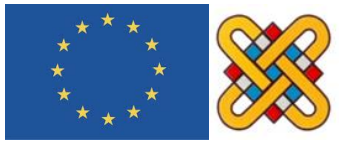


UNIVERSITY OF
WESTERN MACEDONIA

An Overview of the Firewall Systems in the Smart Grid Paradigm

P. Radoglou-Grammatikis, P. Sarigiannidis*, T. Liatifis, T. Apostolakos, S.Oikonomou
University of Western Macedonia
Department of Informatics & Telecommunications Engineering
Communication: psarigiannidis@uowm.gr

Global Information Infrastructure and Networking Symposium 2018 (GIIS 2018)

Outline

- Introduction
- Motivation and Contribution
- Smart Grid Overview
- Advanced Metering infrastructure (AMI)
- Substations
- SCADA Systems
- Synchrophasor Systems
- Microgrids
- Security Challenges in the Smart Grid
- Firewall Systems
- Deployment Goals of a Firewall
- Firewall Limitations
- Firewall Types
- Analyzing Firewall Cases in the Smart Grid Paradigm
- Best Practices for a Firewall in the Smart Grid
- SDN-Based Firewalls
- Conclusions
- SPEAR Project
- SPEAR Objectives
- SPEAR Architecture
- SPEAR Future Steps

Introduction

- The smart grid constitutes a technological evolution of the traditional electrical grid, by introducing ICT services.
- The ICT services offer various benefits, such as increased reliability, better service quality and efficient energy management, but also generate multiple security issues, since it combines various heterogeneous technologies and systems.
- A basic and necessary countermeasure against cyberattacks is the firewall systems. A firewall can be considered as a mechanism which controls the network traffic and determines through specific rules the authorized internal and external communications.

This work provides a study of the firewall systems in the smart grid paradigm, by analyzing various instances and providing new research directions in this field.

This project has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreement No. 787011 (SPEAR).

Motivation and Contribution

Motivation 1: Firewalls constitute crucial systems for the overall security of the Information Technology (IT) and industrial environments.

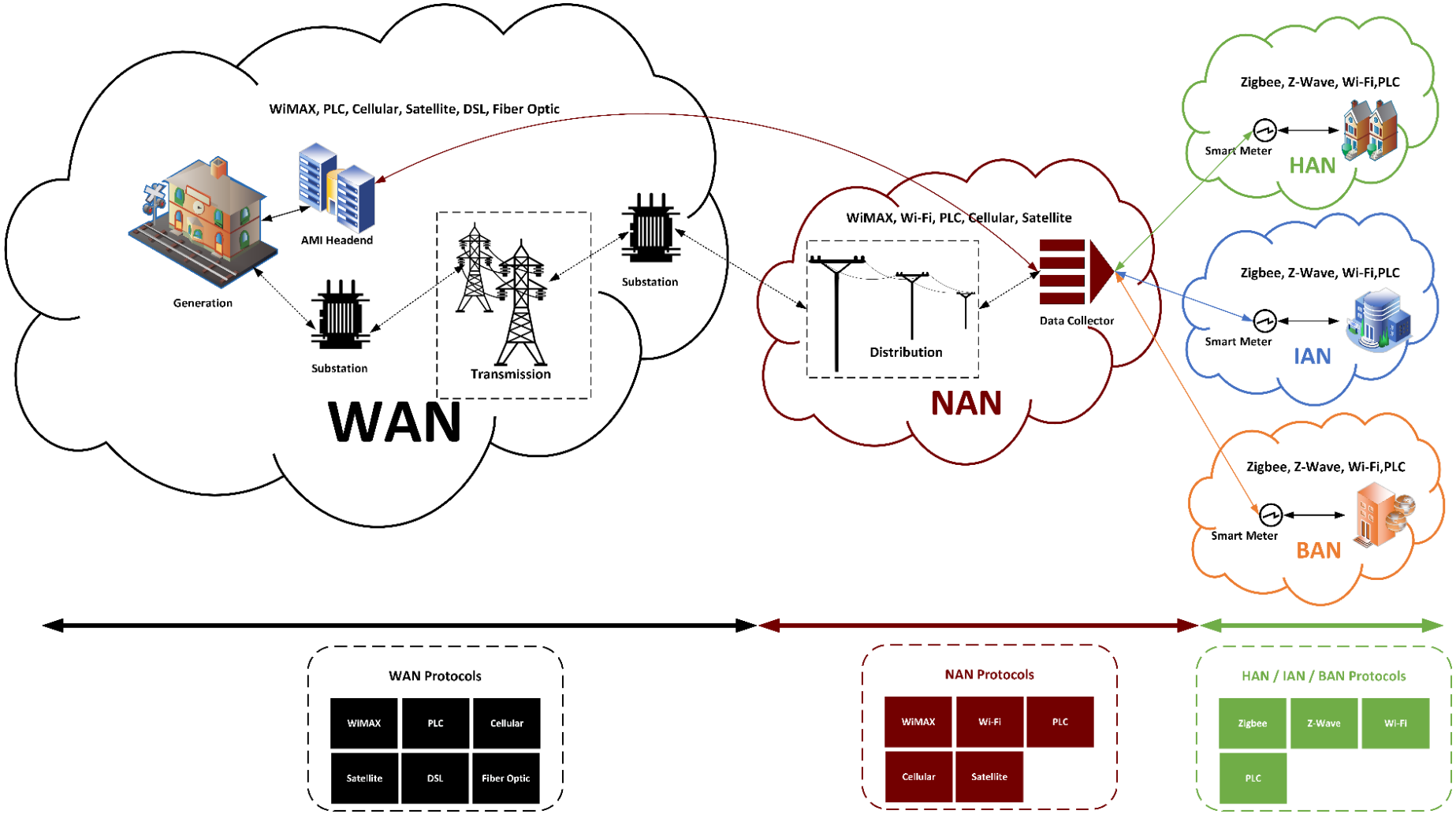
Motivation 2: Although multiple studies examine the security issues of the smart grid, none of them analyze the use of firewalls in this field.

