An innovative G3-PLC simulator: application to the comparison of network performances between several cyber-security protocols and mechanisms in a smart metering system

Nicolas ANGLADE[(1)], Cyril GREPET[(1)], Olivier GENEST[(1)], Vincent MAURY[(1)], Alain MOREAU[(1)]

[(1)] TRIALOG, 25 rue du Général Foy, 75008 Paris, France, e-mail: firstname.lastname@trialog.com

Abstract

TRIALOG has developed a G3-PLC simulator, based on ns-3. This simulator has been used to perform a comparison of network performances between several cyber-security protocols and mechanisms in a smart metering system. Four reference distribution networks, six smart metering use-cases and three metrics have been modelled in the simulator to compare three cyber-security protocols (IPSec, DTLS and DLMS/COSEM).

The expected result of this study is to show which security protocols and mechanisms perform the best on a G3-PLC-based AMI, depending on the required use-cases and on the distribution network topology. At the end, it will help the DSOs and their suppliers to choose the best cyber-security protocol depending on their requirements.

Index Terms

PLC, G3-PLC, Simulation, NS-3, Cyber-security, Smart metering, IPSec, DTLS, DLMS/COSEM.

I. CONTEXT AND OBJECTIVE OF THE STUDY

MANY Advanced Metering Infrastructures (AMI), designed to offer remote management and reading of smart electricity meters, are emerging all around the globe. The presence of smart meters within houses raises a great amount of fears among the public regarding their hacking: over-billing, remote power cut, but also privacy issues. Distribution System Operators (DSO), in charge of smart metering, need thus to ensure the security of communications between the smart meters and their central information system, notably authentication and data ciphering. But in addition to allaying public concerns, security is also obviously required by the DSO for their own management of the AMI.

Many DSO have chosen Power Line Communications (PLC) as a cost-effective technology for the last-mile segment, corresponding to the communication between the Data Concentrator (DC) and the smart meters. In several projects (such as those conducted by Enedis, Creos and Ores), the communication stack is based on G3-PLC [1], IPv6, UDP, and DLMS/COSEM [2] layers. In such a stack, cyber-security mechanisms may be implemented at different layers.

TRIALOG is currently running a study aiming to compare the performances of 3 cyber-security solutions, offering the same level of cyber-security, in the scope of a G3-PLC-based smart metering system. This study is being performed using TRIALOG's G3 PLC communication network simulator. The methodology, the work status and the expected impact are presented in this paper.

II. SIMULATION

A. Simulation framework

TRIALOG's G3 PLC simulator is based on Network-Simulator 3 (ns-3) and simulates all Open Systems Interconnection (OSI) model layers, that is, covers both physical and network aspects. It has actually been developed as a module for the ns-3 simulator.

It is based on ns-3 PLC module (as described in [3]) for physical layer simulation. On top of that, a full metering stack has been implemented, including G3-PLC, IPv6, UDP and DLMS/COSEM. Security protocols and mechanisms such as IPSec, DTLS and DLMS/COSEM security have been implemented in the simulator.

B. Physical layer simulation

This simulator allows to define an electricity network, either graphically or through script writing, by specifying and positioning cables, loads and communication nodes. Several physical distribution network topologies can thus be configured, to represent situations such as high-rise buildings, dense urban areas with blocks, suburban houses, rural environments, etc.

For each load or node, PLC characteristics such as impedance and noise have to be specified, including their variations over both time and frequency.

The physical PLC module is then able to compute the channels transfer functions. For each PLC link, the resulting SNR is computed, leading to a probability to correctly receive and decode any frame transiting though it at any time.

C. Communication stack simulation

The communication layers (from data link layer to application layer) are implemented in the ns-3 module, in C++ language. It includes all the automated mechanisms such as network joining, bootstrapping, tone-mapping, route establishment, neighbor discovery and ping.

D. Execution time simulation

It cannot be considered that DC and meters treat incoming frames and provide answers instantaneously. Therefore, the required execution time is simulated for both DC and meters.

For security mechanisms, the computation time is simulated based on the processing power of the node:

- For the DC, it is considered to use an ARM processor (on the order of a 32 bits signle core at 800 MHz).
- For the meter, it is considered to use a smaller microcontroller (on the order of a 32 bits single core at 16 MHz).

Executions timings are defined for the following operations:

- Communication stack processing: frame routing, stack automated mechanisms, etc.
- Applicative processing: data reading, data writing, etc.
- Cyber-security computing: ciphering, authentication, etc.

III. APPLICATION TO SMART METERING

A. Distribution network modelling

Due to the important diversity of distribution networks (in terms of size, topology, length, load, density, etc.), it is not realistic to define only one topology that could be used as an universal example.

Hence, 4 topologies are modeled:

- Rural: 6 meters distributed every 50 meters on a 250m length network.
- Dense urban: 400 meters distributed over 20 buildings of 5 floors, among 4 parallel streets.
- High-rise building: 35 meters distributed over 7 floors, with an distance of 20m between the transformer substation and the building
- Residential area: 86 meters, distributed over 4 streets, with one house every 15m, and with an initial distance of 100m between the transformer substation and the first meter.

In each of these topologies, it is considered that the DC is installed in the MV/LV transformer substation, and every home is considered to have a single meter.

The effects of the homes and their devices are represented by a load, modeled by a RLC circuit, and a noise spectrum.

