Vulnerability of Wireless Smart Meter to Electromagnetic Interference Sweep Frequency Jamming Signals

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

Co-authors: [1]Martin Schaarschmidt, [2]Sven Fisahn
Electromagnetic Effects and HPEM Bundeswehr
Research Institute for Protective Technologies and
NBC Protection (WIS)
Munster, Germany
{MartinSchaarschmidt, SvenFisahn}@bundeswehr.org

[3]Heyno Garbe
Institute of Electrical Engineering and
Measurement Technology
Leibniz Universität Hannover
Hannover, Germany
garbe@geml.uni-hannover.de

***Abstract*— The installation and use of smart home technology that uses wireless communication channels, according to the 802.11 standard series, is rapidly increasing. This article discusses the effect of Electromagnetic Interference Sweep Frequency Jamming Signal applied to a wireless smart meter installed in a three-phase domestic and light commercial electricity distribution board. More specifically, a method of frequency jamming signal generation technique, jamming signal radiation and its interference measurements method are explained in this paper. Then, the impact of disturbances are discussed and mitigation mechanisms such as construction material shielding, digital filtering and a systematic approach of electromagnetic risk assessment are given.**

Keywords — Jamming, Smart meter, Sweep frequency jamming, EMI measurement methods.

I. Introduction

In a low-voltage (240-400 V) power distribution system, smart home metering devices can read the voltage and current of each phase of a three-phase consumer unit and then display active power, reactive power as well as the power factor of each phase remotely [1]. These measurements can be used internally or sent to a Supervisory Control and Data Acquisition (SCADA) engineer of the local Distribution System Operator (DSO) to operate the system more efficiently. Other features of these smart devices are their switching capabilities. The importance of smart meters and their widespread use in Europe are described in more detail in several sections of the European Commission publications [2].

The network standards IEEE 802.11n and IEEE 802.3 are used for wireless and Ethernet communication by smart meters in order to control the circuit in addition to monitor and record the measurement results.

After the old electricity meters were replaced with Static Digital Energy Meters SDEMs, energy consumption costs and consumer complaints increased due to misinterpretation of electricity utilization. Subsequently, in [3] the susceptibility of SDEMs to conducted Electromagnetic Interference EMI via power electronic switches and power line telecommunication was examined. The results show that SDEMs are immune to this type of interferences.

However, the vulnerability of smart meters that use a Wi-Fi communication channel to EMI radiation has not yet been assessed in the past. This article describes the method for measuring EMI radiation on the smart meter's wireless communication channel and the associated plan for mitigating related disturbances.

II. Related Work

Designing and building an interference source that disturbs Wi-Fi signal requires only a low level of expertise, making intentional attackers prone to deliberate interference, especially if they interfere with the switching states (on or off) of circuit breakers CBs.

Furthermore, Grecia Romero used commercial low-power jammers as a source of intentional electromagnetic interference (IEMI) to disrupt commonly used wireless communication devices in the transportation sector [4]. A similar method is used to jam the smart meter's Wi-Fi signal in the next section of this report. Also, the average percentage of disturbing signal power which cover the actual signal, between the access point (AP) and the Client (smart meter reading platform), will be discussed in more detail in the following divisions.

A. Sweep period and jamming signal

Wireless Network communication jamming methods, including sweep frequency jamming period SFJP, are explained in [5]. SFJP is one the most common methods of jamming the Wi-Fi signal by covering the bandwidth of communication channel. The SFJP in this experiment uses a frequency range of 2.4 to 2.5 GHz and the mathematical model of the SFJ signal is given in Equations (1) and (2) below.

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

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

where; f_1 = 2.4 GHz , f_2 = 2.5 GHz And SP = sweep period.

The IEEE 802.11n physical layer is the interface between the wireless medium and the MAC layer. Due to the use of orthogonal frequency division multiplex OFDM, it can be operated in both 2.4 GHz and 5.0 GHz frequency bands with a very variable data rate of 65 Mbit/s to 600 Mbit/s [4].