Contribution 1: Examining and analyzing many firewall cases related to the smart grid paradigm.

Contribution 2: Identifying the requirements of firewalls in the smart grid.

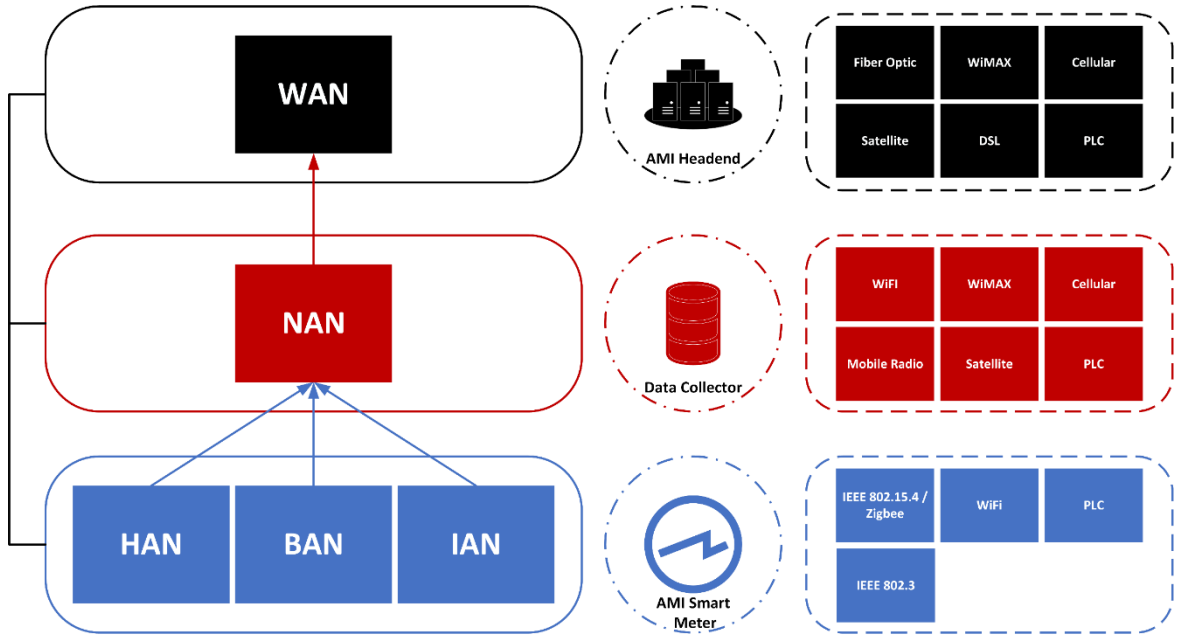
Contribution 3: Providing research directions for future research work in this field.

Smart Grid Overview



Advanced Metering Infrastructure (AMI)

- **AMI** provides all operations that are necessitated for the bidirectional data exchange flow between the end users and utility companies.
- **Smart Meter**: Smart meters undertakes to monitor the power consumption and other measurements of the electrical appliances.
- **Data Collectors**: Data collectors are responsible for storing the information of multiple smart meters that belong in a specific geographic area.
- **AMI Headend**: AMI headend is a server which receives, stores and manages the information of multiple data collectors.



AMI integrates multiple heterogeneous technologies, systems and protocols. This heterogeneity and the corresponding constraints generate many security issues.

