“From Honeypot-oriented Risk Analysis to Islanding Solutions in Energy Systems

Prof. Panagiotis Sarigiannidis

University of Western Macedonia

psarigiannidis@uowm.gr

Introduction

SDN-μSense

Summary

In the era of hyper-connected digital economies, the smart technologies play a vital role in the operation of the electrical grid, transforming it into a new paradigm called smart grid.

SCADA Systems

SCADA Systems utilise legacy industrial protocols such as Modbus, Profinet, IEC 61850, IEC104, DNP3, IEC-104 that are characterised by severe cybersecurity flaws since they do not integrate appropriate authentication and authorization mechanisms.

Internet of Things

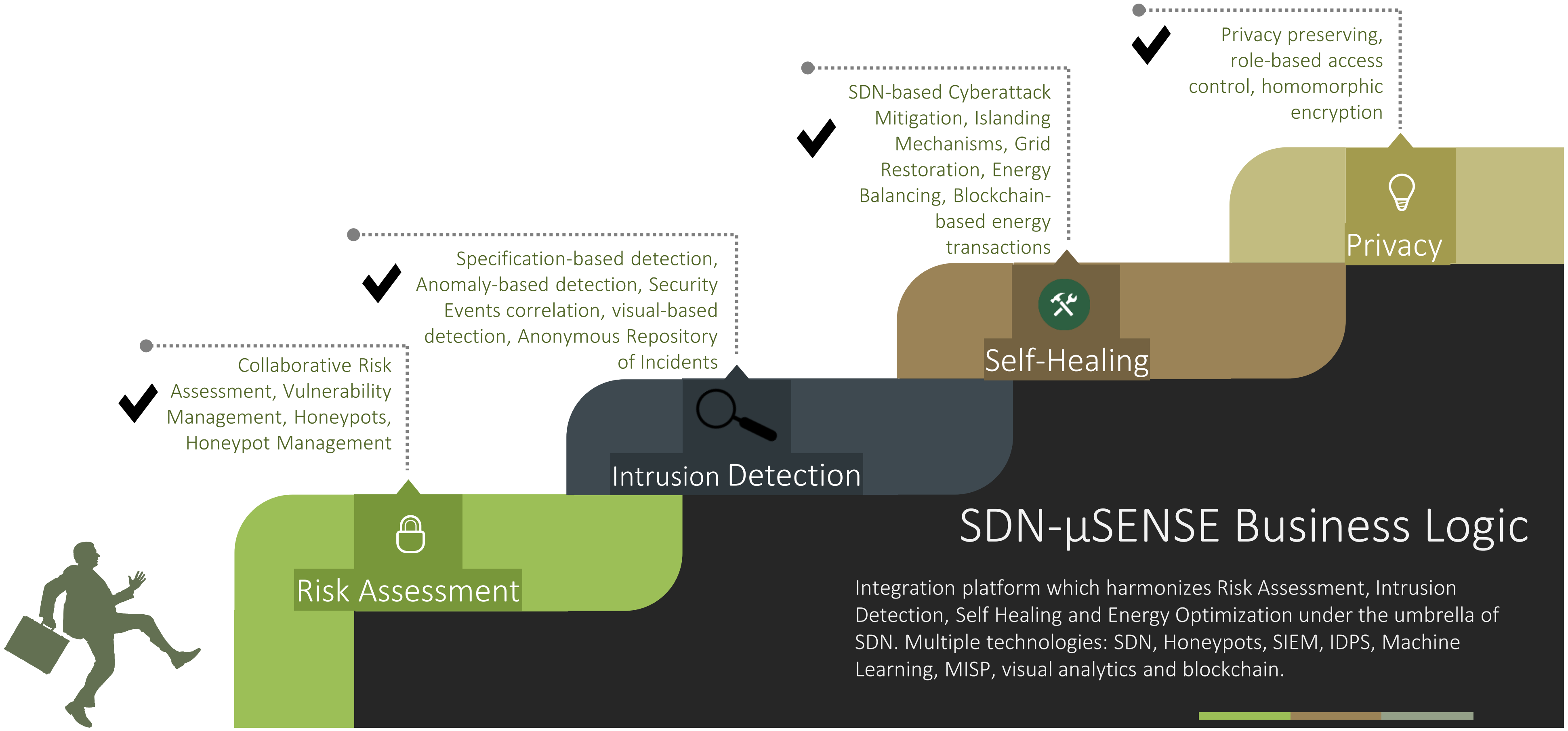
IoT generates crucial security concerns since it is based on Internet, which is insecure by its nature. Also, it combines novel technologies such as Wire-less Sensor Networks (WSNs) that bring the corresponding cybersecurity issues, such as sinkhole, sybil and wormhole cyberattacks.

