Susceptibility of Power Line Communication (PLC) Channel to DS, AM and Jamming Intentional Electromagnetic Interferences

Authors: [1]Arash Nateghi,
Electromagnetic Effects and HPEM
Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS)
Munster, Germany
nateghi@geml.uni-hannover.de

[2]Martin Schaarschmidt, [3]Sven Fisahn
Electromagnetic Effects and HPEM Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS)
Munster, Germany
{MartinSchaarschmidt, SvenFisahn}@bundeswehr.org

Co-author: Heyno Garbe
Institute of Electrical Engineering and Measurement Technology
Leibniz Universität Hannover
Hannover, Germany
garbe@geml.uni-hannover.de

Abstract— The use of power lines as a communication channel for transferring data between communication devices for power systems in smart grid communication systems is growing rapidly. This paper describes three different types of methods for radiating and conducting Intentional Electromagnetic Interference signals: Amplitude Modulated, Damped Sinusoidal and Sweep Frequency Jamming Signals. The severity of all three types of IEMI signals on a power line communication channel using a single phase of a three-phase, low-voltage power distribution board is compared. The method for measuring interference is then explained and the influence of radiated and conducted interferences on data transmission is assessed. After discussing the IEEE 1901 power line communication channel's vulnerability to IEMI, this article explains the need for a systematic risk-based approach, in coalition with the rules-based perspective, to mitigate its impact.

Keywords — IEMI, Power Line Communication, PLC, EMI measurement methods, Smart-Grid communication, AM, DS, Sweep Frequency Jamming signal, risk-based approach.

I. INTRODUCTION

One of the key aspects of the smart grid infrastructure is to include a system that is decentralised from the national power grid in order to work independently and that can also communicate with other local decentralised networks to compensate for energy shortages or to donate the generated electricity surplus. With the latest technology from providers of smart grid communication solutions such as Siemens[1] and ABB[2], the Power Line Communication PLC can transmit data with overhead lines or underground lines with variable channel bandwidths from 2 to 256 kHz and up to 2 Mbps per transmission direction [1].

The PLC network is also used in buildings to reduce the material and installation costs of the communication network and to provide flexibility and faster data communication of up to 1200 Mbps compared to wireless communication. Two dLAN 200 AVplus PLC adapters [2] are used for this experiment, which can be connected to the power socket in the building and establish a communication network connection with channel bandwidth of 2 to 28 MHz and a data rate of up to 200 Mbps via single-phase Low Voltage (LV) 240 V wiring.

Previously described PLC technologies used in power grids and smart buildings use the same concept of data transmission over power lines and are all subject to Intentional Electromagnetic Interference (IEMI), especially those considered part of critical infrastructures.

The susceptibility of Static Digital Energy Meters SDEMs to electromagnetic interference from electromagnetic switches and power line telecommunications was examined in [3]. The results show that SDEMs are immune to this type of interference. The immunity of the energy meter using a PLC in disturbed LV networks was assessed in [4] after considering five different types of environmental electromagnetic interference (EMI) caused by the power line.

In this article, however, the focus is on generating three different types of IEMI signals: Amplitude Modulated (AM), Damped Sinusoidal (DS), and Sweep Frequency Jamming (SFJ). On the one hand, to assess the susceptibility of the PLC channel itself to IEMI via emitted and also conducted signal propagation and, on the other hand, to compare the interference strength of all three types of the above-mentioned IEMIs.

II. RELATED WORK

Designing and creating a source of interference that disrupts the PLC channel requires little expertise. As a result, deliberate attackers are prone to intentional interference, especially when the communication channel of a critical infrastructure such as a smart grid is interrupted.

dLAN 200 AVplus PLC adapter using MCM technology (Multi-Carrier Modulation) by dividing the data stream into several bit streams with a total bandwidth of 2 to 28 MHz, as shown in Figure 1.

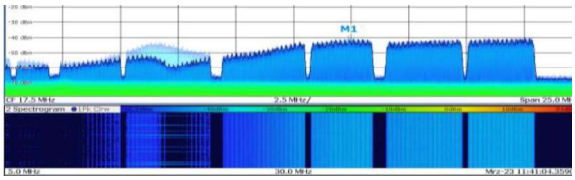

Figure 1. dLAN 200 AVplus PLC Multi-Carrier Modulation.