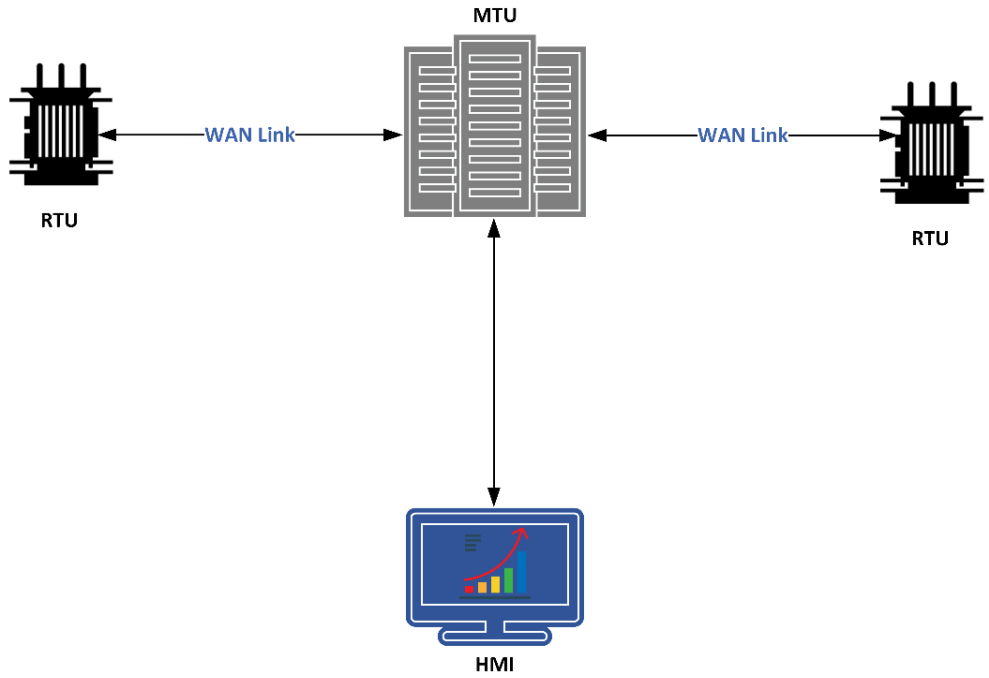
Substations

- Substations participate in the generation, transmission and distribution operations of the electrical grid.
- They receive the generated power, configure the distribution function and control the power increase.
- They can include various devices and software components such as Intelligent Electronic Devices (IEDs), SCADA systems, synchrophasors and GPS.

Substations include multiple legacy industrial and IT devices that are vulnerable to various cyberattacks. Replay attacks, DoS, DDoS and botnets are typical examples.

SCADA Systems

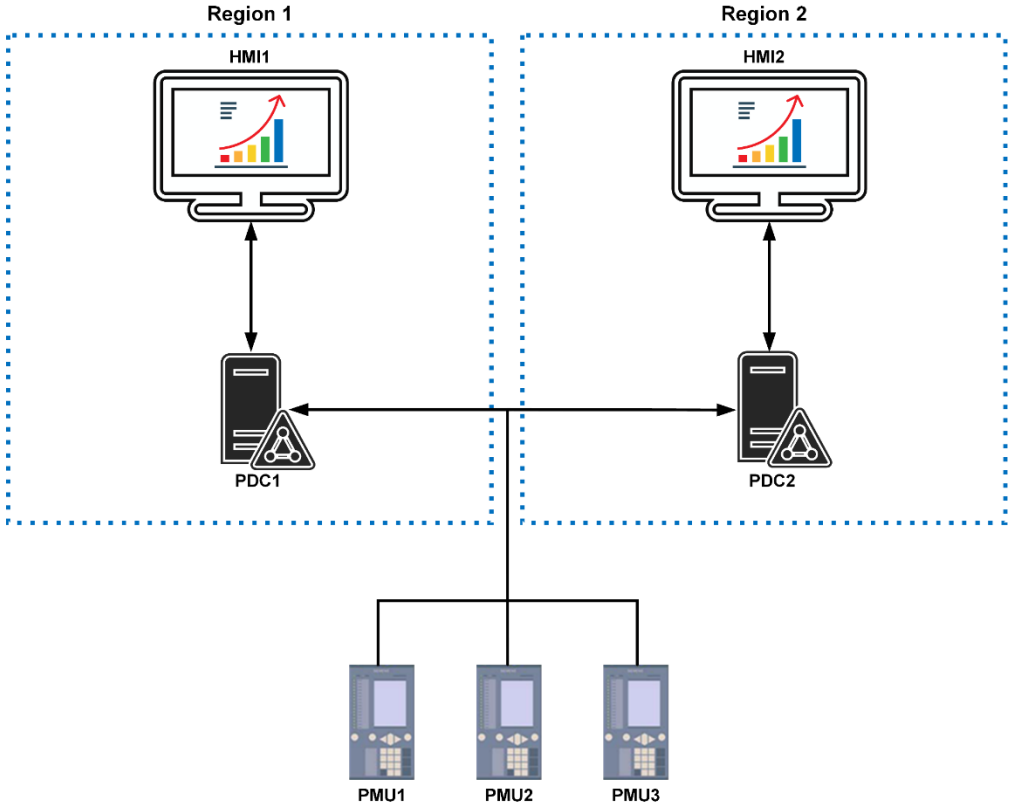
- **Supervision Control And Data Acquisition (SCADA)** systems are part of the industrial environment and their primary operation is to monitor and control the functionality of other components.
- **Logic controllers** (e.g., **Programmable Logic Controller (PLC)**, **Remote Terminal Unit (RTU)**) are mainly responsible for collecting data from the measuring instruments, detecting abnormal behaviors and activating or deactivating technical components.
- The **Master Terminal Unite (MTU)** is the hardware device that represents all the received data from the logic controllers to the operator of the SCADA system.
- The **Human Machine Interface (HMI)** is a software package with graphics capabilities through which the system operator can monitor the processes of the SCADA system.



