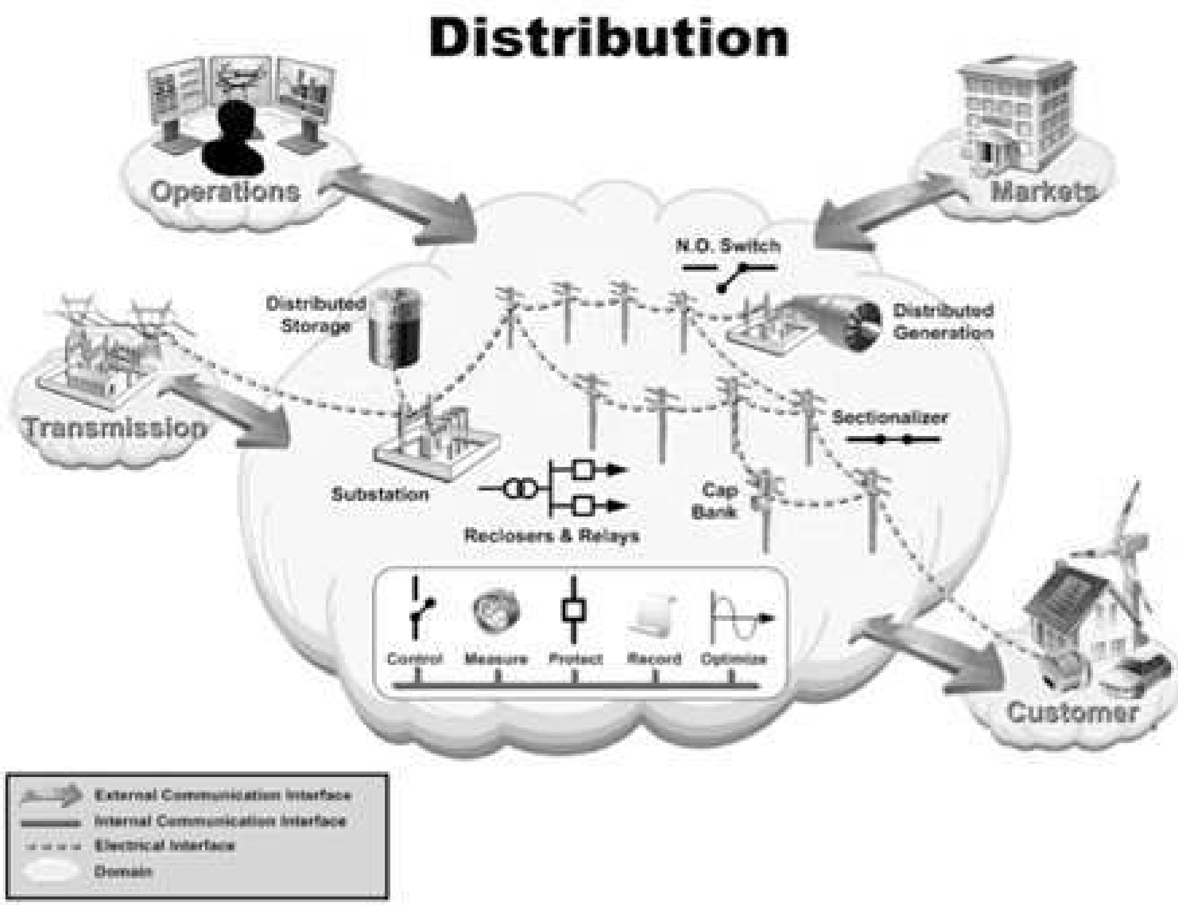


Smart Grid Conceptual Model



FI-Lab

Smart Grid Conceptual Model



IT infrastructures of Smart Grid

- ✓ Information and communication infrastructures will play an important role in connecting and optimizing the available grid layers.
- ✓ Grid operation depends on control systems called **S**upervisory **C**ontrol and **D**ata **A**cquisition (**SCADA**) that monitor and control the physical infrastructure.
- ✓ At the heart of these SCADA systems are specialized computers known as **P**rogrammable **L**ogic **C**ontrollers (**PLCs**).

Smart Grid Cyber Security Specificities

- ✓ An important aspect of cyber security for critical infrastructure protection focuses on a basic understanding and awareness of real-world threats and vulnerabilities that exist within the industrial automation and control system architectures used in most process industries and manufacturing facilities.
- ✓ **As a large system of distributed and interconnected systems, the smart grid offers an exceptionally large attack surface**.
- ✓ Every asset of the smart grid is a potential target for a cyber attack.