Advanced Metering Infrastructure

AMI is composed of several networks (HAN, NAN, WAN) and components (smart meters, data collectors and AMI headend that constitute an attractive target for the cyberattackers). MiTM attacks, DoS, False Data Injection (FDI), ransomware, etc. are characteristic examples.

SDN-microSENSE Business Logic

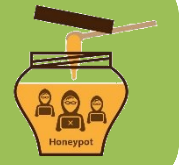
SDN-µSense



Honeypots

◆ Honeypots are defined as an information system resource whose value lies in unauthorized or illicit use of that resource.

01



02

◆ A honeypot is a computer system that is set up to act as a decoy to lure cyber-attackers, to detect and learn about new cyber threats and attack patterns and to improve the cyber security strategy of the organization.

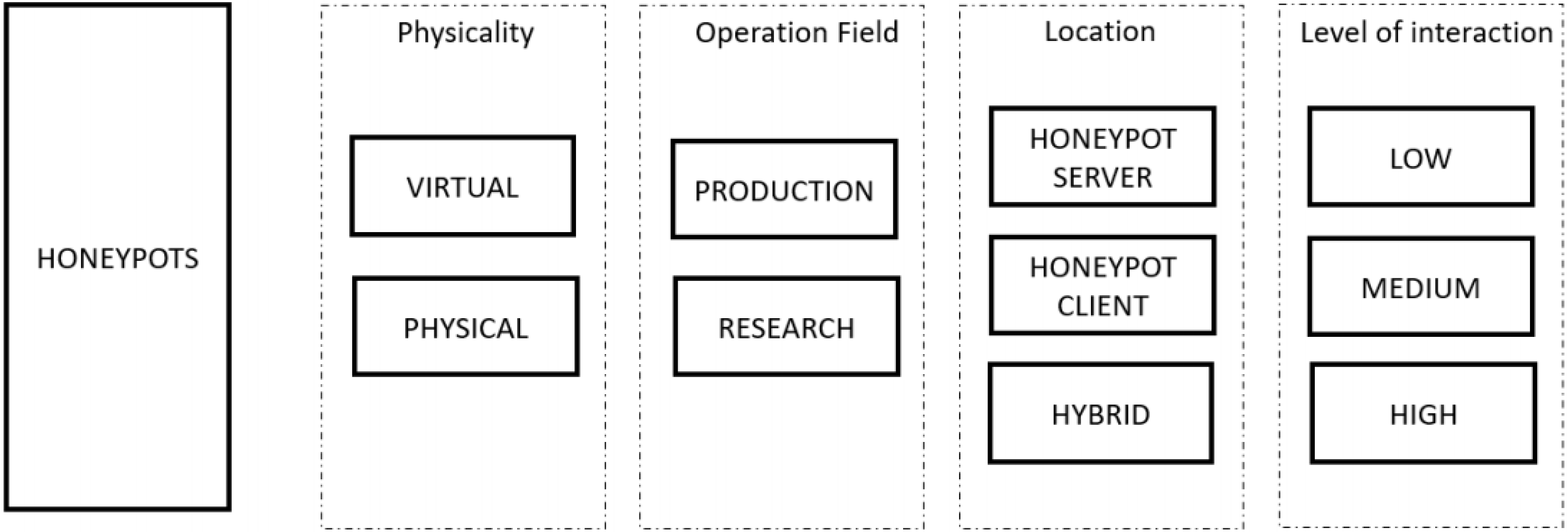
◆ Security personal often use honeypots as a tool to gather intelligent on the attacker. Attackers constantly modify their methods to take advantage of different types of attacks. If the security operator/administrator does not configure the honeypot properly, it might appear suspicious to an experienced attacker and simply avoid it.

