# AN INNOVATIVE G3-PLC SIMULATOR

## APPLICATION TO THE COMPARISON OF NETWORK PERFORMANCES BETWEEN SEVERAL CYBER-SECURITY PROTOCOLS AND MECHANISMS IN A SMART METERING SYSTEM

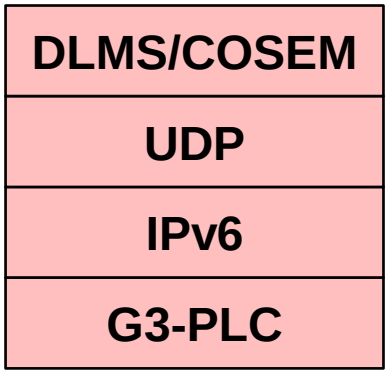
Olivier GENEST – TRIALOG

olivier.genest@trialog.com

# Introduction

## Context and objective of the study

- Many AMI are being deployed
- Many DSOs have chosen PLC as a cost-effective technology for last-mile segment (DC-meter on LV distribution network)
- Numerous projects have chosen a G3-PLC based stack:




- Cyber-security requirements are strong for smart metering
- Hence, upper layers security must be implemented
- In such stack, it may be at network (IPSec), transport (DTLS) or application (DLMS/COSEM) layer

➔ The goal of the study is to evaluate the performances of these 3 security protocols in a smart metering system

# G3-PLC Simulator

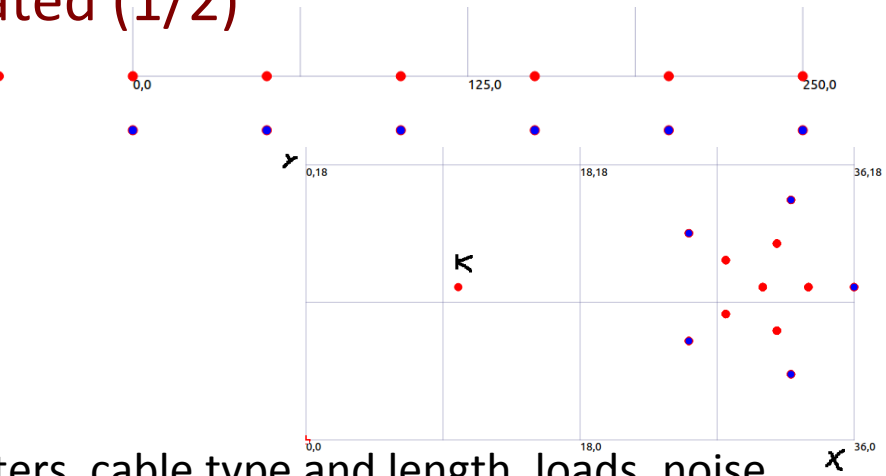
## Trialog has developed a G3-PLC simulator

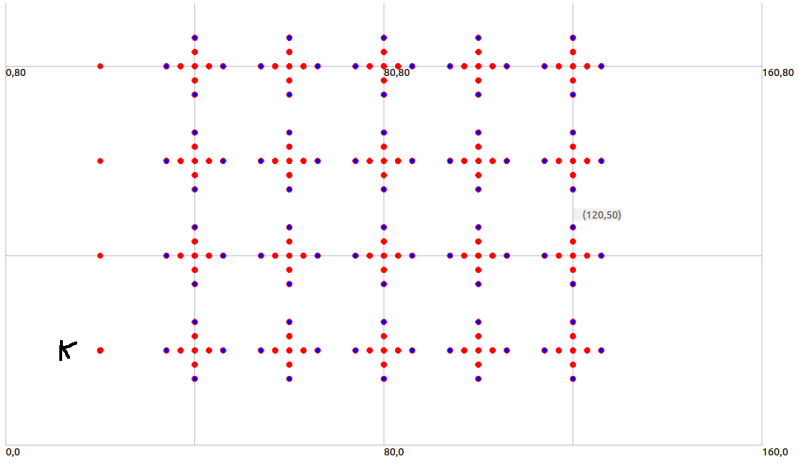
- Based on ns-3 and PLC module
  - Source for PLC module: F. Aalamifar, A. Schlögl, D. Harris and L. Lampe, “Modelling Power Line Communication Using Network Simulator-3”, 2013 IEEE Global Communications Conference (GLOBECOM)
- Physical layer
  - Physical layer is simulated by defining
    - Nodes, cables (type and length)
    - Loads
    - Noise
  - Physical simulation computes an SNR and thus a BER
- Communication stack
  - All previously mentioned layers are implemented, incl. automated mechanisms
- Execution time
  - Execution time is simulated:
    - Communication stack processing
    - Applicative processing
    - Cyber-security computing

