This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787011.

SPEAR NEWSLETTER

6th newsletter March 2021

Dear reader,

You are reading the 6th issue of our newsletter, published by the SPEAR project, a Horizon 2020 program funded by European Union under grant agreement No. 787011.

This issue presents the awards and distinctions that the SPEAR consortium has received for publications to scientific conferences.

You can always stay up-to date about our latest success stories in our dedicated web page of the SPEAR website:

https://www.spear2020.eu/Awards

Project Details

- **Project no.** 787011
- **Research and Innovation Action:** Co-funded by the Horizon 2020 Framework Programme of the European Union
- **Call identifier:** H2020-DS-2016-2017 (Digital Security Focus Area)
- **Topic: DS-07-2017:** Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors
- **Project Start date:** May 1st, 2018 (36 months duration)

SPEAR Publications

The SPEAR consortium continuously updates the SPEAR website about new publications, which are also uploaded in Zenodo. You can find bellow our latest publications:

- T. Rokkas and I. Neokosmidis, "Factors affecting the market adoption of cyber-security products in energy and electrical systems," presented at the ARES 2020: The 15th International Conference on Availability, Reliability and Security, Jul. 2020: https://zenodo.org/record/4436107
- V. Mladenov, V. Chobanov, P. Sarigiannidis, P. I. Radoglou-Grammatikis, A. Hristov, and P. Zlatev, "Defense against cyber-attacks on the Hydro Power Plant connected in parallel with Energy System," presented at the 2020 12th Electrical Engineering Faculty Conference (BulEF), Sep. 2020: https://zenodo.org/record/4478873
- I. Siniosoglou et al., "NeuralPot: An Industrial Honeypot Implementation Based On Deep Neural Networks," presented at the 2020 IEEE Symposium on Computers and Communications (ISCC), Jul. 2020: https://zenodo.org/record/4478601

Communication

Website

https://www.spear2020.eu

LinkedIn

https://www.linkedin.com/company/spear2020

YouTube

https://www.youtube.com/channel/UCw6-d5G01ToBhCmaUnHIcpw

Project Coordinator:
Prof. Panagiotis Sarigiannidis
University Of Western Macedonia, Greece

E-mail: psarigannidis@uowm.gr

DISCLAIMER: The content of this document reflects only the author's views and not the views of the European Commission / Research Executive Agency (REA). The European Commission and REA are not responsible for any use that may be made of the information included in this document.

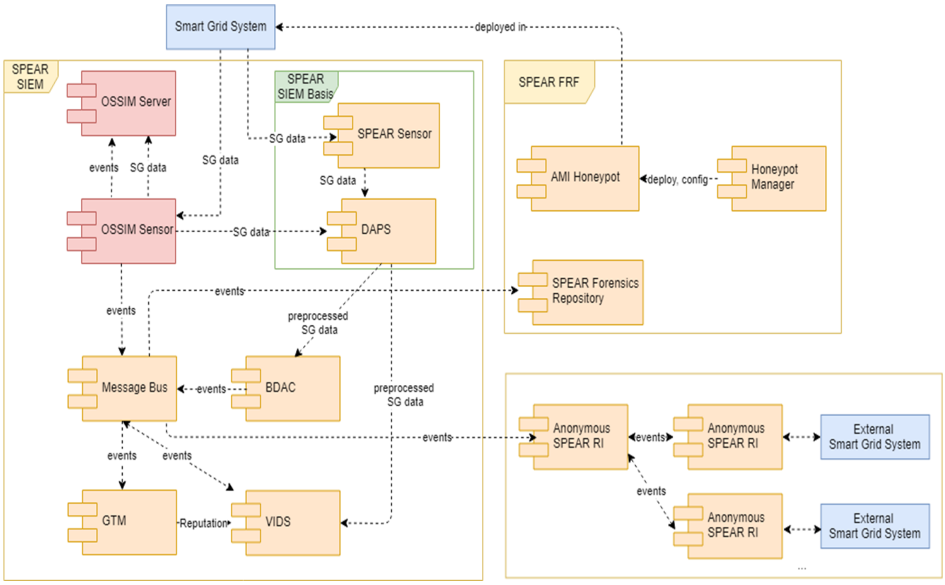
SPEAR Architecture

The SPEAR project aims to introduce a three-tier platform architecture that is able to ensure confidentiality, integrity and availability of smart-grid oriented data and services. The SPEAR architecture consists of the following major layers:

SPEAR SIEM: The SPEAR system information and event management framework aims at detecting and illustrating anomalies on operational data and network traffic that could indicate a cyber-attack or any kind of anomaly that needs immediate action.

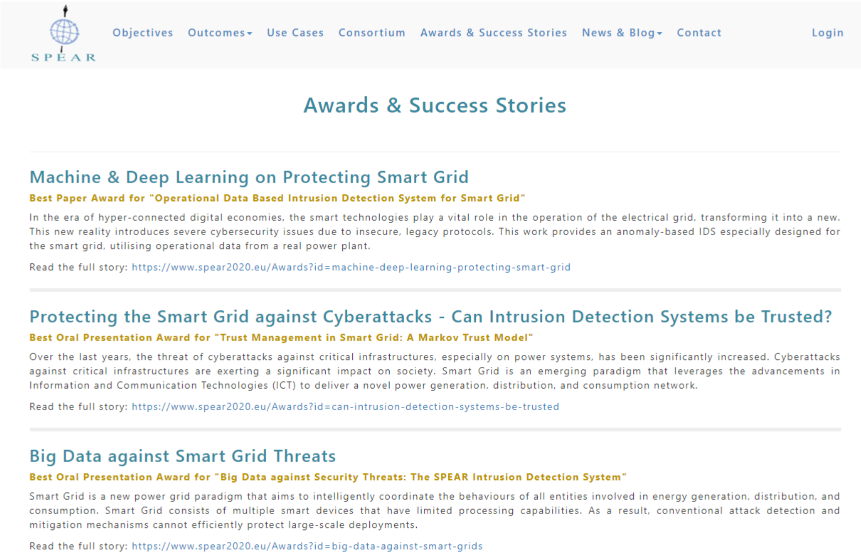
SPEAR FRF: The SPEAR Forensic Readiness Framework encompasses tools that process forensic data and prepare evidences which can be used in courts. In addition, FRF realizes the optimal deployment of honeypots to trap attackers and collect precious evidences.

Anonymous SPEAR-RI: The SPEAR Anonymous Repository of Incidents enables communication and transaction of security incidents among energy providers and operators in Europe. Anonymisation techniques guarantee that the participating organisations will not get exposed.



SPEAR Architecture

SPEAR Awards & Success Stories



Awards & Success Stories

Machine & Deep Learning on Protecting Smart Grid

Best Paper Award for "Operational Data Based Intrusion Detection System for Smart Grid"

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. This new reality introduces severe cybersecurity issues due to insecure, legacy protocols. This work provides an anomaly-based IDS especially designed for the smart grid, utilising operational data from a real power plant.

Read the full story: https://www.spear2020.eu/Awards?id=machine-deep-learning-protecting-smart-grid

Protecting the Smart Grid against Cyberattacks - Can Intrusion Detection Systems be Trusted?

Best Oral Presentation Award for "Trust Management in Smart Grid: A Markov Trust Model"

Over the last years, the threat of cyberattacks against critical infrastructures, especially on power systems, has been significantly increased. Cyberattacks against critical infrastructures are exerting a significant impact on society. Smart Grid is an emerging paradigm that leverages the advancements in Information and Communication Technologies (ICT) to deliver a novel power generation, distribution, and consumption network.