03

04

◆ A honeypot supports the security team to understand the attacker's methodologies, learn more about known and unknown attacks and in this way to better protect the real production systems.

Honeypots Classification



Honeypots as a Risk Analysis Mechanism

SDN-μSense

Risk Assessment

Risk assessment is needed for each asset in the organization that requires protection; this assessment must answer the three key questions listed below.

- What assets do we need to protect?
- How are those assets threatened?
- What can we do to counter those threats?

Honeypots are defensive mechanisms that can hide and protect the real assets of the examined architecture. They work as **countermeasures** in a risk assessment process, aiming to (a) detect potential intrusions, b) mitigate them and (c) increase the threat intelligence.

Asset
Anything that has value to the organization

Threat
A potential cause of an unwanted incident which may result in harm to a system or organization

Vulnerability
A weakness in an asset or group of assets which can be exploited by a threat

Risk
The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

Honeypots in SDN-microSENSE

SDN-μSense

Three EPES Honeypots and Honeypot Manager

In the context of the SDN-microSENSE, the Electrical Power and Energy Systems (EPES) Honeypots & Honeypot Manager constitute part of the SDN-microSENSE Risk Assessment Framework (S-RAF). First, they aim to protect the EPES devices, by emulating their services based on the respective EPES protocols (Modbus, IEC104 and IEC 61850). Secondly, the Honeypot Manager re-directs potential, anomalous events to the EPES Honeypots in order to identify and collect more information about them (e.g., malicious patterns).

Modbus Honeypot

Emulate any device, which uses the Modbus/TCP protocol.

Honeypot Manager

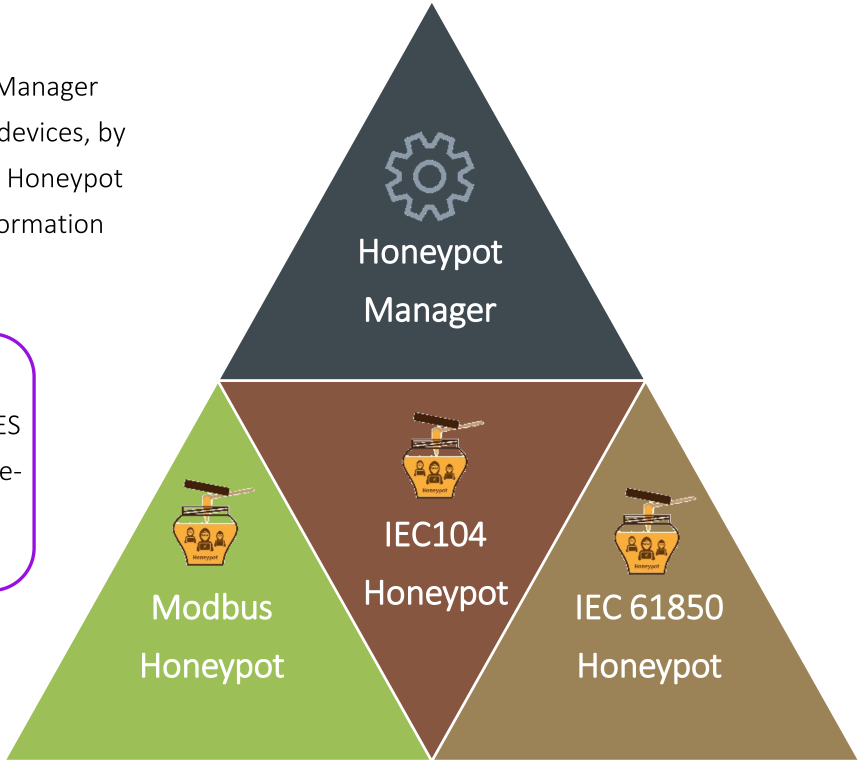
Deploy and handle the lifecycle of the EPES honeypots. Through the SDN-Controller re-directs malicious network traffic to EPES honeypots.