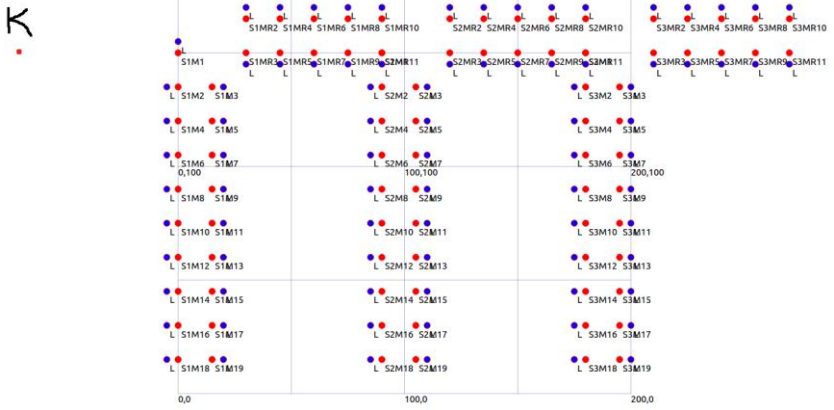
# Smart metering simulation

## A smart metering system is simulated (1/2)

- Distribution network modelling
  - 4 network topologies are defined:
    - Rural
    - High-rise building
    - Dense urban
    - Residential area
  - Each topology defines number of meters, cable type and length, loads, noise
    - Home modelling is based on several measurements campaigns performed by Trialog in Europe
    - Transformer modelling is based on literature