The SCADA protocols such as Modbus, Distributed Network Protocol (DNP3), IEC 61850, IEC 60870-5 do not include authentication mechanisms. Therefore, they are vulnerable to various cyberattacks.

Synchrophasor Systems

- **Phasor Measurement Unit (PMU)**: A PMU is a device which executes various measurements from current/voltage waveforms, such as frequency, phase angle, active power and reactive power.
- **Phasor Data Concentrator (PDC)**: A PDC undertakes to aggregate the information of PMUs and transform them in a single flow. The communication between PMUs and PDCs is usually carried out through IEEE C37.118.2 and IEC 61850 standards.
- **Graphical User Interface (GUI)**: GUI application is responsible for visualizing appropriately the various data from PDCs.

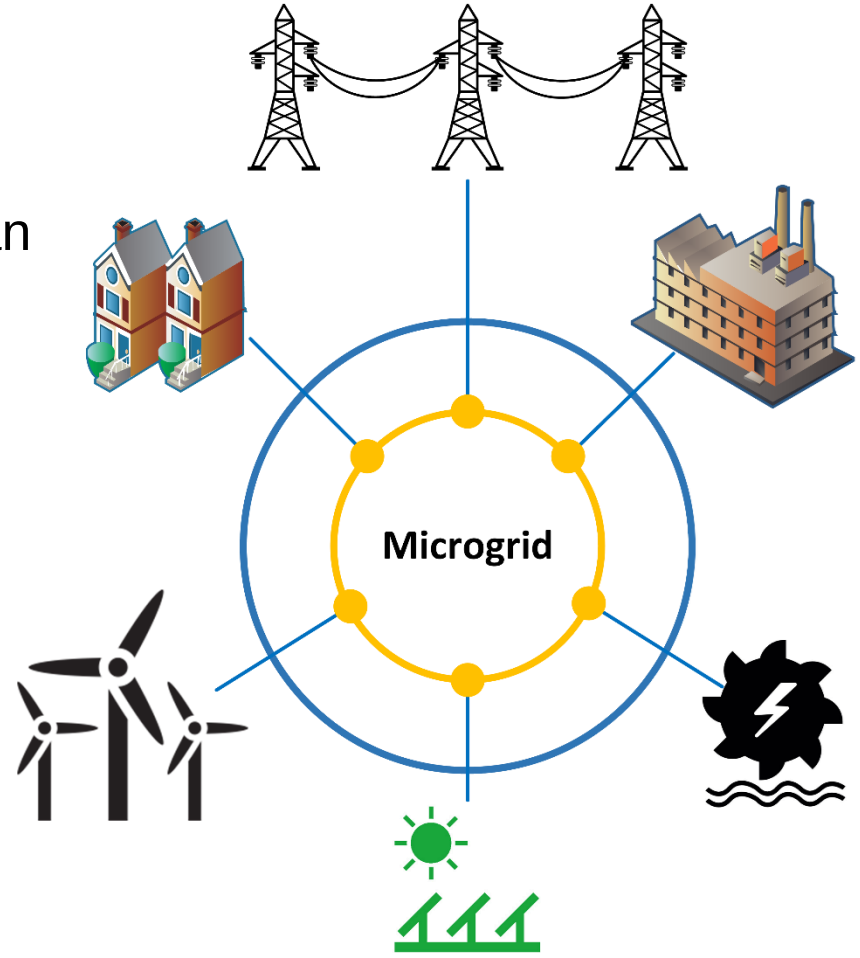


Like SCADA systems, synchrophasors employ vulnerable protocols, such as Modbus, DNP3 and IEC 61850 that enable various cyberattacks.

Microgrids

A microgrid is an independent distribution grid which can operate in conjunction with the main electrical grid, but usually employs Distributed Energy Resources (DERs) to operate autonomously.