Smart Grid Cyber Security Specificities

- ✓ An attack over a critical node may jeopardize the grid security and lead a cascade effect to a whole system blackout.
- ✓ The smart grid cyber security challenge is about protecting the ever-growing number of smart grid assets and their communication channels from fast-growing and continuously evolving cyber threats.

Smart Grid Cyber Security Specificities

- ✓ These issues face the SCADA Systems and Distribution Control Systems (DCS) that comprise most industrial environments, and impact not on the common IT infrastructure like Windows-based computers and network appliances (switches, routers and firewalls), but also embedded "proprietary" equipment such as programmable logic controllers (PLC), remote terminal units (RTU), intelligent electrical device (IED), basic process controllers (BPCS), safety instrumented systems (SIS), operator panels, and ancillary systems that are the basis of most integrated ICS architectures.

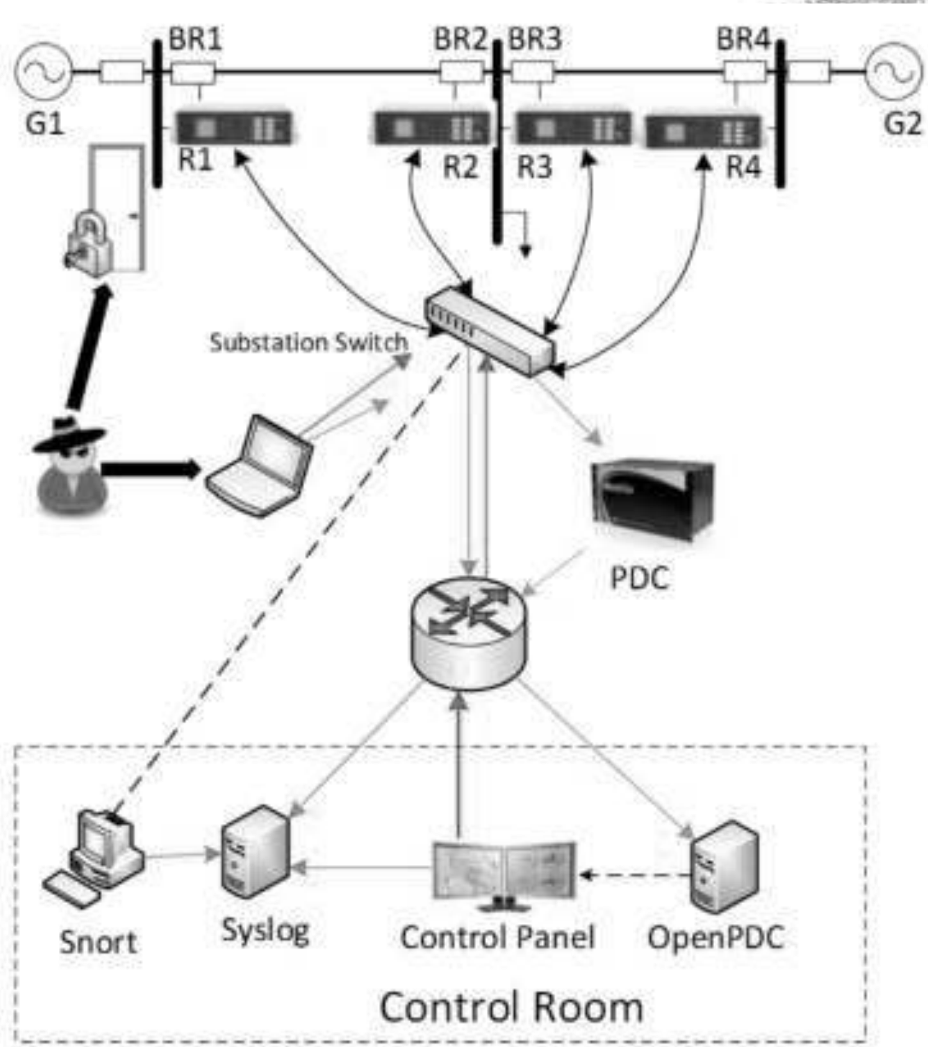
Smart Grid Cyber Security Specificities

✓ There are destructive cyber-attacks against SCADA systems as **Advanced Persistent Threats** (**APT**), were able to take over the PLCs controlling the centrifuges, reprogramming them in order to speed up the centrifuges, leading to the destruction of many and yet displaying a normal operating speed in order to trick the centrifuge operators and finally can not only shut things down but can alter their function and permanently damage industrial equipment.