The OFDM symbol duration T_u is specified between 4 µs to 3.6 µs according to the physical layer specification of the IEEE 802.11n standard [6]. For the 20.0 MHz bandwidth of 2.4 GHz frequency band, the IFFT length is equal to 64 and subcarrier spacing (Δf) of OFDM, which is a useful part of the OFDM, given by the following Equations (3) and (4).

$$\Delta f = \frac{\text{Bandwidth}}{\text{IFFT lenght}} = \frac{20\text{MHz}}{64} = 312.5\ \text{kHz} \tag{3}$$

$$\Delta f = \frac{1}{T_u}\ \rightarrow\ T_u = 3.2\ \mu\text{s} \tag{4}$$

For this experiment the sweep period SP values of the jamming signal in Eq. (1) are selected in the range of 0.45 µs and 50 µs. The SP values are selected in ten step values from 50 µs to 10 µs. From less than 10 µs to 0.45µs, the SP values are the product of T_u=3.2 µs (from Eq. (4)) and each one of 2, 1.7, 0.5, 1/3, 1/4, 1/5, 1/6, and 1/7 values [4]. (All thirteen SP values are; 50, 40, 30, 20, 10, 6.4, 5.5, 1.6, 1.06, 0.8, 0.64, 0.53, 0.45)

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.

One of the sweep periods (SP=10 µs) and its jamming signal are plotted by Matlab, as can be seen in Figure 1.

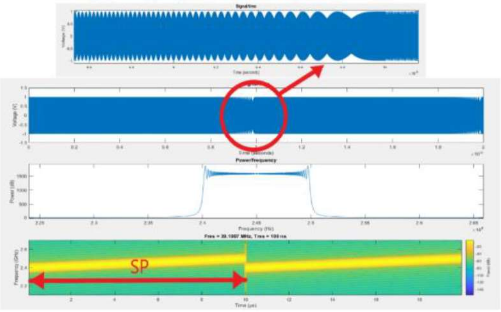


Figure 1. Sweep frequency and jamming signal.

B. *Matlab Code*

The mathematical model from Eqs. (1) and (2) is written on the Matlab platform and the code is provided below in Table 1.

Table 1 Matlab code for jamming signal, FFT and sweep period.

Jammed signal (V/time)	Fs=1e10;
	tf=10e-6;
	n = 2;
	t1 = (0 : 1/Fs : tf-1/Fs);
	t = (0 : 1/Fs : n*tf-1/Fs);
	f1 = 2.4e9;
	f2 = 2.5e9;
	SLOPE = (f2-f1)./(2*tf);
	F = f1 + SLOPE .* t1;
	y1=1 * cos(2*pi*F.*t1);
	y = repmat(y1,[1,n]);
	figure; subplot(3,1,1);
	plot(t,y);xlabel('Time(seconds)')
	ylabel('Voltage(V)') title('Signal/time');
	axis([0 n*tf -1.5 1.5]);

FFT (Power/Freq)	fy=fft(y1);
	Freq = (0 : 1/tf : Fs);
	subplot(3,1,2)
	plot(Freq(1:end/2), abs(fy(1:end/2)))
	xlabel('Frequency (Hz)')
	ylabel('Power (dB)')
	title('Power/frequency')

Sweep Period (Freq/time)	subplot(3,1,3) pspectrum(y,Fs,'spectrogram', ...'FrequencyLimits', [2.1e9 2.7e9], 'TimeResolution', 0.0000001, 'OverlapPercent',99, 'Leakage',0.85);

III. Smart Meter and Consumer Unit

The three-phase distribution board, installed smart meter and related graphical user interface (GUI) that works for the defined IP address are illustrated below in Figure 2.