This section describes all three types of IEMI signals (AM, DS, and SFJ).

A. Sweep Frequency Jamming signal

Grecia Romero [5] used low-power commercial jammers as a source of Intentional Electromagnetic Interference (IEMI) to interfere with communications equipment commonly used in the transportation sector. A similar technique is used to perturb the PLC channel by using a capacitive coupler to conduct and a single wire to radiate the IEMI signal, which are discussed in more detail in the following sections of this paper.

Digital Network communication jamming methods, including SFJ, are explained in [6]. SFJ is one the most common methods of jamming the communication channel by covering the bandwidth of communication channel. The FSJ in this experiment uses a frequency range of 2 to 28 MHz and the mathematical model of the SFJ signal is given in Equations (1) and (2).

$$i(t) = I\cos(2\pi f(t)t), \quad 0 < t < SP \tag{1}$$

$$f_i(t) = \frac{d}{dt}[f(t)t] = \frac{f_2 - f_1}{SP}t + f_1\,, \tag{2}$$

where; $f_1 = 2$ MHz , $f_2 = 28$ MHz And SP = sweep period.

[1] https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/smart-communications/powerline-carrier-power-link.html
[2] https://library.e.abb.com/public/204088346e0545838b5599bdd7ebdfe6/896_ETL600_2011_low.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska- Curie grant agreement No 812790.

For this experiment, the SP values of the interference signal in Eq. (1) are chosen to be 20 µs and 80 µs to have a random range of SPs, rather than targeting the actual time interval given in Equations (3) and (4) below.

$$\Delta f = \frac{\text{Bandwidth}}{\text{IFFT lenght}} = \frac{26\text{MHz}}{64} = 604.25\ \text{kHz} \quad (3)$$

$$\Delta f = \frac{1}{T_u} \rightarrow T_u = 2.46\ \mu s \quad (4)$$

One of the SFJ signal with SP =20 µs is plotted by Matlab and shown in Figure 2.

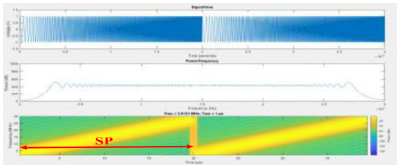

Figure 2. Total frequency bandwidth sweep frequency jamming signal.

Moreover, after measuring the carrier frequency of each individual data stream and its bandwidth, a pulsed type of jamming signal was generated in order to compare the interfering effects with the previously defined jamming signal. For the PLC channel of the dLAN 200 AVplus there are nine frequency subdivisions with predefined centre frequencies (f_{cs} = 2.7, 4.6, 6.15, 8.65, 12, 16.15, 19.5, 23.15 and 26.45 MHz). Three sweep period values are also selected at random: 20 µs, 40 µs and 80 µs. One of the jamming signals and its related FFT are plotted by Matlab and shown in Figure 3.

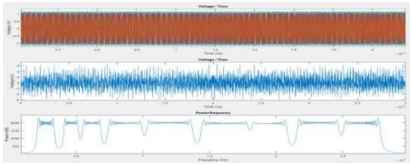

Figure 3. Pulsed sweep frequency jamming signal.

B. Amplitude Modulated signal

Mathematical equation for amplitude modulated signal is given below in Eq. (5).

$$i(t) = A_c\cos(2\pi f_c.t) + A_m\cos(2\pi f_m.t)\cos(2\pi f_c.t) \quad (5)$$

where; f_m: modulation frequency, f_c: carrier frequency

Am: modulation amplitude , Ac: carrier amplitude

AM signal is generated by using Matlab and shown in Figure 4. The left diagram shows the AM signal and the right diagram shows the addition of nine AM signals with the centre frequencies specified in Section II.A.

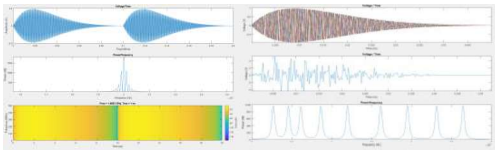

Figure 4. Ampitude Mudulated and pulsed AM signals.