Read the full story: https://www.spear2020.eu/Awards?id=can-intrusion-detection-systems-be-trusted

Big Data against Smart Grid Threats

Best Oral Presentation Award for "Big Data against Security Threats: The SPEAR Intrusion Detection System"

Smart Grid is a new power grid paradigm that aims to intelligently coordinate the behaviours of all entities involved in energy generation, distribution, and consumption. Smart Grid consists of multiple smart devices that have limited processing capabilities. As a result, conventional attack detection and mitigation mechanisms cannot efficiently protect large-scale deployments.

Read the full story: https://www.spear2020.eu/Awards?id=big-data-against-smart-grids

The SPEAR awards and success stories in the SPEAR website

Motivated by the market needs for new cybersecurity solutions in the energy domain, as well as the significant research gaps in this domain, the SPEAR consortium is committed to produce innovative research, resulting to its recent distinction in scientific conferences. In particular, the SPEAR consortium received three awards (one best paper award and two best oral presentation awards) in conferences for novel research in the smart grid domain.

A new section in the SPEAR website gathers all awards and distinctions that have been received by the SPEAR consortium. You can access this page on the following link: https://www.spear2020.eu/Awards

You can read the full stories of our awards in the next pages.

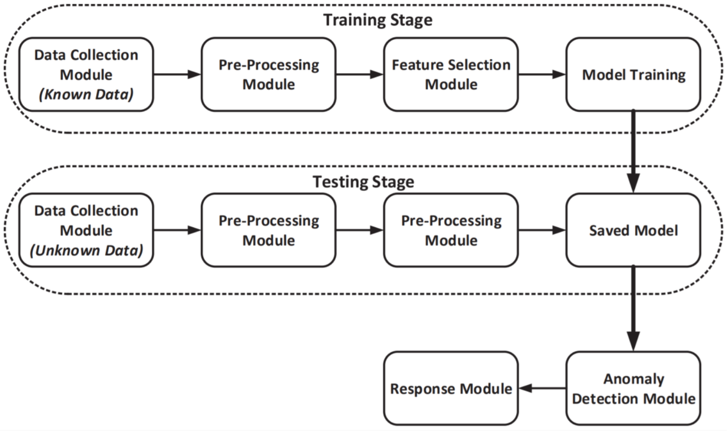
Machine & Deep Learning on Protecting Smart Grid

Best Paper Award for "Operational Data Based Intrusion Detection System for Smart Grid"

G. Efstathopoulos, P. Radoglou Grammatikis, P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. Angelopoulos and S. Athanasopoulos, "Operational Data Based Intrusion Detection System for Smart Grid", in IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, Limassol, Cyprus, 2019, pp. 1-6. [Online] Available: https://zenodo.org/record/3834769

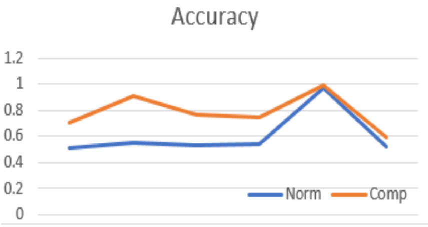
In the era of **hyper-connected** digital economies, the smart technologies play a vital role in the operation of the **electrical grid**, transforming it into a new paradigm. This new reality introduces **severe cybersecurity issues** due to **insecure**, **legacy protocols**. Our latest work entitled "**Operational Data Based Intrusion Detection System for Smart Grid**" proposed a novel approach for **protecting** modern smart grids by timely **detecting cyberthreats** and indications of attacks. This work was presented at the **IEEE International Workshop on Computer Aided Modelling and Design of Communication Links and Networks** and won the **best paper award**.