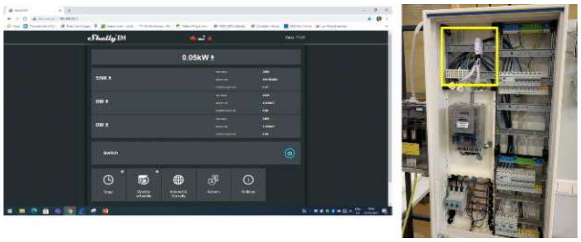


Figure 2. Consumer unit, smart meter and related GUI.

As shown in Figure 2, a current transformer is connected for each phase of three phases and from the main bus-bar three cables are connected to the internal voltage transformer of the smart meter. The smart meter can communicate directly with other Wi-Fi devices through HTTP protocol which allows remote control of electric appliances through mobile phone, PC or building automation system [1].

IV. Measurement method

This section describes the test tools and measurement devices to measure IEEE 802.11n network performance. The general layout of the measurement setup is shown in Figure 3.

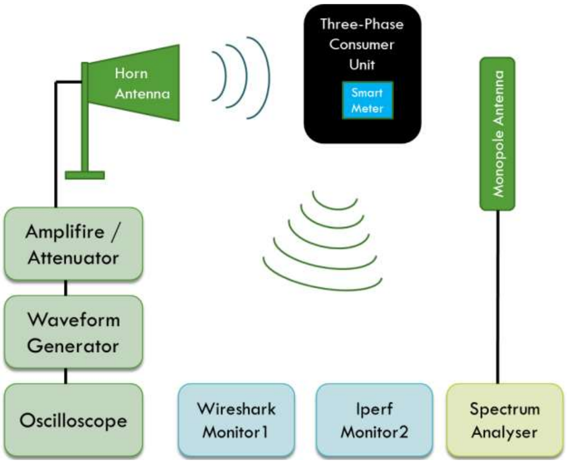
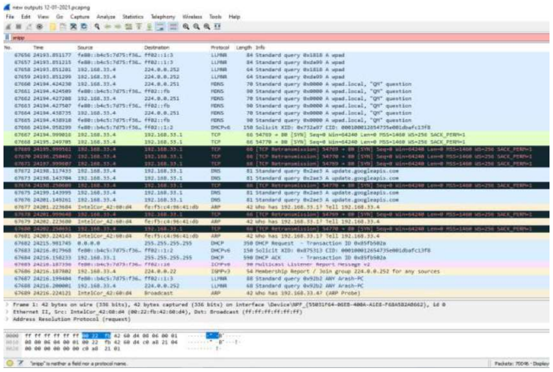


Figure 3. Method of measurement setup layout.

A. *Network performance monitor*

Wireshark is a platform for a more detailed analysis of network packets [7]. After the interference signal is applied to the 802.11n network, information about data packets is recorded with Wireshark in the first PC and displayed. Wireshark uses colours to identify different types of traffic in a snapshot. In Figure 4 below, the TCP traffic is light purple, the UDP traffic is light blue, and packets with fatal errors are black, meaning they were not delivered properly.