C. Damped Sinusoidal signal

The mathematical equation for the damped sinusoidal signal is given below in Eq. (6).

$$i(t) = I * e^{-\lambda t}\text{Sin}(2\pi ft) \quad (6)$$

where; λ: decay constant

The DS signal in Figure 5 is generated using Matlab. The diagram on the left shows the DS signal and the diagram on the right shows the addition of nine DS signals with the centre frequencies specified in Section II.A.

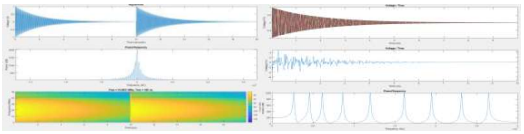

Figure 5. Damped Sinusoidal and pulsed DS signals.

III. Consumer Unit and PLC Modems

As shown in Figure 6, two PLC modems are connected to a single phase socket on the power distribution test board, and an Ethernet cable from each modem is connected to two separate PCs. The associated application shows the connectivity of the modems and the data rate capability of the PLC channel. It is important to connect all modems to the same circuit while sharing the network for a better data transfer rate.

Figure 6. Consumer unit, PLC modems and associated application.

IV. Measurement Setup

This section describes the test tools to demonstrate the IEMI signals defined in the previous sections, and measurement devices to monitor and analyse the PLC network performance. The general layout of the test and measurement setup for performing the conducted IEMI on the PLC channel is shown in Figure 7.

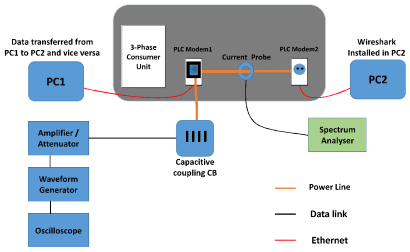

Figure 7. Method of measurement setup layout for conducted IEMI.

The general layout of the test and measurement setup for IEMI radiation on the PLC channel is shown in Figure 8.

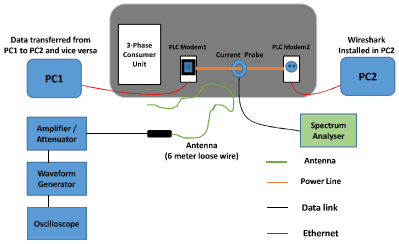

Figure 8. Method of measurement setup layout for radiated IEMI.

The test arrangements are carried out in a room in which the PLC modem functions as in an actual situation.

In Figures 7 and 8, PC1 and PC2 are connected to each of the PLC modems, which are plugged into a socket on the same

circuit and share data and files over the PLC channel. The IEMI signal is generated using arbitrary waveform generator and the signal amplitude is amplified by 0%, 50% and 100% amplification of the 100 W maximum power of the high frequency EMC power amplifier. The oscilloscope is used to confirm the properties of the IEMI signal generated by the waveform generator. A FCC current probe is used in conjunction with a spectrum analyser to measure the signal flowing through the power line conductor. In Fig. 7, a capacitive coupling board is used to block the DC signal and couple the AC signal of the conducted IEMI into the power line conductor. In Figure 8, a six meter long single wire is used to emit the IEMI signals predefined in the previous section and to interfere with the PLC channel. The reason for using a single cable instead of a verified antenna for the IEMI radiation is to assess the vulnerability of the PLC channel even with a low-tech signal emitter that doesn't require expert knowledge to build.

A. Packet transfer rate monitor

During the twenty-second conduction and radiation of AM, DS and SFJ interference signals to the PLC network, Wireshark records information about the transmission rate of data packets[3]. Wireshark's statistics tool can be used to analyse all the different protocols such as the transmission control protocol (TCP), the server message block (SMB) and the IPv6 of the transmitted signal.