Smart Grid Attack Dataset

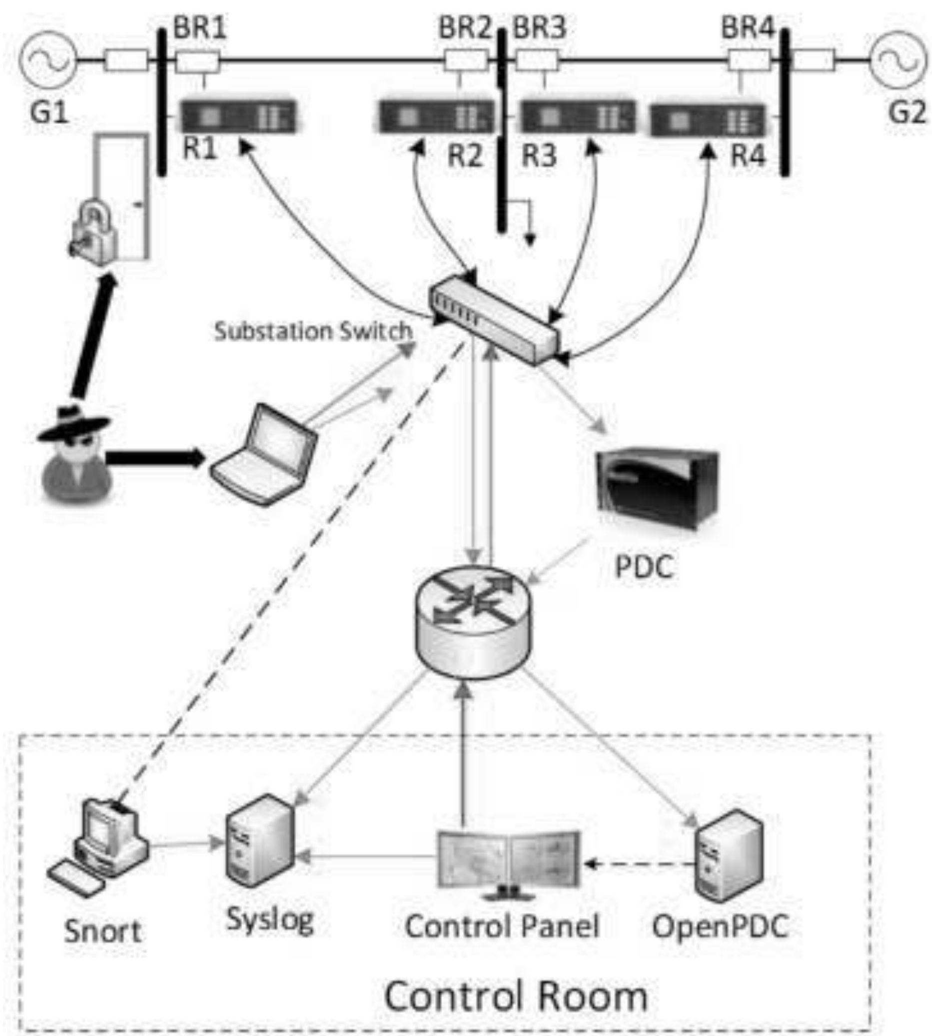
✓ The figure shows the power system framework configuration used in generating the attack scenarios.