new outputs 12-01-2021.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
snipp

```
No.   Time            Source                Destination      Protocol Length Info
67656 24193.851177    fe80::b4c5:7d75:f36.. ff02::1:3        LLMNR    84 Standard query 0x1818 A wpad
67657 24193.851215    fe80::b4c5:7d75:f36.. ff02::1:3        LLMNR    84 Standard query 0xda99 A wpad
67658 24193.851281    192.168.33.4          224.0.0.252      LLMNR    64 Standard query 0x1818 A wpad
67659 24193.851299    192.168.33.4          224.0.0.252      LLMNR    64 Standard query 0xda99 A wpad
67660 24194.424230    192.168.33.4          224.0.0.251      MDNS     70 Standard query 0x0000 A wpad.local, "QM" question
67661 24194.424509    fe80::b4c5:7d75:f36.. ff02::fb         MDNS     90 Standard query 0x0000 A wpad.local, "QM" question
67662 24194.427288    192.168.33.4          224.0.0.251      MDNS     70 Standard query 0x0000 A wpad.local, "QM" question
67663 24194.427507    fe80::b4c5:7d75:f36.. ff02::fb         MDNS     90 Standard query 0x0000 A wpad.local, "QM" question
67664 24194.438735    192.168.33.4          224.0.0.251      MDNS     70 Standard query 0x0000 A wpad.local, "QM" question
67665 24194.438918    fe80::b4c5:7d75:f36.. ff02::fb         MDNS     90 Standard query 0x0000 A wpad.local, "QM" question
67666 24194.958299    fe80::b4c5:7d75:f36.. ff02::1:2        DHCPv6   150 Solicit XID: 0x732a97 CID: 000100012654735e001dbafc13f8
67667 24194.999018    192.168.33.4          192.168.33.1     TCP      66 54769 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67668 24195.249705    192.168.33.4          192.168.33.1     TCP      66 54770 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67669 24195.999161    192.168.33.4          192.168.33.1     TCP      66 [TCP Retransmission] 54769 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67670 24196.250402    192.168.33.4          192.168.33.1     TCP      66 [TCP Retransmission] 54770 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67671 24197.999607    192.168.33.4          192.168.33.1     TCP      66 [TCP Retransmission] 54769 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67672 24198.117433    192.168.33.4          192.168.33.1     DNS      81 Standard query 0x2ae5 A update.googleapis.com
67673 24198.143704    192.168.33.4          192.168.33.1     DNS      81 Standard query 0x2ae5 A update.googleapis.com
67674 24198.250600    192.168.33.4          192.168.33.1     TCP      66 [TCP Retransmission] 54770 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67675 24199.143995    192.168.33.4          192.168.33.1     DNS      81 Standard query 0x2ae5 A update.googleapis.com
67676 24201.149261    192.168.33.4          192.168.33.1     DNS      81 Standard query 0x2ae5 A update.googleapis.com
67677 24201.223604    IntelCor_42:60:d4     fe:f5:c4:96:41:db ARP     42 Who has 192.168.33.1? Tell 192.168.33.4
67678 24201.999640    192.168.33.4          192.168.33.1     TCP      66 [TCP Retransmission] 54769 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67679 24202.223600    IntelCor_42:60:d4     fe:f5:c4:96:41:db ARP     42 Who has 192.168.33.1? Tell 192.168.33.4
67680 24202.250651    192.168.33.4          192.168.33.1     TCP      66 [TCP Retransmission] 54770 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
67681 24203.224143    IntelCor_42:60:d4     fe:f5:c4:96:41:db ARP     42 Who has 192.168.33.1? Tell 192.168.33.4
67682 24215.981745    0.0.0.0               255.255.255.255  DHCP     350 DHCP Request  - Transaction ID 0x85fb582a
67683 24216.017968    fe80::b4c5:7d75:f36.. ff02::1:2        DHCPv6   150 Solicit XID: 0x875313 CID: 000100012654735e001dbafc13f8
67684 24216.158233    192.168.33.1          255.255.255.255  DHCP     590 DHCP ACK      - Transaction ID 0x85fb582a
67685 24216.187350    fe80::b4c5:7d75:f36.. ff02::16         ICMPv6   90 Multicast Listener Report Message v2
67686 24216.187802    192.168.33.4          224.0.0.22       IGMPv3   54 Membership Report / Join group 224.0.0.252 for any sources
67687 24216.199404    fe80::b4c5:7d75:f36.. ff02::1:3        LLMNR    88 Standard query 0x92b2 ANY Arash-PC
67688 24216.200001    192.168.33.4          224.0.0.252      LLMNR    68 Standard query 0x92b2 ANY Arash-PC
67689 24216.224121    IntelCor_42:60:d4     Broadcast        ARP      42 Who has 192.168.33.4? (ARP Probe)

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{55031f64-06E8-400A-A1E8-F68A5B2A0602}, id 0
> Ethernet II, Src: IntelCor_42:60:d4 (00:22:fb:42:60:d4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 22 fb 42 60 d4 08 06 00 01
0010  08 00 06 04 00 01 00 22 fb 42 60 d4 c0 a8 21 04
0020  00 00 00 00 00 00 c0 a8 21 01

"snipp" is neither a field nor a protocol name.          Packets: 70046 · Display
```

Figure 4. Wireshark platform in monitor 1.