B. Interference to Signal Ratio

The frequency spectrum analyser in the frequency range from 2.0 Hz to 26.5 GHz is used to monitor the conducted and radiated interference signal power quantity P_I and the conducted signal power magnitude P_S of the PLC channel. Then Interference to Signal power Ratio ISR is determined from below equation (7).

$$\text{ISR} = 100 * \left(\frac{2P_S - P_I}{P_S}\right) \% \qquad (7)$$

For example, Figure 9 shows that all of the actual signal is covered after the conducted SFJ signal is applied. In this case, the actual magnitude of the power spectrum of the communication signal before the distortion is P_S = -54.60 dBm and the magnitude of the interference signal P_I = -33.36 dBm.

From Eq. (7), $\text{ISR} = 100 * \left(\frac{2*(-54.60)-(-33.36)}{-54.60}\right) = 138.9\%$.

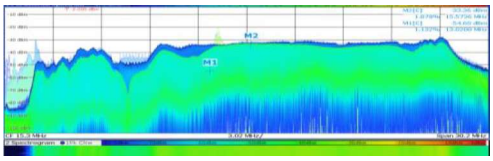

Figure 9. Spectrum analyser to display the P_I coveres P_S totally.

This is a high percentage of the power spectrum coverage of the SFJ signal (almost 39% more than the power of the actual signal), which completely distorts the PLC network connection between PC1 and PC2.

V. Measurement Results

A total of twenty-one IEMI signals are radiated and coupled into the PLC network: three AM-pulse signals (0%, 50% and 100% amplification), three DS-pulse signals (0%, 50% and 100% amplification), six SFJ signals with overall bandwidth coverage of 2 to 28 MHz with 20 and 80 SP values (0%, 50% and 100% amplification) and nine SFJ-pulse signals with 20, 40 and 80 SP values (0%, 50% and 100% amplification). All IEMI signals are applied for a period of 20 seconds and the average of the data packets transmitted via a PLC network is recorded with Wireshark. In addition, the ISR% is derived from Eq. 7 in the previous section. The results of the ISR% coverage and the data packet transmission rate for the conducted IEMI signals to the PLC channel are shown in Figure 10.

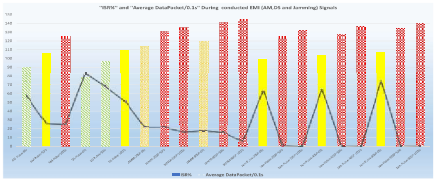

Figure 10. "ISR%" and "Average DataPacket/0.1s" during conducted EMI (AM, DS and SFJ) Signals.

The results of the ISR% coverage and the data packet transmission rate for the radiated IEMI signals to the PLC channel are shown in Figure 11.

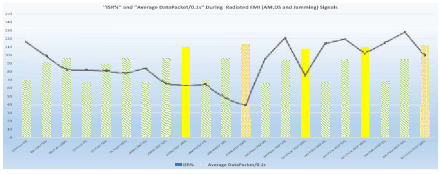

Figure 11. "ISR%" and "Average DataPacket/0.1s" During radiated EMI (AM, DS and SFJ) Signals.

ISR% is shown using a bar chart and the average-data-packet/0.1s is shown using a line graph in Figures 10 and 11. The bar charts in Figures 10 and 11 are filled with various shapes and colors that are coded to indicate the severity of the IEMI signals conducted or radiated on the PLC channel. Table 1 classifies the conducted IEMI disturbances on the PLC channel based on ISR% and observed severity of IEMI signals.

Table 1.Conducted IEMI disturbances and severity classification.

Shapes and colors	Classified severity	ISR%	IEMI Signals
Diagonal lines (white and green)	No disturbances	Bellow 100%	-AM Pulse 0% -DS Pulse 0% -DS Pulse 50%
Solid (yellow)	Data packet transfer delayed	100-110%	-AM Pulse 50% -DS Pulse 100% -Jam pulse 80SP 0% -Jam pulse 20SP 0% -Jam pulse 40SP 0%
Confetti (white and orange	Data packet transfer stopped but restored after 20s disturbances	110-120%	-JAMM 20SP 0% -JAMM 80SP 0%
Squares (white and red)	Complete disconnection and zero data transfer	Above 120%	-AM Pulse 100% -JAMM 20SP 50% -JAMM 20SP 100% -JAMM 80SP 50% -JAMM 80SP 100% -Jam pulse 20SP 50% -Jam pulse 20SP 100% -Jam pulse 40SP 50% -Jam pulse 40SP 100% -Jam pulse 80SP 50% -Jam pulse 80SP 100%