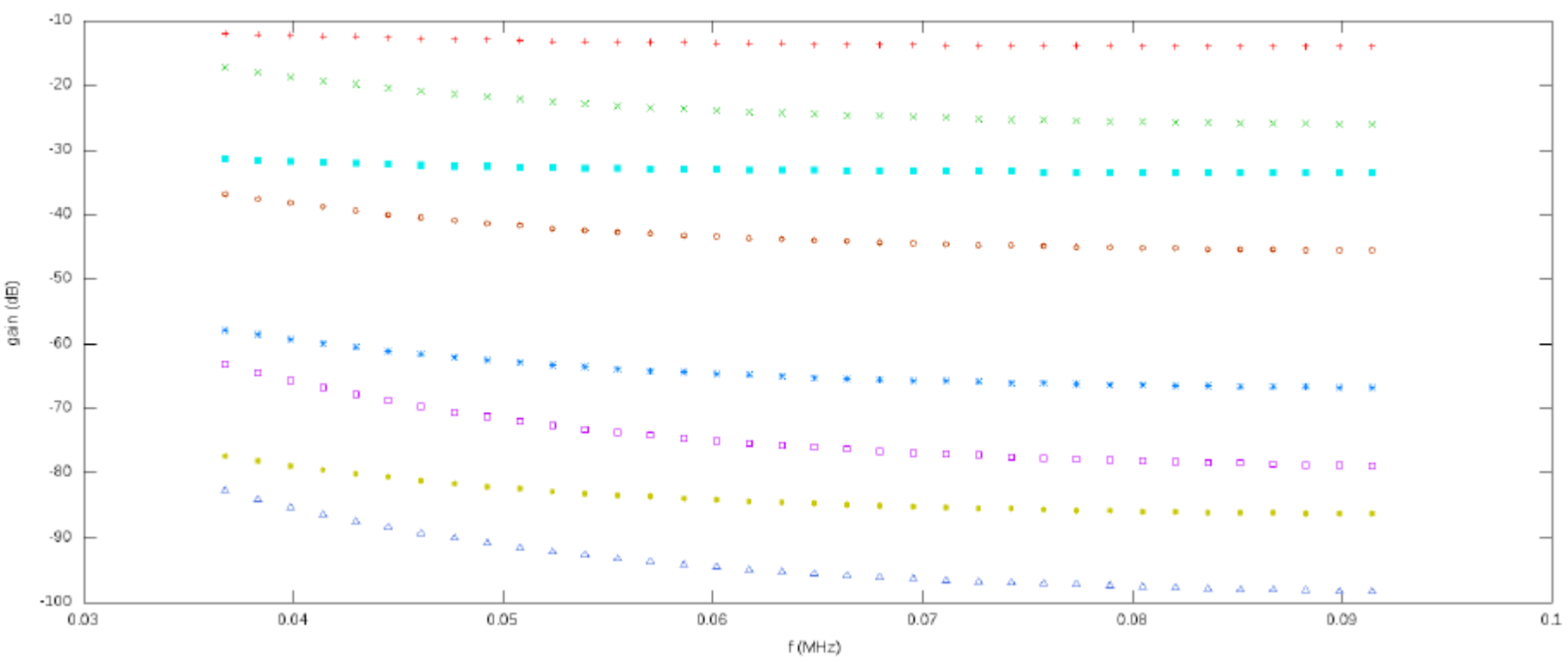



# Smart metering simulation

## Example of physical simulation results

- Subset of meters in dense urban case
- Bode magnitude of DC -> meters channel



# Smart metering simulation

## A smart metering system is simulated (2/2)

- Metering use-cases
  - 6 metering use-cases are implemented:
    - Metering data collection
    - Daily collection
    - Alarm reporting
    - Breaker control
    - Contract setup
    - Firmware upgrade
- Metrics
  - 3 metrics are defined for comparison
    - Percentage of achieved applicative use-cases
    - Total time needed to execute the applicative use-cases
    - Total PLC time needed to execute the applicative use-cases

## Cyber-security protocols comparison

- G3-PLC offers network access control, but it is not sufficient
  - Ensuring privacy of metering data requires end-to-end protection between meter and Data-Concentrator or Information-System
- 3 upper-layer protocols for security are selected
  - IPSec
  - DTLS
  - DLMS/COSEM security
- These protocols are modelled using 3 characteristics:
  - Handshake (number and duration of handshake frames)
  - Overhead
  - Encryption time (during handshake)

| | | |
|---|---|---|
| Handshake | | 120 / 113 / 59 / 52 bytes |
| Encryption time | **Meter** (microcontroller) | 250 ms |
| | **DC** (ARM processor) | 5 ms |
| Overhead | Header | 20 bytes |
| | Encapsulation | 0 byte |
| | Integrity | 8 bytes |
| | **Total** | **28 bytes** |

# Cyber-security study

## Security protocols configuration choices

- Use of modern cryptography algorithms and protocols
  - AES-GCM for ciphering, Elliptic-curves for asymmetric cryptography
  - DTLS 1.2, IKEv2 for IPSec
- Both Pre-Shared Key (PSK) based and Certificate-based authentications are simulated
- When available, Forward Secrecy is activated in the security protocol
  - It allows to protect data secrecy of past message even if the device key is compromised
- The protocols are configured to suit metering application
  - As all PLC nodes are managed by one entity, compatibility modes and algorithms can be left out, reducing implementation complexity
  - When negotiating the algorithms to use, only one choice is proposed
  - The certificates are tailored to include only necessary extensions

# Work status and expected impact

## Work is still in progress

- All the preliminary work has been performed
- All the layers of the communication stack have been implemented
- Remaining work:
  - Implementation of the use-cases and simulation scenarios;
  - Confrontation of simulated physical transfer functions to real field data;
  - Validation of the communication stack dynamic.
- Trialog is expecting to complete this work end of year 2016

# Work status and expected impact

## Expected results and impact

- Results will show which security protocol offer the best performances, depending on the use-cases and network topology
- These results will help the DSOs and their suppliers to choose the best cyber-security solution according to their requirements

- The developed simulator may also be used in the future for other studies:
  - Scope other than smart metering
  - Feasibility of use-cases, for specific use-cases or network topology
  - Establishing devices minimal unitary performances required to fulfil system performances requirements

# Thank you for your attention

olivier.genest@trialog.com