B. *Data rate monitor*

The bit rate per second (date rate) can be monitored with Iperf tool [8]. For this experiment, the data rate of the specified server is measured with a duration of 20 seconds. The data is transferred between the smart meter (AP) and the second PC (the Client) while the Iperf is running on a related Java platform (see Figure 5).

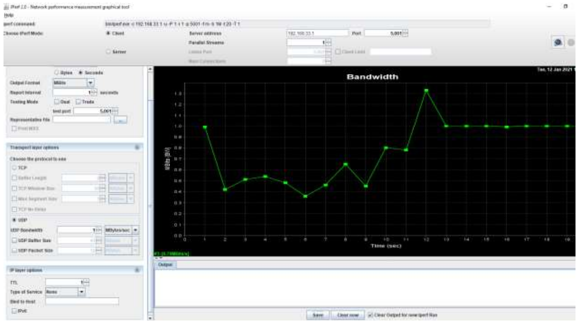


Figure 5. Iperf with its related Java platform in monitor 2.

C. Spectrum Analyser

The frequency power spectrum of the 802.11n network can be monitored by using the frequency spectrum analyser (Rohde & Schwarz FSW26) in the frequency range from 2.0 Hz to 26.5 GHz. The Interference signal power magnitude P_I and wireless signal power magnitude P_S can be measured by this analyser. Then Interference to Signal power Ratio ISR is calculated from below equation (5).

$$ISR = 100 * (\frac{2P_S - P_I}{P_S})\ \% \qquad (5)$$

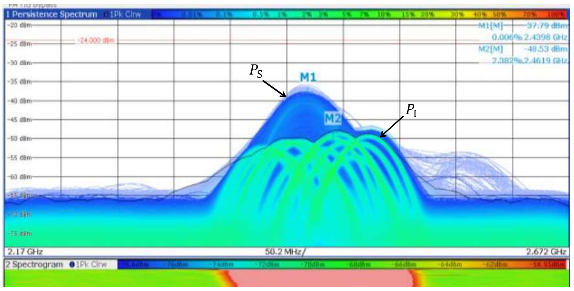


Figure 6. Spectrum analyser showing the partial coverage of P_S by P_I.

As shown in Figure 6, much of the actual signal is covered (distorted) by the interfering signal. In this case, the actual magnitude of the power spectrum of Wi-Fi signal before distortion is Ps = -37.79 dBm and the magnitude of the interference jamming signal is P_I = -48.5 dBm.

From Eq. (5), $ISR = 100 * (\frac{2*(-37.79)-(-48.53)}{-37.79})$ =71.57%.

This is a fairly high percentage of power spectrum coverage of interference signal that can disconnect the Wi-Fi connection between AP and the Client or interrupt the switching state of CBs controlled by installed smart meter.

D. Signal Generator and Amplifire/Attenuator.

The jammed signal modelled in Section *II.B* is given to the arbitrary waveform generator (Tektronix AWG70001A) and then the high frequency EMC power amplifier (EMV 0.7 to 8.0 GHz) is used to be able to vary the power amplitude within the required level of 0 to 100%. The initial steps to amplify the power are five, from 0 to 50, and then the steps are increased to ten, from 50 to 100%.

Figure 7 shows the signal generator and amplifier preparing the interfering signal to be sent to the horn antenna in order to emit the interfering signal propagating in the laboratory environment. An additional 30 dB attenuator, which represents the attenuation between the distribution board and the antenna placed on the outside wall, is connected between the RF output of the amplifier and the horn antenna.