To classify the severity of conducted IEMI signals taking ISR% into account, the JAMM 20 and 80 SP values cover the greatest proportion of actual data streams. The second largest impact is the 20, 40, and 80 SP Jam-pulses in a row, which proves that increasing the SP value can distort the PLC channel more. DS-pulse signals have less disruptive effects compared to AM-pulse signals, which can be explained by their narrower frequency band compared to AM signals shown in Figures 4 and 5. Although JAMM signals have a larger ISR% compared to Jam-pulse signals, the average data packet transmission rate for Jam-pulse signals is lower. This effect can be explained by taking into account the energy distribution of the Jam-pulse signals, which focuses on the desired centre frequency rather than the overall coverage of the bandwidth shown in Figures 2 and 3. Table 2 classifies the emitted IEMI

[3] https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs

disturbances on the PLC channel based on ISR% and observed severity of IEMI signals.

Table 2. Radiated IEMI disturbances and severity classification.

Shapes and colors	Classified severity	ISR%	IEMI Signals
Diagonal lines (white and green)	No disturbances	Bellow 100%	-AM Pulse 0% -DS Pulse 0% -AM Pulse 50% -DS Pulse 50% -AM Pulse 100% -DS Pulse 100% -JAMM 20SP 0% -JAMM 80SP 0% -JAMM 20SP 50% -JAMM 80SP 50% -Jam pulse 20SP 0% -Jam pulse 20SP 50% -Jam pulse 40SP 0% -Jam pulse 40SP 50% -Jam pulse 80SP 0% -Jam pulse 80SP 50%
Solid (yellow)	Data packet transfer delayed	100-110%	-JAMM 20SP 100% -Jam pulse 20SP 100% -Jam pulse 40SP 100%
Confetti (white and orange	Data packet transfer stopped but restored after 20s disturbances	110-120%	-JAMM 80SP 100% -Jam pulse 80SP 100%

As can be seen from Table 2, JAMM 80 SP and Jam-pulse 80 SP IEMI signals with 100% amplification can only stop the data packet transmission with the greatest severity compared to other emitted IEMI signals. In addition, JAMM 20 SP Jam-pulse 20 SP and 40 SP with 100% gain can only delay the data transmission in the PLC network. Figures 10 and 11 show that emitted IEMI Jam-pulse signals have a significantly lower impact on data packet transfer rate compared to conducted ones. The emitted Jam-pulse with 50% gain has a higher data packet transmission rate than the 0% gain, which in the case of a conductive Jam-pulse signal with 50% gain has a much lower data packet transmission. This can be explained by the power reflection of the single wire antenna, which reduces the overall severity of the Jam-pulse IEMI signals when 50% gain (only 12 W of amplification and 8 W of reflection) is applied in compare with 0% gain (0 W amplification and no reflection) and 100% gain (52 W amplification and 38 W reflection). Although conducted IEMI signals can interfere with the PLC channel more than radiated IEMI signals, a better designed antenna can cause even more interference compared to a six meter long wire used for this experiment.

VI. Mitigation plan

The home communications network may not be as sensitive as critical infrastructures that use the PLC channel to communicate critical signals such as telemetry and switching signals, and EMI interference on the PLC network can have a huge impact on system operation. Therefore, a mitigation plan should be implemented to protect them from deliberate EMI attacks. In the past, the IEMI risk assessment and associated mitigation plan were within the set of rules and standards. Nowadays communication and network systems are so complex and only the use of standards cannot provide solid protection against IEMI risks for these systems. In addition, the uncertainty in the EM environment has further increased the risk of interference. In order to protect the communication networks such as the PLC channel from IEMI attacks, a systematic risk-based approach is required that uses the rules-based approach as a foundation. Then, extends the activity of the risk assessment by taking into account other elements that were not previously considered such as non-technical aspects of IEMI attacks. As part of the necessary mitigation plan from IEMI risk, Frank Sabath introduced a systematic risk assessment method called TSECA (a threat scenario and an analysis of the effects and criticality) in the following steps [7]: 1. Define the threat scenario, 2. Construct scenario interaction model and system structure model, 3. Determine effects and failure modes, 4. Evaluate each effect and failure mode and assign a severity classification category, 5. Identify failure detection and threat warning methods and 6. Identify corrective measures for failure modes and Document analysis.