A microgrid integrates many of the aforementioned technologies and systems, such as substations, smart meters, data collectors, SCADA systems, etc. Therefore it inherits the corresponding vulnerabilities

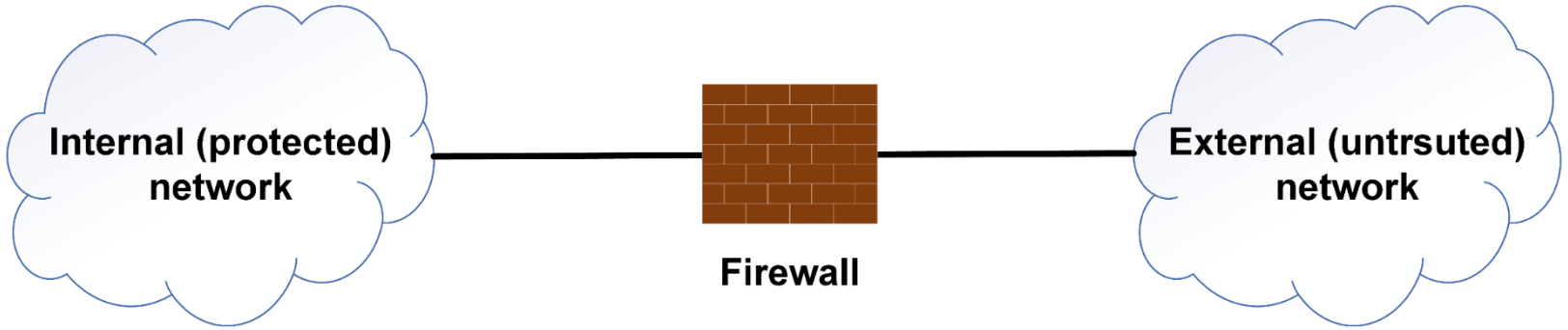


Security Challenges in the Smart Grid

- The interconnected and independent nature of devices, as well as their constrained capabilities regarding the computing resources make impossible the applicability of the conventional security mechanisms.
- The heterogeneity of various technologies which the smart grid combines increases the complexity of the security processes, since each technology is characterized by different vulnerabilities.
- The tremendous amounts of data which is generated by the multiple interactions among the devices make harder their management and the functionality of the access control systems.

Firewall Systems

A firewall is a hardware or software protection system which continuously monitors and controls the network traffic, which is exchanged between the target systems utilizing a specific predetermined security policy as well as control rules.



Positive Policy: That which is not expressly prohibited is permitted.

Negative Policy: That which is not expressly permitted is prohibited.

Deployment Goals of a Firewall

Goal 1: The entire network traffic from inside to outside and vice versa must be monitored and controlled by the firewall system.

Goal 2: Based on the predetermined security policy and the corresponding access control rules, only the authorized network traffic must be allowed.

Goal 3: The firewall system itself should be protected against cyberattacks.

Goal 4: In some cases, a firewall system should be able to perform various tasks that are not security related (e.g. network address translator).

Goal 5: In some cases, a firewall system should be able to perform various tasks that are not security related (e.g. network address translator).

Firewall Limitations

Limitation 1: The firewall cannot provide protection services against attacks that bypass it.

Limitation 2: The firewall cannot provide protection services against internal attacks.

Firewall Types

Firewalls can be classified into four categories based on their functionality:

- **Packet filtering firewall**: Depending on specific rules each incoming or outgoing packet is forwarded or discarded. These rules are based on the source and destination IP addresses, source and destination transport-level addresses, transport protocols and network interfaces.
- **Stateful inspection firewall**: A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections.
- **Application-level gateway**: An application-level does not allow the end-to-end application-layer communication. On the contrary, it plays the role of a proxy between a client and a server controlling the access privileges.
- **Circuit-level gateway**: An Circuit-level does not allow the end-to-end transport-layer communication. On the contrary, it plays the role of a proxy between a client and a server controlling the access privileges.

Analyzing Firewall Cases in the Smart Grid Paradigm

- Our analysis was based on various papers that either develop a firewall system for the electricity industry sector or provide useful instructions for such systems.
- The papers examined provide significant information, such as methodologies, instructions and tools
- Most of the firewalls examined concern the SCADA systems, while few efforts focus on AMI and substations.
- Most of the papers examined focused on the Modbus and DNP3 protocols
- None of the firewalls examined take into consideration the interactions of the microgrids and synchrophasor systems.