IEC104 Honeypot

Emulate any device, which uses the IEC60870-5-104 protocol

IEC 61850 Honeypot

Emulate any device which uses the IEC 61850 honeypot



Honeypot Manager

Management of EPES Honeypots' lifecycle

Honeypots as Virtual Machines

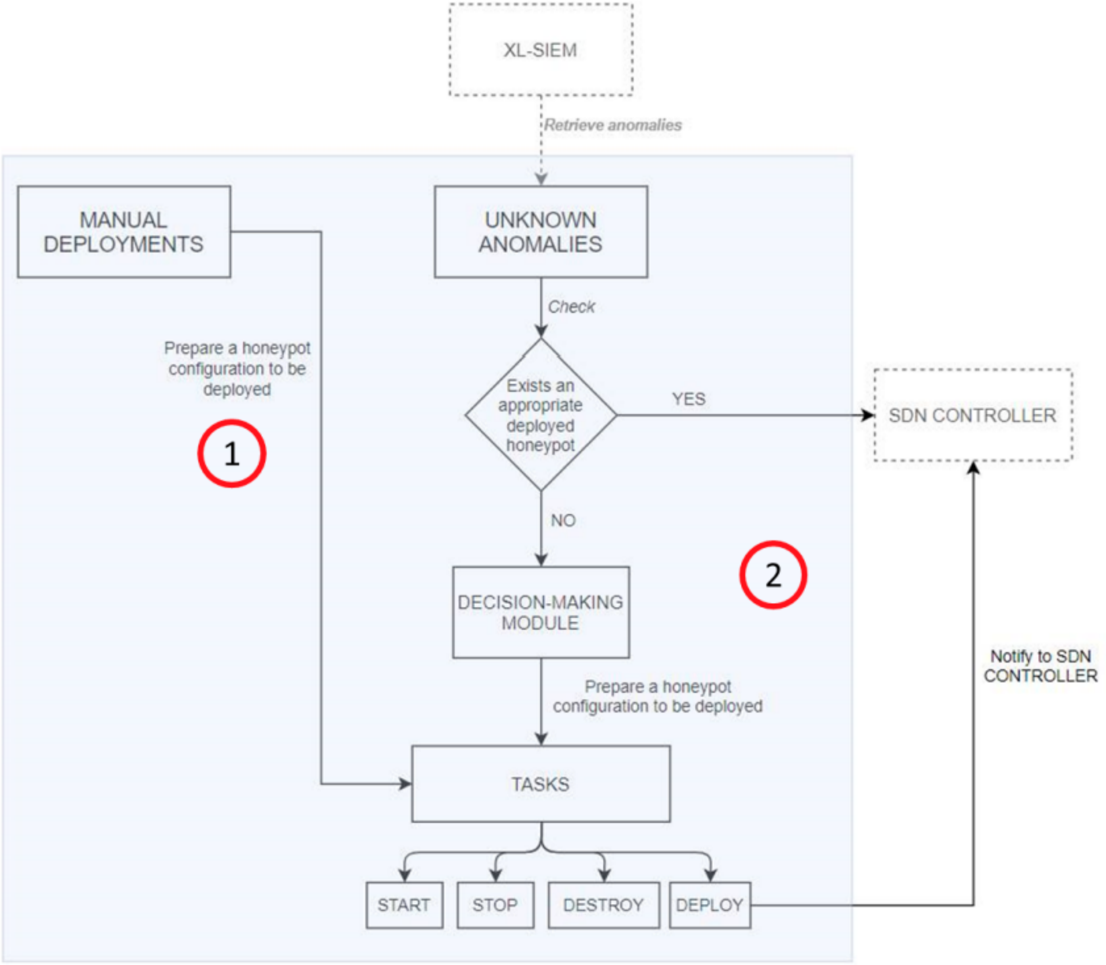
It handles the lifecycle of the virtual machines in which the honeypots will be deployed. (Each AMI honeypot deployed in separate VM).

Redirects Malicious Traffic to EPES Honeypots

The Honeypot Manager receives the unknown security events from the SDN-microSENSE detectors and thanks to the SDN Controller re-directs the respective, malicious network traffic to the respective EPES Honeypots in order to collect more data regarding the specific security events.