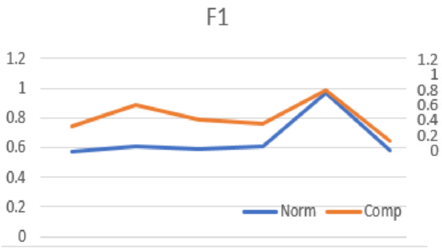
A Novel Cybersecurity Approach

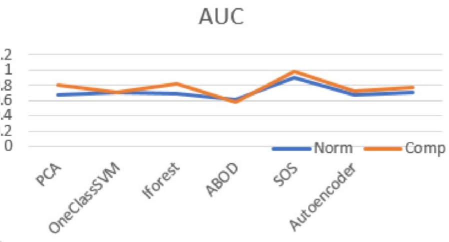


- **Anomaly-based IDS** especially designed for the **smart grid**, utilising operational data from a real power plant
- Evaluation of **multiple machine learning** and **deep learning models**, introducing novel parameters and feature representations in a comparative study
- The evaluation analysis demonstrates the **efficacy** of the proposed IDS and the improvement due to the suggested complex data representation

An Accurate & Efficient Tool for Energy Stakeholders







- Metrics: **Accuracy, F1, AUC** (Area Under Curve)
- Evaluation Environment: **Power plant of PPC S.A.,** in Greece (https://www.dei.gr/)
- Via the proposed complex representation, the overall average **Accuracy** was **increased by 29%**, the **F1 score** by **22%** and the **AUC** by **8%**.

Paving the Way to a New Energy Market

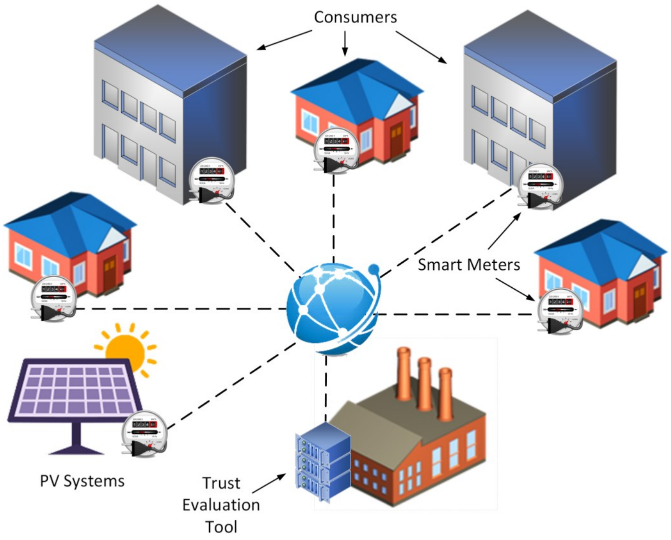
The new solution introduced by this work paves the way for **more accurate IDS**, capable to **detect a variety of threats** in modern smart grids, thus, enabling the operators to **timely respond to security incidents** and rendering smart grids more **secure** and **trusted**. Moreover, the proposed solution opens **new market opportunities** in the energy domain, including:

- Commercial **intrusion/anomaly detection**
- **Preventing** energy failures like **blackouts** & enhancing **islanding schemes for isolating the attack**

Protecting the Smart Grid against Cyberattacks - Can Intrusion Detection Systems be Trusted?

Best Oral Presentation for "Trust Management in Smart Grid: A Markov Trust Model"

D. Pliatsios, P. Sarigiannidis, G. Efstathopoulos, A. Sarigiannidis, A. Tsiakalos, 'Trust Management in Smart Grid: A Markov Trust Model', Proceedings of 10th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2020. [Online] Available: https://zenodo.org/record/4044528