Best Practices for a Firewall in the Smart Grid

- The independent and interconnected nature of the smart grid demands a distributed firewall model which should include individual modules possessing the ability to inspect packets from all communication layers and also efficiently big data without reducing the performance the smart grid.
- This distributed firewall has to manage various security events and identifies possible anomalies and critical states, informing the security administrator timely.
- A crucial issue for the deployment of such a firewall, is to determine its location installation. A good practice is the distinction between the private and public networks, by monitoring and controlling their communication.
- If there are entities, such as servers that need to be available to the public network, they should be placed in demilitarized zones.
- A firewall in the smart grid should be characterized by a simple configuration process including a quick installation and configuration process as well as appropriate diagnostic tools.

SDN-Based Firewalls

- The Software Defined Network (SDN) technology can contribute significantly to the development of a distributed firewall for the smart grid.
- The global visibility offered by SDN enables the development of fine-grained monitoring mechanisms at different locations.
- The dynamic programmability allows the development of appropriate preventive countermeasures such as isolating compromised devices, dropping malicious traffic and disconnecting or reconnecting sensors and meters.
- Also, dynamic programmability can assure the timely detection and rapid response to disturbances.

Conclusions

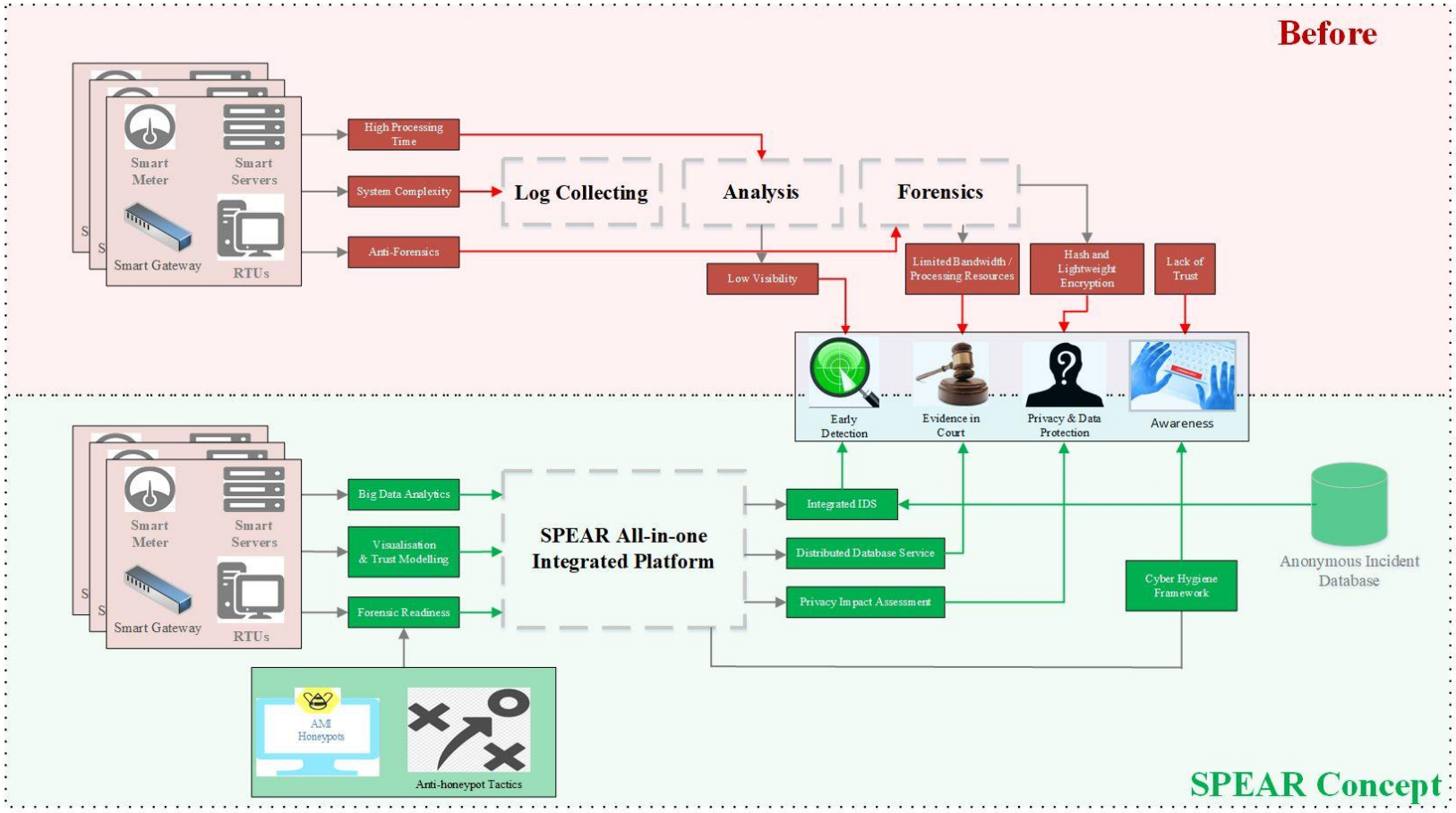
- We presented an analysis regarding the firewall systems in the smart grid paradigm.
- Most of the research efforts in this field focus on SCADA systems without taking into account the heterogeneous nature of the smart grid and its multiple interactions.
- We provided best practices for deploying a firewall in the smart grid paradigm.
- In our future work, we intend to implement a decentralized firewall for the overall protection of the smart grid following the directions of this work.