EPES Honeypots' Security Events

The EPES honeypots generate new informative security events based on the interaction with the cyberattacker



Modbus Honeypot

SDN-μSense

A DNN Modbus Honeypot

Emulating both server and client Modbus entities

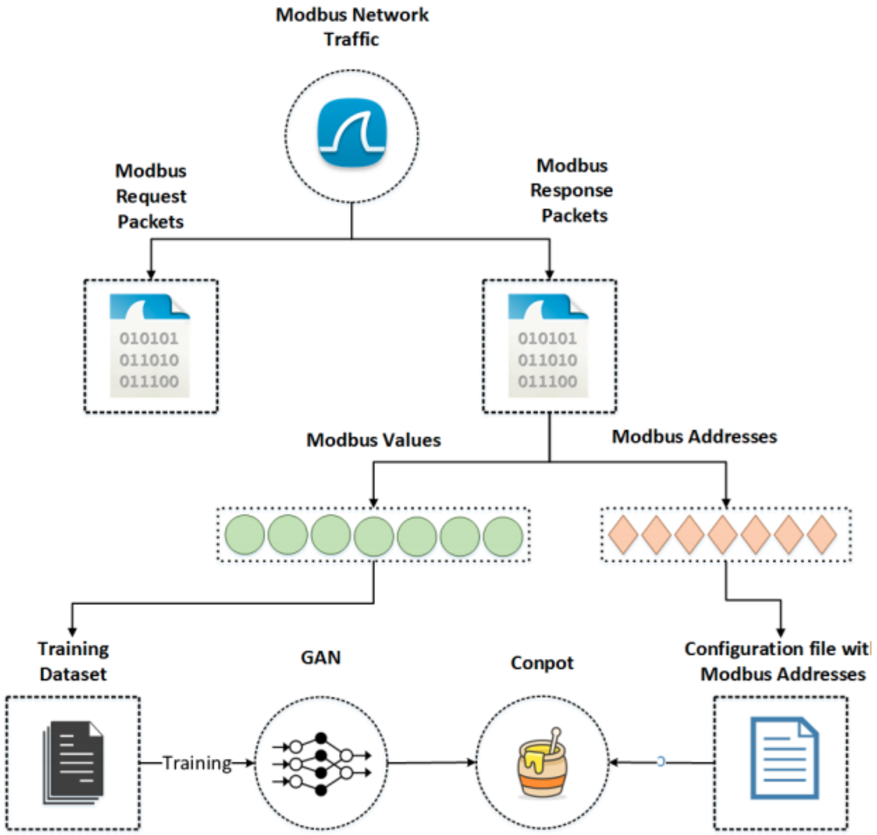
The Modbus honeypot has the ability to emulate both entities operating like a server, such as an RTU or client entities like an HMI

Supporting more Modbus/TCP function codes not available in Conpot

The current version of Conpot does not support adequately all Modbus function codes. In the context of the SDNmicroSENSE project, the Modbus honeypot adopts Conpot in order to emulate the server side of the Modbus TCP/IP communication, thereby incorporating more Modbus function codes.

Imitating the Modbus/TCP behaviour of real assets

Both sides of the Modbus honeypot (i.e., server and client) have the ability to mimic the behaviour of real devices, generating similar Modbus/TCP network traffic.



Modbus honeypot Operation Flow as Server

Modbus Honeypot GAN

SDN-μSense

A DNN Modbus Honeypot

Input Module

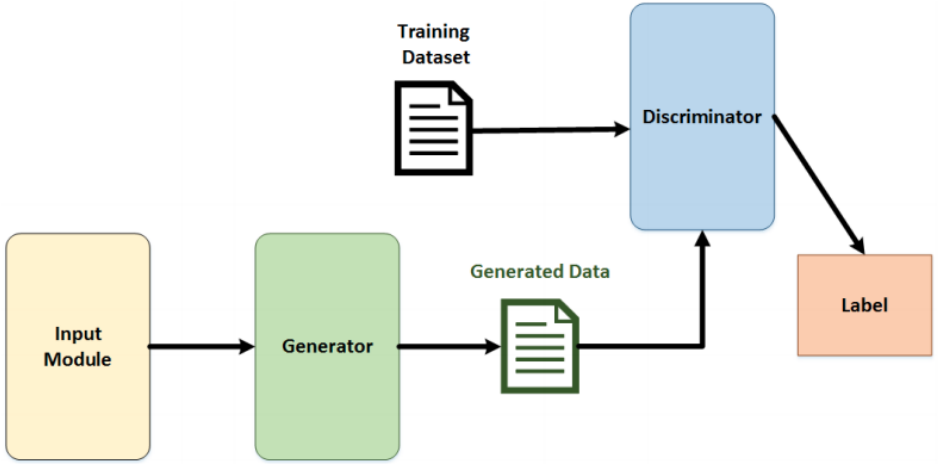
Input noise given to the Generator to produce the emulated data. The random noise is created using the normal distribution with mean μ = 0 and a standard deviation of σ = 1.