Mississippi State University and
Oak Ridge National Laboratory



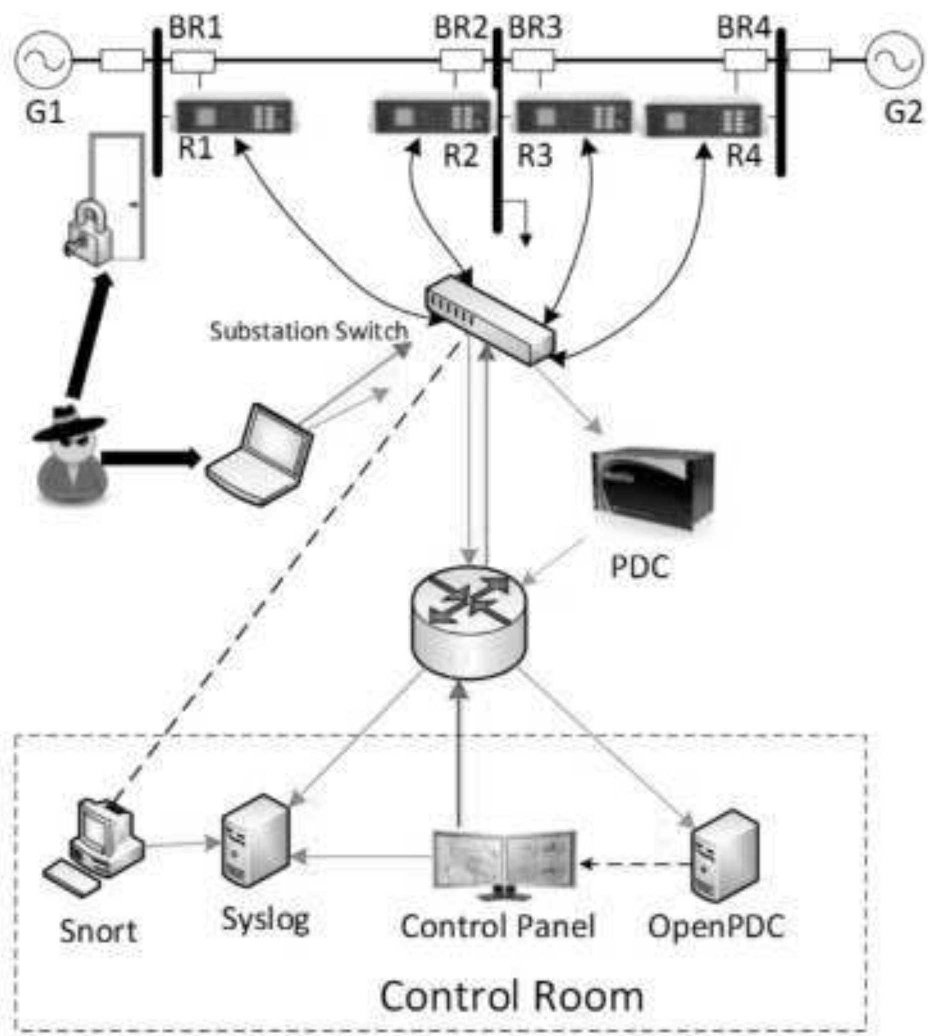
Smart Grid Attack Dataset

- ✓ In the network diagram G1 and G2 are power generators, R1 through R4 are Intelligent Electronic Devices (IEDs) that can switch the breakers on or off.
- ✓ These breakers are labeled BR1 through BR4.