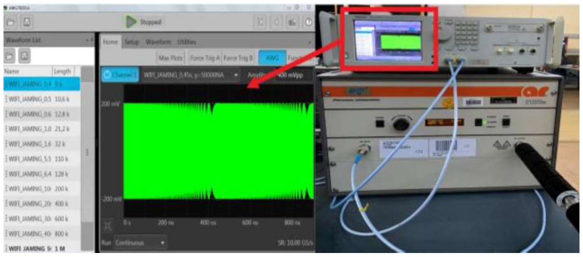


Figure 7. Waveform generator and power amplifier.

E. Anttenas

1) Horn-Antenna

The RGA-60 double ridged guide antenna (Horn Antenna) is a linearly polarized broadband antenna covering 1.0 GHz to 18.0 GHz and used for electromagnetic interferences measurements and specification compliance testing. It's used to irradiate the interfering signal and disturb the 802.11n network as it shown in Figure 8 [9].

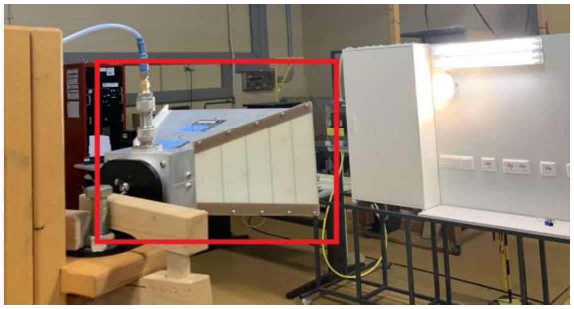


Figure 8. Horn Antenna to transmit the jamming signal.

2) High-Power OmniDirectional Antenna

A high-power omnidirectional antenna with a frequency range of a 2.0 GHz to 6.0 GHz is positioned next to the consumer unit in order to record the transmitted Wi-Fi signal before and after the applied jamming signal, as shown in Figure 9. The measured data are transmitted to the spectrum analyser for detailed analysis, as already mentioned in Section *IV.C* [10].

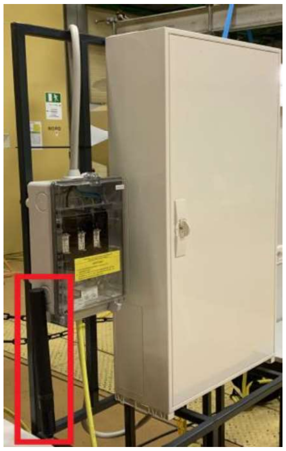


Figure 9. Omnidirectional antenna adjacent to consumer unit.

V. Measurement Results

The experimental setups are done in a room where the consumer unit is functioning like in an actual situation.

The interfering signals are radiated with the thirteen sweep periods (SPs) of 0.45 µs to 50 µs described before. For each SP, the power of the interfering signal is attenuated by the installed power amplifier from 0 to 100% in the sixteen steps mentioned earlier. For every step of SP and all the steps of power amplifications the achieved bit rate of data transfer is monitored and recorded. The results are normalised and given in below Figure 10 [11].

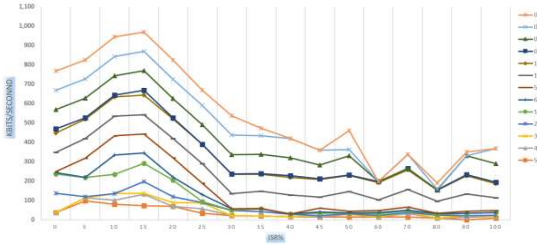


Figure 10. Bit rate ratio as a function of ISR for each SP.