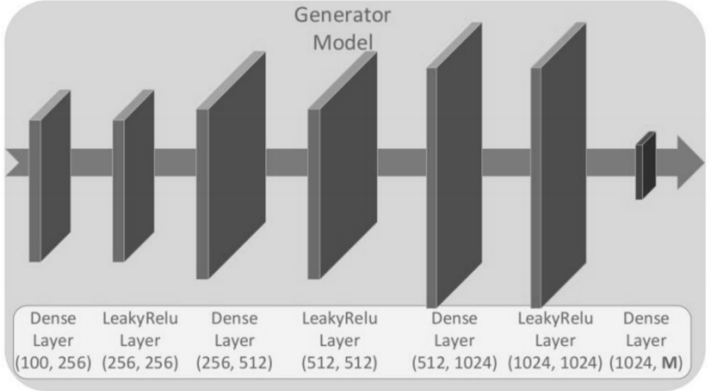
Generator

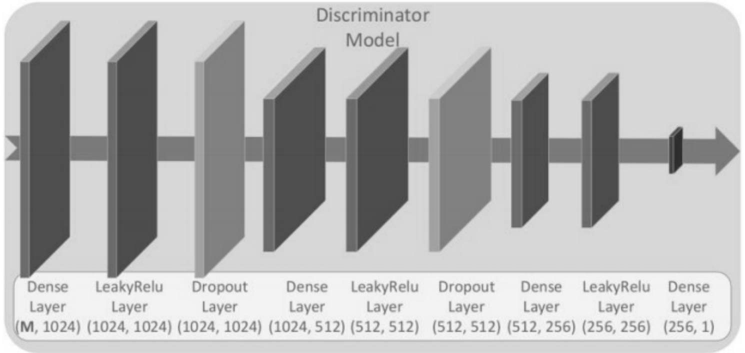
Produce an output that identical to the real data. Seven layers; Binary cross-entropy loss function; Adam Optimizer

Discriminator

Classifying real data, originating from the input dataset and the generated data originating from Generator







From Honeypot-oriented Risk Analysis to Islanding Solutions in Energy Systems

SDN-μSense

Step #1 01

Step #2 02

Step #3 03

Step #4 04

EPES Honeypots Deployment

The EPES honeypots are deployed successfully, emulating the behavior of the real EPES devices.

Honeypots' Security Events

The EPES honeypots generate security events based on their interaction with the cyberattackers.

Security Events Analysis

Based on the criticality of the security events, the Islanding solutions are activated

Identifying and Applying the Optimal Islanding Scheme

The islanding mechanisms identify and apply the optimal islanding scheme

Islanding solutions in Energy Systems

SDN-μSense

Terminology

- **Microgrid**

A microgrid is a decentralized group of electricity sources and loads that normally operates connected to and synchronous with the traditional wide area grid but can also disconnect and operate autonomously in "island mode".

- **Distributed energy resources (DERs)**

DERs are resources used for electricity generation and storage, connected to the grid at a distribution level. Typically, DERs can include renewable energy sources such as solar panels and wind turbines.

Definition

SDN-μSense

Intentional islanding is the process in which a microgrid controller disconnects a local circuit from the main power grid on a dedicated switch and forces the distributed generators to provide power to the entire local load.

Modern energy systems have microgrids as core building blocks and utilise DERs to enable the use of intentional islanding solutions in case of severe failures in the power grid.

When is it used?

When a critical event occurs, such as a fault or outage of an overloaded line, it may cause overloading of additional lines and as a result, subsequent outages and a cascading failure. These are costly events which may threaten the integrity of the energy system.

- Intentional Islanding is used as a last measure to separate the grid into several controlled, sustainable islands, to alleviate the impact of the fault and reduce the undesirable technical, economic and social consequences of a possible blackout.