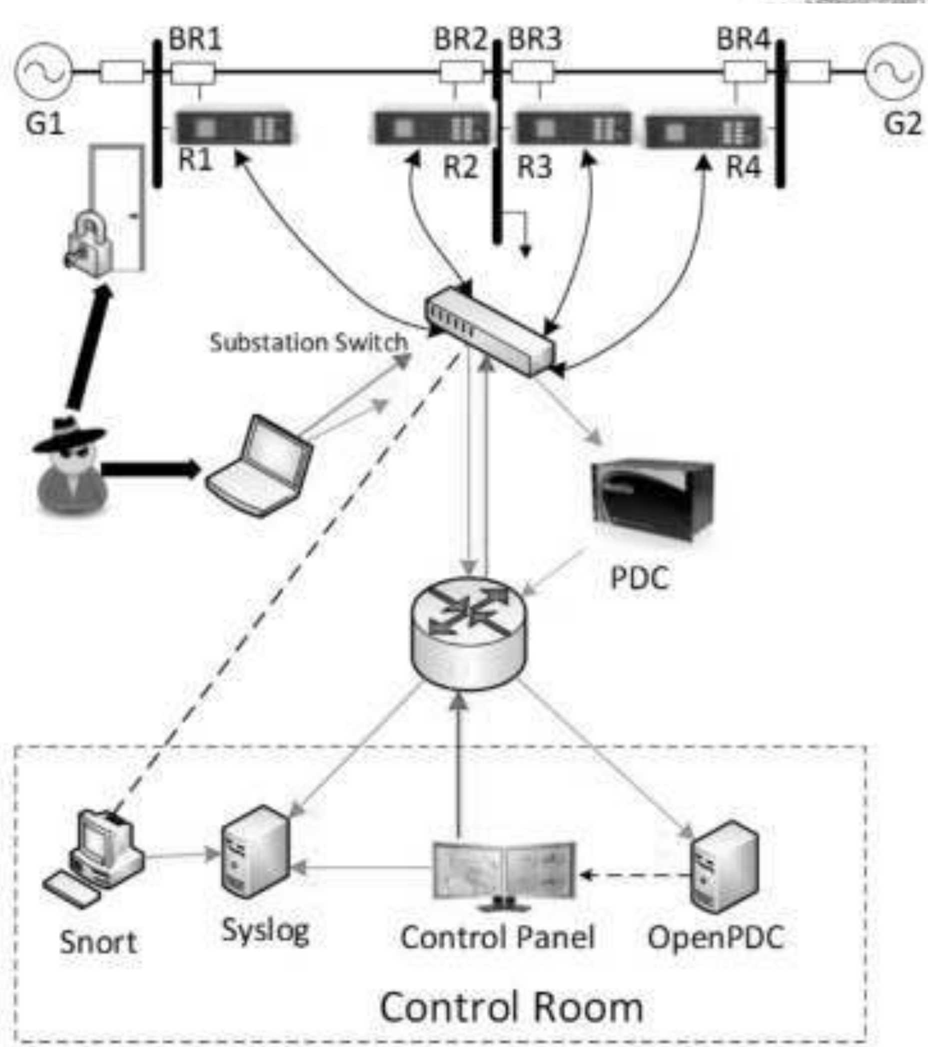
Smart Grid Attack Dataset

- ✓ We also have two lines. Line One spans from breaker one (BR1) to breaker two (BR2) and Line Two spans from breaker three (BR3) to breaker four (BR4).
- ✓ Each IED automatically controls one breaker. R1 controls BR1, R2 controls BR2 and son on.



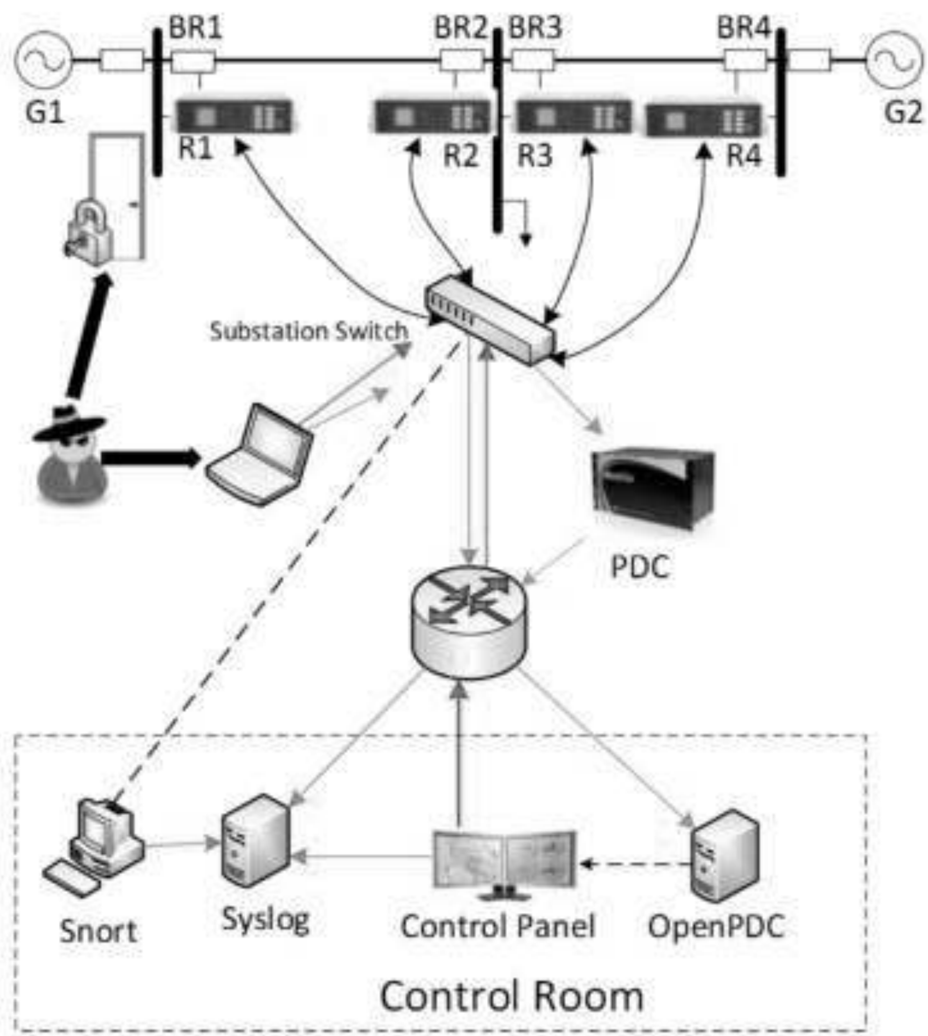
Smart Grid Attack Dataset

- ✓ The IEDs use a distance protection scheme which trips the breaker on detected faults whether actually valid or faked since they have no internal validation to detect the difference.



Smart Grid Attack Dataset

- ✓ Operators can also manually issue commands to the IEDs R1 through R4 to manually trip the breakers BR1 - BR4.
- ✓ The manual override is used when performing maintenance on the lines or other system components.



Smart Grid Attack Dataset

✓ The dataset comprised of 128 independent variables and 3 classes - markers (***No Events, Normal Events, Attack***).