SPEAR Project

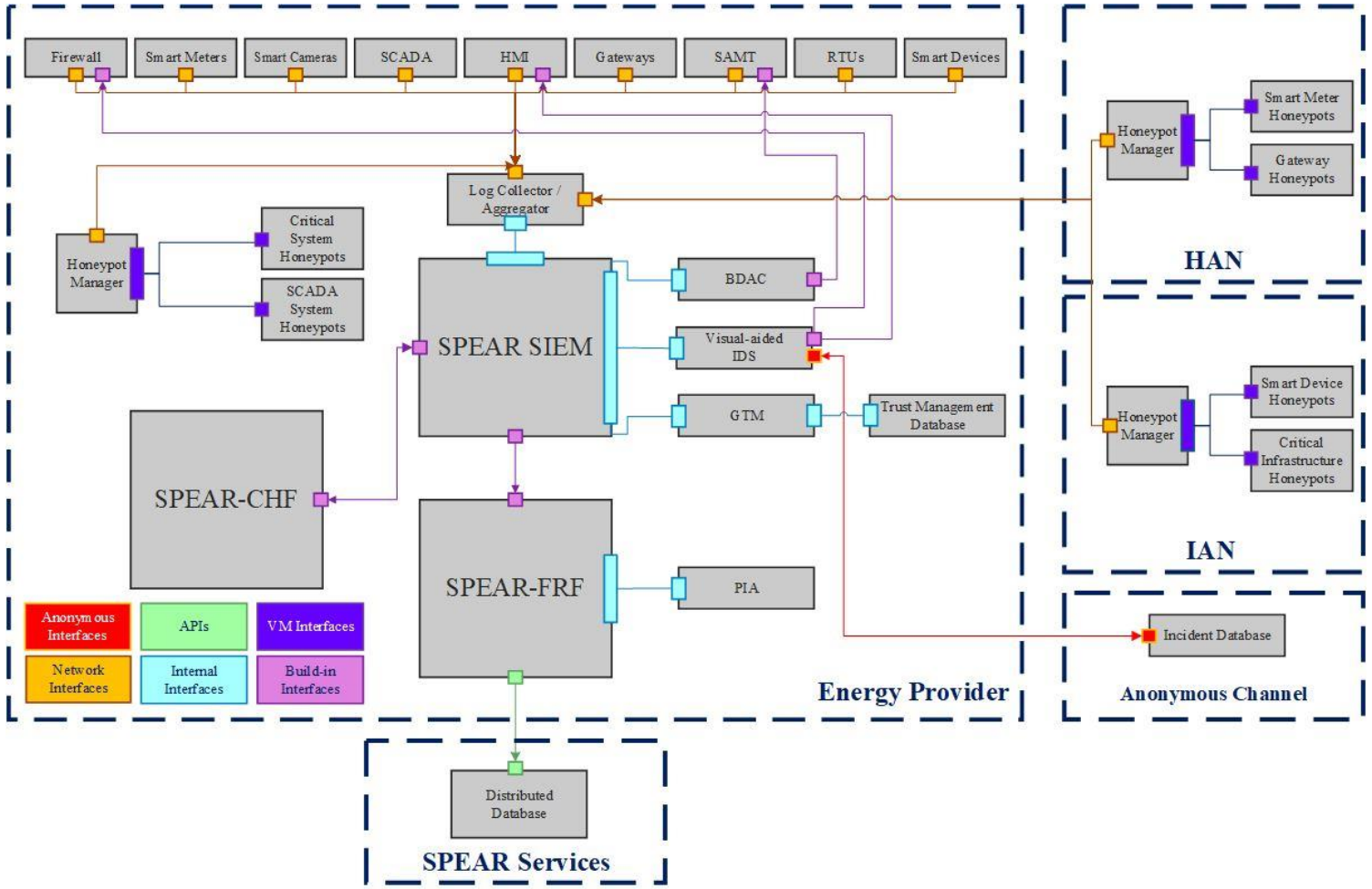
The SPEAR (Secure and PrivatE smArt gRid) project is a research program, co-funded by the Horizon 2020 framework programme of the European Union. SPEAR aims at developing an integrated platform of methods, processes, tools and supporting tools for:

- Timely detection of evolved security attacks such as APT, DoS and DDoS attacks using big data analytics, advanced visual-aided anomaly detection and embedded smart node trust management.
- Developing an advanced forensic readiness framework, based on smart honeypot deployment, which will be able to collect attack traces and prepare the necessary legal evidence in court, preserving the same time user private information.
- Implementing an anonymous smart grid channel for mitigating the lack of trust in exchanging sensitive information about cyber-attack incidents.
- Performing risk analysis and awareness through cyber hygiene frameworks, while empowering EU-wide consensus by collaborating with European and global security organisations, standardisation bodies, industry groups and smart grid operators.
- Exploiting the research outcomes to more CIN domains and creating competitive business models for utilising the implemented security tools in smart grid operators and actors across Europe.