Depending on the cases, either the load and noise is connected directly to the meter (representing a meter inside the home) or there is a small distribution cable between the meter and the load and noise (representing a meter outside the home).

Two reference loads and noises are implemented, depending on the rural or urban character of the simulated network. These characteristics are based on several measurement campaigns performed by TRIALOG in Europe to characterize the electrical distribution network as a PLC channel.

The presence of the MV/LV transformer nearby the DC has also been modeled by a specific load, extracted from [4].

For this first approach, all previously mentioned values do not depend on time.

B. Smart metering use-cases

Several applicative use-cases are implemented:

- Metering data collection: every 15 minutes, 2 tariff indexes and 1 status register are read on each meter.
- Daily collection: every 24 hours, an end-of-billing made of 2 tariff indexes, and a load profile with 24 power points is read on each meter.
- Alarm reporting: in case of specific event on meter side, an alarm is raised (i.e. a packet containing an alarm code is sent by the meter application to the DC).
- Breaker control: upon request, the DC sends an order to control the breaker to a specific meter.
- Contract setup: upon request, the DC sends a tariff calendar to a specific meter, including day profiles, seasons

and special days.

- Firmware upgrade: upon request, the DC sends a firmware of about 200 kB to a specific meter.

Theses applicative uses-cases are implemented on meter side and on DC side, and their triggering is defined in the simulation scenario.

C. Metrics

In order to compare the simulations, the following metrics are used:

- Percentage of achieved applicative use-cases: this metric shows if all the applicative use-cases were successfully completed.
- Total time needed to execute the applicative use-cases: this metric shows the total amount of time required to execute the applicative use cases (including the PLC transmission time but also the processing time).
- Total PLC time needed to execute the applicative use-cases: this metric shows the amount of time needed to execute the applicative use-cases, only from a PLC point of view, regardless the processing time of the devices.

IV. CYBER-SECURITY PROTOCOLS COMPARISON

A. Smart metering cyber-security requirements

Cyber-security requirements are strong in smart metering systems, as sensitive data are being manipulated and meters are remotely controlled. Therefore, all the key requirements of cyber-security are applicable to AMI: confidentiality, integrity, authentication and non-repudiation.

In particular, having a group security for network access control, such as the one offered by G3-PLC, is not sufficient to ensure proper confidentiality between the meters. As a consequence, end-to-end individual cyber-security is required.

B. Selection of relevant protocols

As mentioned in part I, the studied smart metering stack is made of G3-PLC [1], IPv6, UDP, and DLMS/COSEM [2] layers.

In such a stack, cyber-security protocols may be implemented at different layers, such as IPSec at network layer, DTLS at session layer, or DLMS/COSEM security mechanisms at application layer.

All these 3 solutions offer cyber-security services in-line with the requirements.

C. Protocols modelling

The cyber-security protocols and mechanisms are all modeled in the same way, by focusing on the following characteristics:

- Handshake: number and size of the frames exchanged during handshake.
- Overhead: number of bytes added to each packet.
- Encryption time: amount of time required to compute the security algorithm. Different values are defined for DC and meter as their hardware architectures are not the same.

D. Network status

Three types of network status are used for the initial state of the simulation:

- a restarting PLC network (following a power outage for example), where every PLC device is restarting and need to execute the bootstrapping, routing and security procedures in order to be accessible;
- a stable PLC network, in a “permanent regime” (all bootstrapping procedure steps have already been performed by all present meters, routing tables are also filled so that every meter knows the route towards the DC and security establishment have been executed);
- a stable PLC network (as described above) with the addition of a single new node at the start of simulation.

Once the simulation is started, the network status will evolve automatically based on the mechanisms (routing, bootstrap, association opening, etc.) invoked by the PLC nodes.

V. WORK STATUS AND EXPECTED IMPACT

A. Work status

Thus far, all the preliminary works have been performed, in particular the definition of the characteristics of the modeled distribution networks, protocols and use-cases, and the choice of the metrics. Also, all the layers of the communication stack have been implemented.

The remaining work mostly deals with the finalization, integration and validation of the G3-PLC simulator:

- 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 from now until end of year 2016.

B. *Expected results and impact*

The expected results will show which security protocols and mechanisms perform the best on a G3-PLC-based AMI, depending on the required use-cases and on the distribution network topology.

These results will help the Distribution System Operators (DSO) and their suppliers to choose the right cyber-security protocols and mechanisms to use in their communication profile, in order to fulfill the security requirements without harmfully impacting the performances of the network.

The developed simulator may also be used in the future to perform other performance studies of G3-PLC networks, not limited to smart metering, for example to evaluate the feasibility of use-cases or to establish the devices minimal unitary performance required to fulfil system overall performance criteria.

REFERENCES

[1] ITU-T G.9903, “Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks”, February 2014

[2] IEC 62056-5-3:2013, “DLMS/COSEM application layer”, June 2013

[3] F. Aalamifar, A. Schlögl, D. Harris and L. Lampe, “Modelling Power Line Communication Using Network Simulator-3”, 2013 IEEE Global Communications Conference (GLOBECOM)

[4] M. Arzberger, K. Dostert, T. Waldeck and M. Zimmermann, "Fundamental Properties of the Low Voltage Power Distribution Grid," Institute of Industrial Information Systems, Karlsruhe, 1997