From Figure 10, for SP values less than 5.5 the data rate does not drop to zero for the entire ISR range during the twenty seconds of test period. Additionally, the 15% ISR is the first critical point at which the data rate drops sharply, and the second critical point is 30% ISR, where the data rate is constantly low or reaches zero for most SP values.

Further analysis is performed for the average percentage coverage of the interference signal over the actual signal. This statistical analysis is carried out on each value of SP versus the bit rate ratio, as shown in Figure 11.

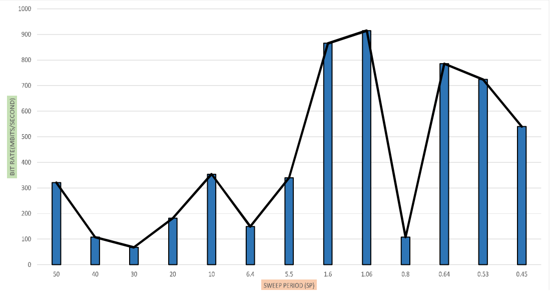


Figure 11.Average percentage of noise coverage of actual signal for each sweeping period over bit rate ratio.

As can be seen from Figure 11, apart from the 0.8 SP value, the rest of the SPs lower than 5.5 have less average noise coverage in the real signal. It means that healthier data will be transferred compared to the SPs higher than 5.5 that are altered for a longer period with a lower data transfer rate. The 0.8 SP value of the jamming signal greatly reduces the bit rate of data transmission due to the targeting of the correct frequency interval of OFDM.

The results in Figures 10 and 11 show that both factors of a higher SP values and an accurate alignment of the OFDM frequency interval with SP value of jamming signal can interfere with the Wi-Fi communication channel and distort the data transmission.

The next section describes some mechanisms that can be used to reduce the risk of the aforementioned disturbances on smart meter wireless signal.

VI. Mitigation plan

Electricity fuse boards or consumer units are installed in every domestic or light commercial premises that have access to electricity. The local electricity Distribution Network Owners (DNOs) which are responsible for providing power supply (three-phases in Germany) are willing to install their smart meters in near future.

The aim is to monitor the flow of energy in a bidirectional framework in order to improve the use of electrical energy. Also, power quality elements such as Negative Phase Sequence (NPS) and Power Factor (PF) can be monitored by the DSO SCADA engineer using dynamic readings captured by smart meters. These factors are some of the fundamental aspects of the smart grid communication system.

Moreover, residents in these properties are also installing their own smart devices that would allow them to have a better ability to control and monitor their energy use.

Apparently, most of the communication between these devices (privately-owned or DNO-owned) takes place over the Wi-Fi channel and they are all vulnerable to intentional electromagnetic interference. A mitigation plan should be implemented to protect them from all unintentional or intentional EMI attacks.

In Germany, the Federal Ministry for Security and Information [12] (Bundesamt für Sicherheit in der Informationstechnik) has introduced BSI TR-03209 - 2, Electromagnetic shielding of buildings - Practical measurements. Various types of building materials have been evaluated in this report to provide additional resistance to EM interference. This is a good start to protect and provide additional security for wireless communication channels used by smart communication devices in all energy consumers. However, the total cost of the construction of new buildings will go up and existing properties will need to be modified, which may not be feasible.

The second method that can be used to mitigate the impact of EMI on the wireless communication signal is through filtering the unwanted noise signal. Bruce DeBruhl and Patrick Tague [8] introduced a digital filtering method that eliminates the interrupting signal and reduces packet errors by 90%. Nevertheless, only one kind of signal disturbance method out of all different kinds of jamming signals introduced in [13] is explained in this report. This makes it even more complicated to design a filter to mitigate the effects of all types of signal jamming attacks.

A more systematic approach is needed to protect the Wi-Fi communication system from EMI interferences, such as jamming signal interference. Frank Sabath introduced a systematic risk assessment method (threat scenario, effects and criticality analysis (TSECA)). The TSECA risk assessment methodology defines the following steps as part of the required mitigation plan [14].