Feature	Description
PA1:VH – PA3:VH	Phase A - C Voltage Phase Angle
PM1: V – PM3: V	Phase A - C Voltage Phase Magnitude
PA4:IH – PA6:IH	Phase A - C Current Phase Angle
PM4: I – PM6: I	Phase A - C Current Phase Magnitude
PA7:VH – PA9:VH	Pos. – Neg. – Zero Voltage Phase Angle
PM7: V – PM9: V	Pos. – Neg. – Zero Voltage Phase Magnitude
PA10:VH - PA12:VH	Pos. – Neg. – Zero Current Phase Angle
PM10: V - PM12: V	Pos. – Neg. – Zero Current Phase Magnitude
F	Frequency for relays
DF	Frequency Delta (dF/dt) for relays
PA:Z	Appearance Impedance for relays
PA:ZH	Appearance Impedance Angle for relays
S	Status Flag for relays

Smart Grid Attack Dataset

- ✓ 128 features are extracted
  - ✓ there are 116 measurements from phasor measurement units (PMU). A PMU or synchrophasor is a device which measures the electrical waves on an electricity grid, using a common time source for synchronization.
  - ✓ 4 features for control panel logs
  - ✓ 4 features for relay logs
  - ✓ 4 features for Snort alerts logs
- ✓ Marker

Smart Grid Attack Dataset

✓ Types of Scenarios (classes - markers):

- **No Events**
- **Short-circuit fault (Normal Events)** – this is a short in a power line and can occur in various locations along the line, the location is indicated by the percentage range.
- **Line maintenance (Normal Events)** – one or more relays are disabled on a specific line to do maintenance for that line.

Smart Grid Attack Dataset

✓ Types of Scenarios:

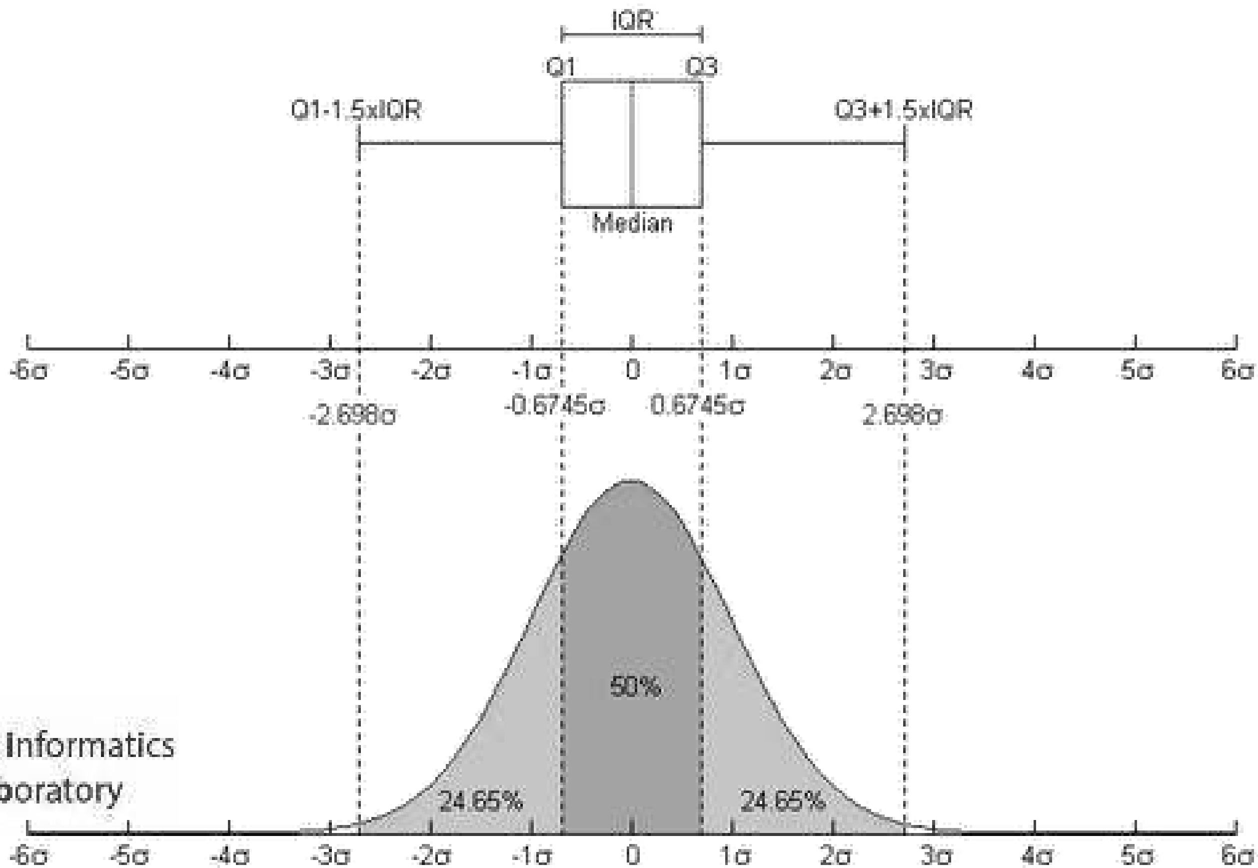
- **Remote tripping command injection (Attack)** – this is an attack that sends a command to a relay which causes a breaker to open. It can only be done once.
- **Relay setting change (Attack)** – relays are configured with a distance protection scheme and the attacker changes the setting to disable the relay function such that relay will not trip for a valid fault or a valid command.
- **Data Injection (Attack)** – here we imitate a valid fault by changing values to parameters such as current, voltage, sequence components etc. This attack aims to blind the operator and causes a black out.