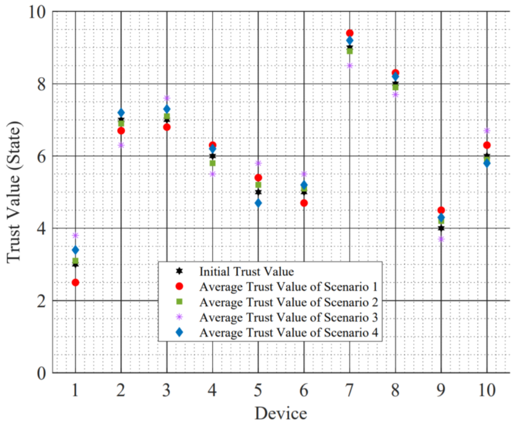


Over the last years, the threat of cyberattacks against critical infrastructures, especially on power systems, has been significantly increased. **Cyberattacks against critical infrastructures are exerting a significant impact on society**. Smart Grid is an emerging paradigm that leverages the advancements in Information and Communication Technologies (ICT) to deliver a novel power generation, distribution, and consumption network. **The smart meters are core components of the Smart Grid, which are deployed throughout the infrastructure**. These meters continuously monitor the energy generation, distribution, and consumption throughout the Smart Grid.

Advanced Intrusion Detection and Prevention Systems cannot be always deployed as the Smart Grid devices have low processing and storage capabilities. **Our latest work entitled "Trust Management in Smart Grid: A Markov Trust Model" was presented at the 9th International Conference on Modern Circuits and Systems Technologies (MOCAST 2020) and won the Best Oral Presentation Award**.

The Trust in Smart Grid Becomes Measurable

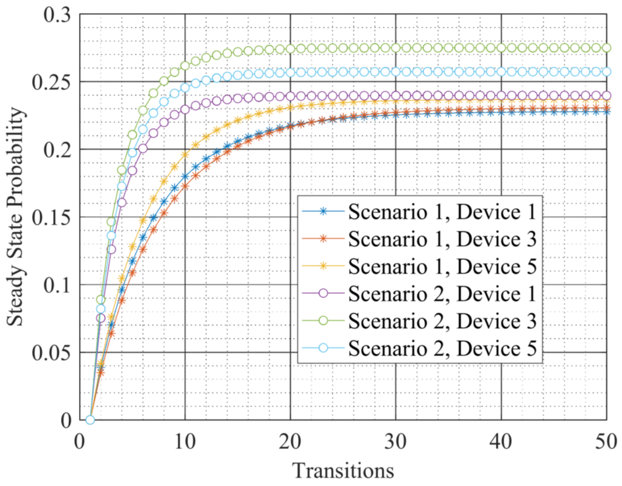
- The security of the Smart Grid can be further enhanced by the deployment of a **trust scheme** alongside an Intrusion Detection System.
- The aim of the trust scheme is to **continuously** monitor a smart grid device interaction with other devices and **evaluate the trust level**.
- When a device has **irregular** behaviour, due to the result of a cyberattack, its **trust level** will be gradually **decreased**. To protect the rest of the Smart Grid, when a device's trust level is **too low**, that device is **isolated** from the rest of the network.



Average Trust Value of Each Device after 50 Transitions

An Accurate & Scalable Trust Scheme for the Energy Domain

- The proposed trust scheme features an **accuracy of up to 100%**
- The math behind the model is validated in a **realistic simulation environment**



Convergence Speed

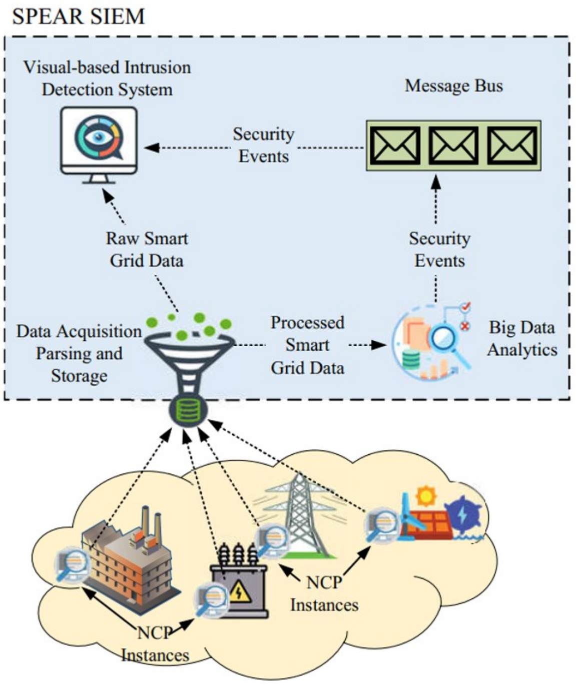
Big Data against Smart Grid Threats

Best Oral Presentation for "Big Data against Security Threats: The SPEAR Intrusion Detection System"