- In case of an emergency, it constitutes an effective solution to preserve reliable power supply in the smart distribution grid, increasing the overall system reliability.

Key Issues

SDN-μSense

WHEN

When should the Intentional islanding be applied

WHERE

Which islands should be formed (i.e. what are the appropriate islanding boundaries)

HOW

How should the Intentional islanding be implemented

Intentional Islanding Problem

The core idea behind the problem of intentional islanding is to decide which transmission lines should be disconnected in order to create stable islands, smaller in size and thus easier to control.

- Often translated into a graph partitioning problem
- Generally considered NP-hard
- Most approaches are based on optimisation theory

Key objectives

- Determine optimal boundaries of islands
- Minimise load-generation imbalance

Intentional Islanding in SDN-microSENSE

SDN-μSense

Inside the SDN-microsense project, novel islanding solutions are proposed, exploiting powerful fitting and generalisation capabilities offered by deep learning architectures.

- Introducing an end-to-end deep graph neural network approach
- Solution to the intentional islanding problem using deep learning formulations for the first time
- Optimising the load and generation balance
- Offering a real-time solution with increased time efficiency

Intentional Islanding using Deep Learning

SDN-µSense

The devised solution is based on the Generalisable Approximate Partitioning (GAP) framework for graph partitioning and the normalized min-cut problem. The islanding problem is formulated as a minimum cut problem as follows:

$$cut(S_k, \hat{S}_k) = \sum_{v_i \in S_k, v_j \in \hat{S}_j} e(v_i, v_j)$$

Where S_k is the k-th set of a given graph, $\hat{S}_k$ represents the remaining sets except S_k and $e(v_i, v_j)$ is the edge between vertex v_i and v_j.

Intentional Islanding using Deep Learning

SDN-μSense

- The GAP method addresses the cut problem using deep learning optimisation, transforming it into a deep learning format as follows:

$$L_{cut} = \sum_{reduce\_sum} (Y \oslash \Gamma)(1 - Y)^T \odot A + \sum_{reduce\_sum} (1^T Y - \frac{n}{g})^2$$

- The normalized min-cut problem is formulated as follows:

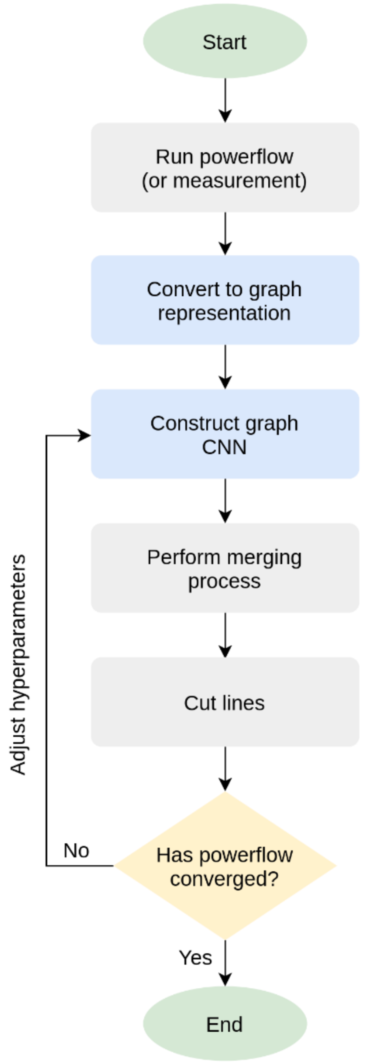
$$L = L_c + L_o = -\frac{Tr(S^T \hat{A} S)}{Tr(S^T \hat{D} S)} + \left|\left| \frac{S^T S}{||S^T S||_F} - \frac{I_K}{\sqrt{K}} \right|\right|$$

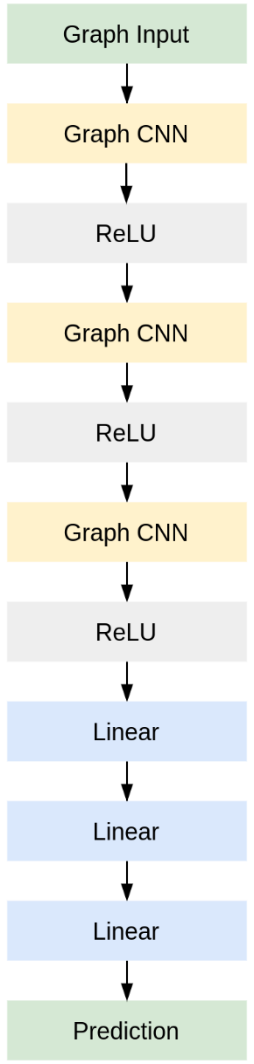
Intentional Islanding using Deep Learning