Smart Grid Attack Dataset

- ✓ **Preprocessing**
  - ✓ Dataset is determined and normalized to the interval [-1,1] in order to phase the problem of prevalence of features with wider range over the ones with a narrower range, without being more important.
  - ✓ The outliers and the extreme values spotted were removed based on the **Inter Quartile Range technique**.

Smart Grid Attack Dataset

✓ Inter Quartile Range technique



Smart Grid Attack Dataset

- ✓ The final dataset containing **159,045** patterns:
  - ✓ 48,455 **No Events**,
  - ✓ 54,927 **Natural** and
  - ✓ 55,663 **Attack**

Methodologies

- ✓ **Extreme Learning Machines (ELM)**
  - ✓ an emerging learning technique provides efficient unified solutions to generalized feed-forward networks,
  - ✓ theories show that hidden neurons are important but can be randomly generated, independent from applications and that ELMs have both universal approximation and classification capabilities, build a direct link between theories namely:
    - ✓ ridge regression (for non-linear least squares problems),
    - ✓ ANN generalization performance,
    - ✓ linear system stability and
    - ✓ matrix theory,

Methodologies

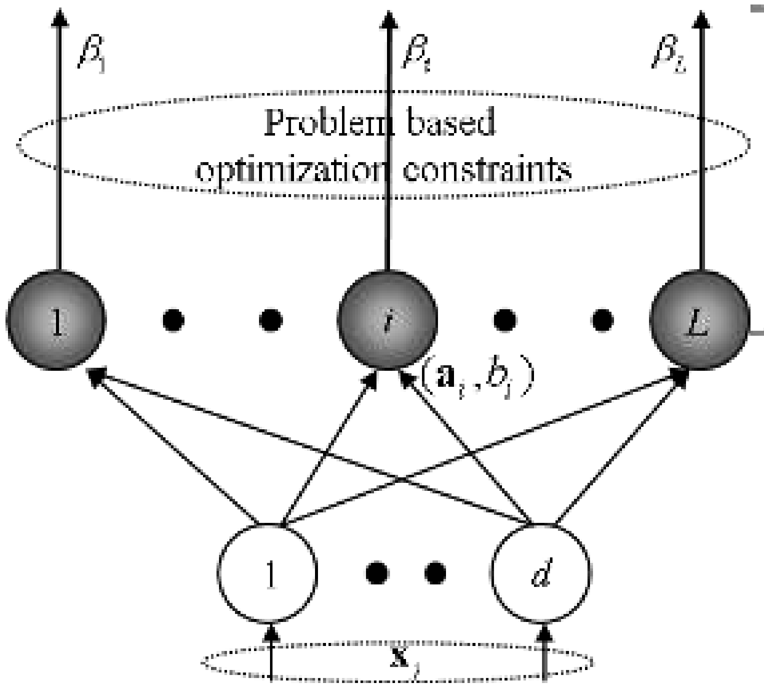
- ✓ **Extreme Learning Machines (ELM)**
  - ✓ works for the "generalized" Single-hidden Layer feedforward Networks (SLFNs) but the hidden layer (or called feature mapping) need not be tuned,
  - ✓ learning theory shows that the hidden nodes/neurons of generalized feedforward networks needn't be tuned and these hidden nodes/neurons can be randomly generated,
  - ✓ all the hidden node parameters are independent from the target functions or the training datasets,
  - ✓ the hidden node/neuron parameters are not only independent of the training data but also of each other,

Methodologies

- ✓ **Extreme Learning Machines (ELM)**
  - ✓ can handle non-differentiable activation functions, and do not have issues such as finding a suitable stopping criterion, learning rate, and learning epochs.
  - ✓ Advantages:
    - ✓ ease of use, **faster learning speed**, higher generalization performance,
    - ✓ suitable for many nonlinear activation function or kernel functions