D. Pliatsios, P. Sarigiannidis, K. Psannis, S. K. Goudos, V. Vitsas, I. Moscholios, "Big Data against Security Threats: The SPEAR Intrusion Detection System", in The 3rd World Symposium on Communication Engineering (WSCE 2020), Thessaloniki, Greece, 2020, pp. 12-17. [Online] Available: https://zenodo.org/record/4575980

Smart Grid is a **new power grid paradigm** that aims to **intelligently coordinate** the behaviours of all entities involved in **energy generation**, **distribution**, and **consumption**. Smart Grid consists of multiple smart devices that have **limited processing capabilities**. As a result, conventional attack detection and mitigation mechanisms **cannot efficiently protect** large-scale deployments.

Our latest work entitled "**Big Data against Security Threats: The SPEAR Intrusion Detection System**" presented the Intrusion Detection System that is being developed in the context of the SPEAR project. The work was presented at the 3rd World Symposium on Communication Engineering (**WSCE 2020**) and won the **best oral presentation award**.



Introducing a Novel Security Information and Event Management Tool

SPEAR introduces an additional defence level in **Security Information and Event Management (SIEM)** tools

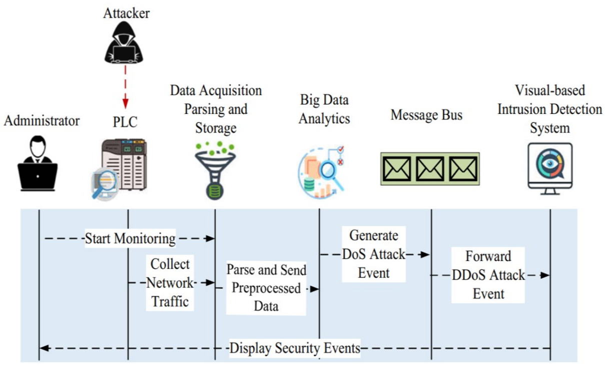
The SPEAR SIEM tool consists of four main components

- Data Acquisition Parsing and Storage
- Big Data Analytics
- Message Bus
- Visual-based Intrusion Detection System

Big Data analytics and **visualization** techniques will timely detect cyberattacks

A Complete Smart Grid Security Solution

SPEAR constitutes a **complete security solution**, tailored to the security requirements of the Smart Grid. The integrated Big Data analytics are capable of monitoring **large-scale deployments** of smart devices. Additionally, **intuitive visualization techniques** can provide real-time information about the smart grid status, as well as detailed alerts in cases of cyberattacks. From the market perspective, the SPEAR solution offers **security automation**, **accelerates time-to-protection**, and **facilitates security operations**.


Attacker
Administrator
PLC
Data Acquisition Parsing and Storage
Big Data Analytics
Message Bus
Visual-based Intrusion Detection System
Start Monitoring
Collect Network Traffic
Parse and Send Preprocessed Data
Generate DoS Attack Event
Forward DDoS Attack Event
Display Security Events

Case Study: Wind Power Plant

- The wind power plant features some unique characteristics according to the **European Program for Critical Infrastructure Protection**
- The SPEAR SIEM tool is installed in the plant's control centre
- The sensors (NCPs) are deployed in the power plant's **Programmable Logic Controllers** (PLCs)
- The network traffic is collected by the NCP Instances and forwarded to the SPEAR SIEM tool for further analysis