SDN-μSense

Pipeline of the intentional islanding method

- Compute the power flow of the power system
- Convert the power system network into a graph
- Each bus corresponds to a vertex in the graph
- Each transmission line and transformer corresponds to an edge
- Deep CNN model
- Merging process (assign isolated buses to nearest cluster)
- Cut lines

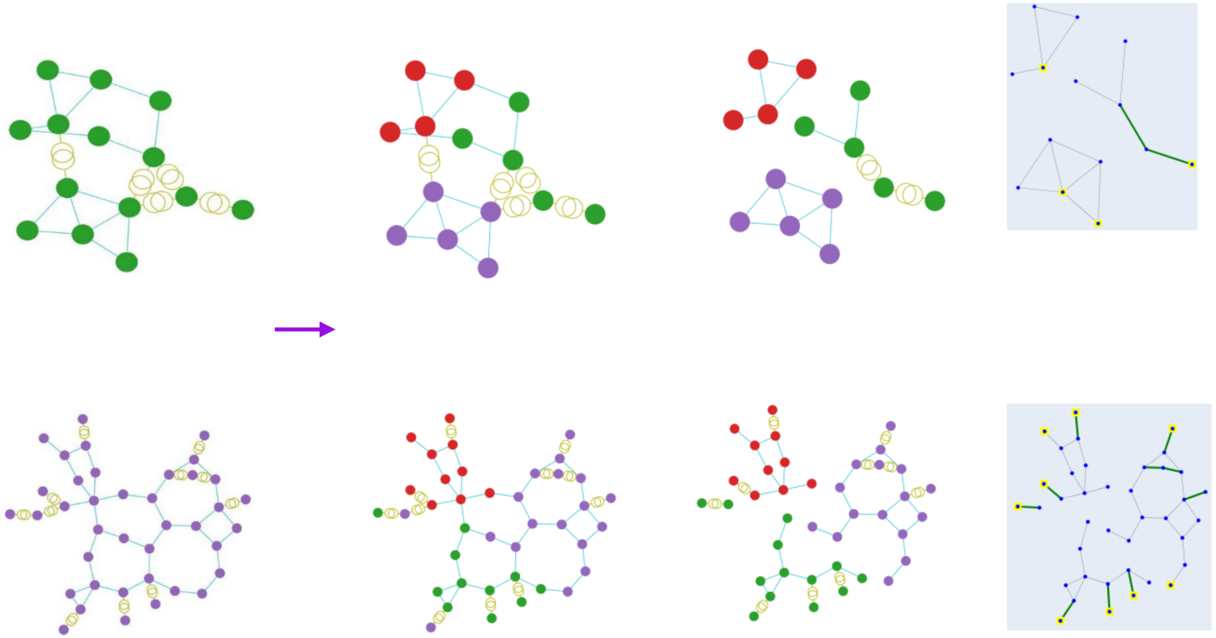




Intentional Islanding using Deep Learning

Evaluation Results

Evaluated on power grids adapted from actual energy systems. The results include the number of lines to be cut, the load-generation imbalance after islanding as well as the total imbalance after the merging process is completed and the cut is applied.



Method	Imbalance	After merge	Lines
GAP	286.95	286.95	**7**
GAP +	80.22	44.46	9
Min-cut	**34.62**	**34.62**	9

Method	Imbalance	After merge	Lines
GAP	1837.53	**185.09**	28
GAP +	1315.09	1315.09	33
Min-cut	**342.90**	342.90	**18**

Thank You & Q/A

Contact us

psarigiannidis@uowm.gr

http://www.sdnmicrosense.eu/

https://www.linkedin.com/groups/12248810/

https://www.youtube.com/channel/UC5xpUNpQQ6eAQvc5JpnWWGw

Thank You

Q/A ?