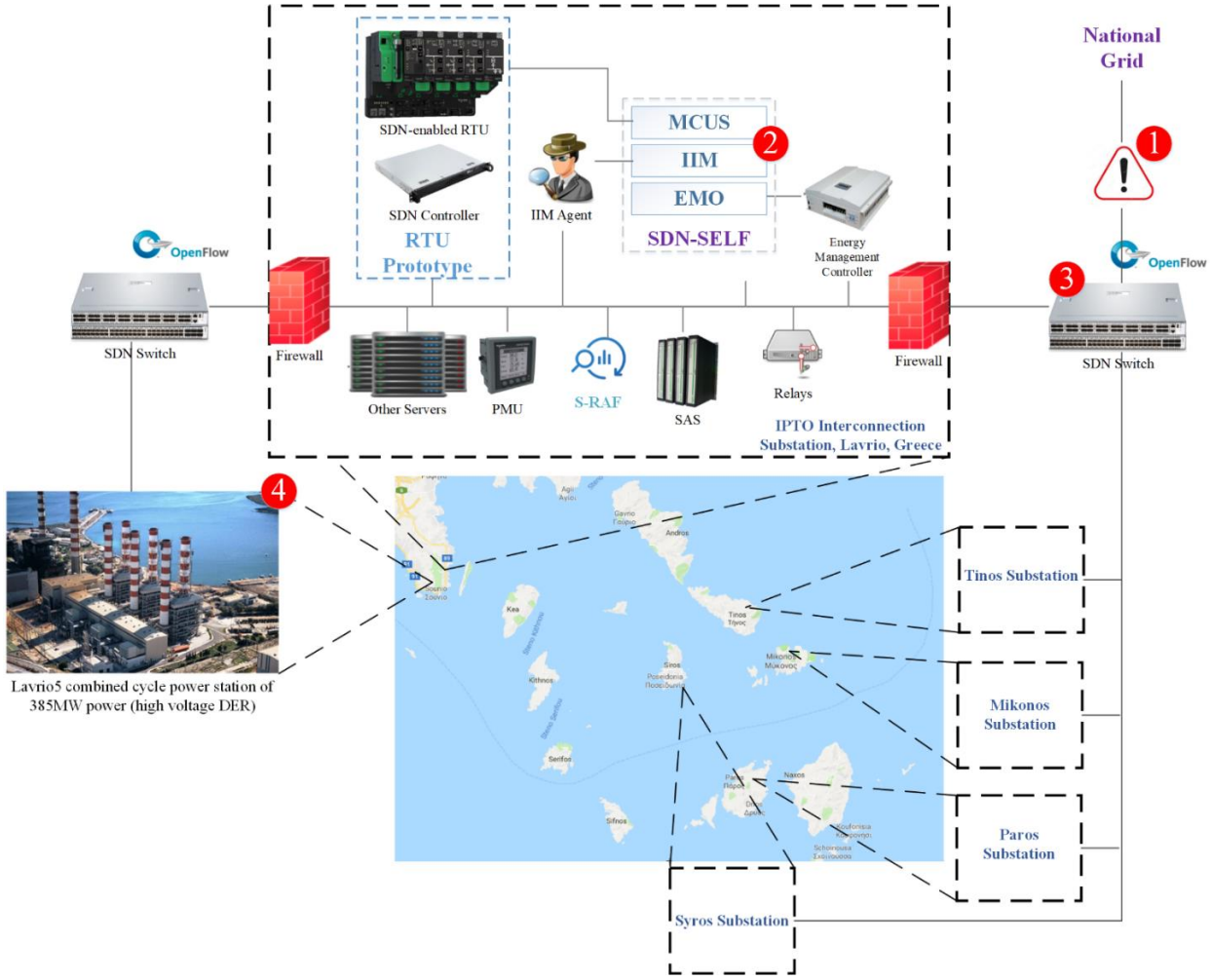
SPEAR Objectives

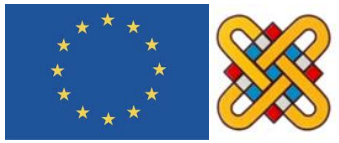


SPEAR Architecture



SPEAR Future Steps





UNIVERSITY OF
WESTERN MACEDONIA

Thank You

Questions ?