Methodologies

✓ Extreme Learning Machines (ELM)



Feature learning
Clustering
Regression
Classification

L Random Hidden Neurons (which need not be algebraic sum based) or other ELM feature mappings. Different type of output functions could be used in different neurons:

$$h_i(\mathbf{x}) = G_i(\mathbf{a}_i, b_i, \mathbf{x})$$

d Input Nodes

SICASEG

- ✓ **A Computational Intelligence System for Identification Cyber-Attacks on Smart Energy Grids**
  - ✓ we propose a novel system that use a **Self-adaptive Evolutionary Extreme Learning Machine** (**SaE-ELM**).
  - ✓ In SaE-ELM, the hidden node learning parameters are optimized by the **Self-adaptive Differential Evolution Algorithm** (**SaDEA**), whose trial vector generation strategies and their associated control parameters are self-adapted in a strategy pool by learning from their previous experiences in generating promising solutions, and the network output weights are calculated using the **Moore–Penrose** (**MP**) generalized inverse.

Results

- ✓ To identify the integrity of SICASEG we have compared the SaE-ELM with other neural network methods such as:
  - ✓ Radial Basis Function (RBF) ANN,
  - ✓ Group Methods of Data Handling (GMDH)
  - ✓ Polynomial ANN (PANN) and
  - ✓ Feed Forward Neural Networks (FNN) trained under Genetic Algorithm (GA)
- ✓ The results showed that the SaE-ELM has much faster learning speed (run thousands times faster than conventional methods) and has much better generalization performance and more accurate and reliable classification results.

Results

✓ Confusion Matrix:

No Events	Natural	Attack	
48318	98	39	**No Events**
74	52645	2208	**Natural**
118	2950	52595	**Attack**

Results

- ✓ The performance comparisons of algorithms:

Classifier	Classification Accuracy & Performance Metrics						
	ACC	RMSE	Precision	Recall	F-Score	ROC Area	Validation
SaE-ELM	**96.55%**	**0.1637**	**0.966%**	**0.966**	**0.965%**	**0.996**	10-fcv
RBF ANN	90.60%	0.2463	0,909%	0.907	0.907%	0.905	10-fcv
GMDH	92.66%	0.1828	0.927%	0.927	0.927%	0.980	10-fcv
PANN	91.34%	0.2162	0.914%	0.913	0.914%	0.961	10-fcv
FNN-GA	94.71%	0.2054	0.947%	0.947	0.947%	0.969	10-fcv

Future Directions

- ✓ feature minimization using **Principal Component Analysis** (**PCA**) or other existing approaches,
- ✓ additional computational intelligence methods such as **Spiking Neural Networks** could be explored and compared on the same security task and
- ✓ scalability of ELM with **Hadoop Distributed File System** (**HDFS**).

Conclusions

- ✓ An innovative Computational Intelligence System for Identification Cyber-Attacks on SEGs has been introduced.
- ✓ It performs classification by using a Self-adaptive Evolutionary ELM, a very fast approach to properly classify cyber attacks with high accuracy and generalization with minimum computational power and resources.
- ✓ This is done to enhance the energetic security and the mechanisms of reaction of the general system, without special requirements.
- ✓ In this way it adds a higher degree of integrity to the rest of the security infrastructure of SEGs.

No System is Safe

References

[1] Chi Cheng, Wee Peng Tay, Guang-Bin Huang, Extreme learning machines for intrusion detection, Neural Networks (IJCNN), International Joint Conference, DOI: 10.1109/IJCNN.2012.6252449, 2012.

[2] Erik Cambria, Guang-Bin Huang, Extreme Learning Machines, IEEE InTeLLIGenT SYSTemS, 541-1672/13, 2013.

[3] Jiuwen Cao, Zhiping Lin, Guang-Bin Huang, Self-Adaptive Evolutionary Extreme Learning Machine, Neural Process Lett (2012) 36:285–305, DOI 10.1007/s11063-012-9236-y.

[4] Yves Aillerie, Said Kayal, Jean-Pierre Mennella, Raj Samani, Sylvain Sauty, Laurent Schmitt, Smart Grid Deployment Requires a New End-to-End Security Approach, White Paper - Cyber Security, Intel Corp, 2015.

[5] Mete Ozay, Inaki Esnaola, Fatos T. Yarman Vural, Sanjeev R. Kulkarni, H. Vincent Poor, Machine Learning Methods for Attack Detection in the Smart Grid, IEEE Transactions on Neural Networks and Learning Systems, 2015, DOI: 10.1109/TNNLS.2015.2404803.

Thanks

kdemertz@fmenr.duth.gr
http://utopia.duth.gr/~kdemertz/