Furthermore, Probabilistic IEMI risk analysis such as fuzzy-based risk analysis are introduced in [8]. In this IEMI risk analysis approach, the probability of occurrence, the probability of breakdown-failure and environmental influences such as distance to the target system, risk level, mobility level and definition zones were taken into account.

VII. Conclusion and next work

In this work three different types of IEMI signals (DS, AM and SFJ) are modelled. Three levels of power gain 0, 50 and 100% are used as variable for all signals. Sweep Frequency Jamming signals are modelled with different SP values and different frequency bandwidth division (total bandwidth and sectional bandwidth of centre frequency of each data stream). In addition, the methods for conducting and radiating the IEMI signal and the EMI measurement are explained. Conducted and radiated disturbing signals are used to interfere with the PLC channel of two connected PCs. Next, the measurement result was analysed to determine the severity of all pre-modelled IEMI signals in the PLC network. From these measurement results and analyses, the susceptibility of the PLC channel to radiated and conducted IEMI signals was demonstrated. Ultimately, a systematic risk-based mitigation mechanism that offers stronger protection against IEMI is recommended in parallel to the rule-based approach.

The next step after this experiment is to install and configure a complex smart grid communication network, which is considered a critical infrastructure. Then test the entire system, especially the wireless and PLC communication channels, against radiated and conducted IEMI signals. And finally, a systematic risk-based IEMI assessment taking into account the technical and non-technical aspects.

VIII. References

[1] L. Lampe, A. M. Tonello und T. G. Swart, Power Line Communications: Principles, Standards and Applications from Multimedia to Smart Grid, 2 Hrsg., Chicago: John Wiley & Sons Inc, 2016.

[2] devolo.com. Accessed: May. 01, 2021. [Online]. Available: https://www.devolo.global/fileadmin/Web-Content/DE/products/eol/dlan-200-avplus/documents/en/devolo_dLAN_200_AVplus_0311_en_online.pdf.

[3] F. Leferink, C. Keyer and A. Melentjev „Static energy meter errors caused by conducted electromagnetic interference'' IEEE Electromagnetic Compatibility Magazine, Fourth Quarter 2016, vol. 5, no. 4, pp. 49-55, doi: 10.1109/MEMC.2016.7866234.

[4] B. Vallbè, J. Balcells, P. Bogónez-Franco, J. Mata and X. Gago, "Immunity of power line communications (PLC) in disturbed networks," 2011 IEEE International Symposium on Industrial Electronics, 2011, pp. 1621-1625, doi: 10.1109/ISIE.2011.5984403.

[5] Romero, Grecia „Identication of the impact mechanisms of the electromagnetic interferences on the Wi-Fi communications''. Signal and Image processing. UNIVERSITÉ DE LILLE 1SCIENCES ET TECHNOLOGIES, 2017, HAL Id: tel-01681189.

[6] al, C. Shahriar et „PHY-Layer Resiliency in OFDM Communications: A Tutorial'' IEEE Communications Surveys & Tutorials, Firstquarter 2015, vol. 17, no. 1, pp. 292-314, doi: 10.1109/COMST.2014.2349883.

[7] Sabath, F „A systematic approach for electromagnetic interference risk management'' in IEEE Electromagnetic Compatibility Magazine, Fourth Quarter 2017, vol. 6, no. 4, pp. 99-106, doi: 10.1109/MEMC.0.8272296.

[8] T. Peikert, H. Garbe and S. Potthast, "Fuzzy-Based Risk Analysis for IT-Systems and Their Infrastructure," in IEEE Transactions on Electromagnetic Compatibility, vol. 59, no. 4, pp. 1294-1301, Aug. 2017, doi: 10.1109/TEMC.2017.2682643.