A. Define the threat scenario
B. Construct scenario interaction model and system structure model
C. Determine effects and failure modes
D. Evaluate each effect and failure mode and assign a severity classification category
E. Identify failure detection and threat warning methods
F. Identify corrective measures for failure modes
G. Document analysis

Regularly monitoring system performance is also mentioned in [14] as an important factor in eliminating the effects of the EMI interference signal.

VII. Conclusion and Next work

In this work, the modelling of the sweep frequency jamming signal is introduced. In addition, the radiation setting methods of the noise signal and the EMI measurement are explained. And then a disturbing signal is emitted to disrupt the 802.11 system network of a smart meter installed in a three-phase consumer unit. After the disturbances, the measurement result has been analysed to identify critical sweep frequencies that can disturb the OFDM of the physical layer of the wireless communication channel.

Ultimately, a few mitigation mechanisms are recommended, e.g. the use of building material that offers stronger protection against external EMI interference, the digital filtering of interfering signals and a systematic EMI risk assessment method.

Following this experiment, the goal is to install and configure a complex smart electricity grid communication network system, which is considered as a critical infrastructure. The next step is to test the entire system, especially the wireless communication channel, against radiated and conducted EMI. And finally, to apply a similar systematic EMI risk assessment including the technical and non-technical aspects of EMI risk assessments mention in the previous Section *VI*.

VIII. References

[1] Shelly.cloud. Accessed: Nov. 3, 2020. [Online]. Available: https://shelly.cloud/products/shelly-3em-smart-home-automation-energy-meter/.

[2] Smart grids and meters, European Commission, 31 July 2014 and last update 12 February 2021. Accessed: Jan. 5, 2021. [Online]. Available: https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters_en.

[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] 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.

[5] 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.

[6] IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*in IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016) , vol., no., pp.1-4379, 26 Feb 2021, doi: 10.1109/IEEESTD.2021.9363693.*

[7] www.wireshark.org. Accessed: Nov. 5, 2020. [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html.

[8] Tague, B. DeBruhl and P „Digital Filter Design for Jamming Mitigation in 802.15.4 Communication'' 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), Lahaina, HI, USA, pp.1-6, doi: 10.1109/ICCCN.2011.6006020.

[9] ELECTRO-METRICS. Instruction manual double ridged guide antenna model RGA-60, 1 GHz - 18 GHz. Accessed: Nov. 22, 2020. [Online]. Available: https://electro-metrics.com/wp-content/uploads/2017/05/RGA-60-INSTRUCTION-MANUAL.pdf.

[10] Alarisantennas.com. High-Power OmniDirectional Antenna 2 – 6 GHz. Accessed: Jan. 15, 2021. [Online]. Available: https://www.alarisantennas.com/wp-content/uploads/2020/11/DIPL-A0059-Version-2.9.pdf.

[11] I. Harjula, J. Pinola and J. Prokkola „Performance of IEEE 802.11 based WLAN devices under various jamming signals'' MILCOM 2011 Military Communications Conference, Baltimore, MD, Oulu, Finland 2011, pp. 2129-2135, doi: 10.1109/MILCOM.2011.6127635.

[12] Electromagnetic Shielding of Buildings- Patrial measurement, BSI TR-03209 - 2, April 2008. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03209/BSI-TR-03209-2.pdf.

[13] Grover, Kanika; Lim, Alvin; Yang, Qing „Jamming and anti-jamming techniques in wireless networks: a survey'' International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), 4th Nov 2014, Vol. 17, doi: 10.1504/IJAHUC.2014.066419.

[14] 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.

[15] S. S. Kolahi, S. Narayan, D. D. T. Nguyen and Y. Sunarto „Performance Monitoring of Various Network Traffic Generators'' UkSim 13th International Conference on Computer Modelling and Simulation, Cambridge, 2011, pp. 501-506, doi: 10.1109/UKSIM.2011.102.