C. R. Physique 15 (2014) 415–420

Contents lists available at ScienceDirect

Comptes Rendus Physique

www.sciencedirect.com

Electromagnetism / Électromagnétisme

Modeling extreme values resulting from compromising electromagnetic emanations generated by an information system

Étude des valeurs extrêmes des signaux électromagnétiques compromettants induits par un système informatique

Chaouki Kasmi [a,b,*], Marc Hélier [b], Muriel Darces [b], Emmanuel Prouff [a]

[a] *French Network and Information Security Agency – ANSSI, 75007 Paris, France*
[b] *Sorbonne Universités, UPMC, UR2, L2E, BC 252, 4, place Jussieu, 75005 Paris, France*

ARTICLE INFO

Article history:
Available online 24 April 2014

Keywords:
Electromagnetic security
TEMPEST
Extreme tendencies
Excess model

Mots-clés :
Sécurité électromagnétiques
TEMPEST
Valeurs extrêmes
Modèle des excès

ABSTRACT

Electromagnetic intelligence and attacks pose unacceptable risks for the security and safety of critical networks and more specifically the power network. In this paper, it is pointed out how the use of the *excess model* allows one to extrapolate the very high level of spurious compromising emanations induced by an information system in realistic power network models. It is shown that the design of appropriate protections and risk management methodologies can be enhanced thanks to the *extreme value statistics*.

RÉSUMÉ

Les thèmes de la confidentialité et de la résilience sont deux enjeux majeurs pour la protection d'une infrastructure critique. La susceptibilité des équipements électroniques vis-à-vis des interférences électromagnétiques intentionnelles et la corrélation potentielle entre le bruit généré par un système électronique et les informations traitées par celui-ci induisent un risque extrêmement fort pour la sécurité de l'information. Dans cette étude, nous nous intéressons à la propagation de signaux compromettants de niveaux élevés mais dont la probabilité est faible. Il est démontré que la conception de protections appropriées ainsi que les méthodologies de gestion des risques peuvent être améliorées par l'étude des valeurs extrêmes.

1. Introduction

Nowadays, the trend is to integrate many more electronic systems into sensitive applications. This can be a critical issue as it tends to make these infrastructures more vulnerable to electromagnetic attacks [1]. It moreover makes the industry

* Corresponding author.
E-mail address: chaouki.kasmi@ssi.gouv.fr (C. Kasmi).

http://dx.doi.org/10.1016/j.crhy.2014.03.002
1631-0705/

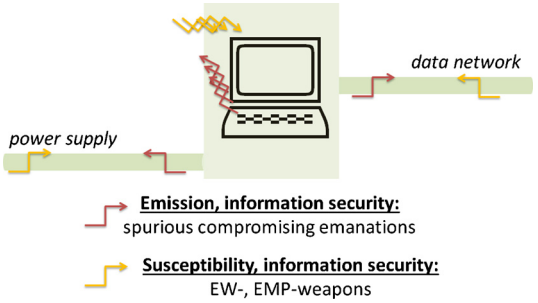

Fig. 1. Electromagnetic security: emission and susceptibility of an information system.

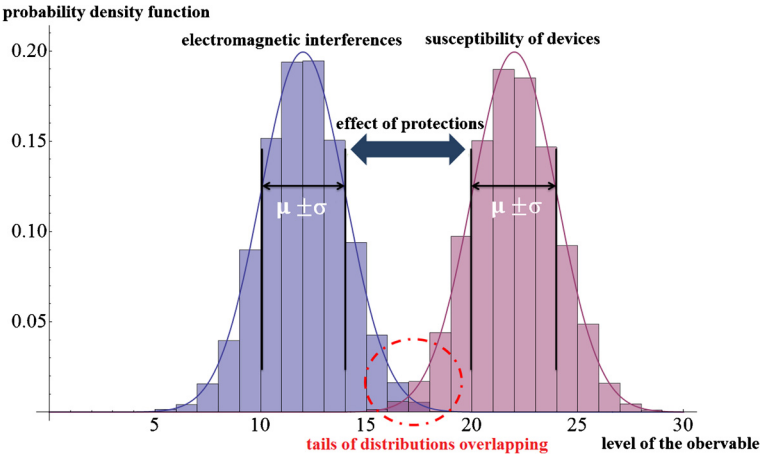

Fig. 2. Probability density function of EMI and device susceptibility levels.

more exposed to the leakage of sensitive information through spurious compromising electromagnetic emanations (SCE) [2] radiated by the involved electronic devices (Electromagnetic interference (EMI) threats depicted in Fig. 1).

The power-grid is of particular interest [3,4], since it connects the secure and public areas as well as all sensitive electronic devices. Due to the complexity of the power network (topology, cable cross-section, etc.), the study is generally carried out by its description through a realistic model in electromagnetic simulation software. The uncertainty (or variability) of the input modeling parameters can be taken into account in such models.

Physical quantities are generally modeled based on *Gaussian* distributions [5]. This implicitly restricts the analysis to the mean contributions of the observables. Protective devices defined under such assumption may be unsuitable for the real risk, as shown in Fig. 2, where the tails of the EMI and the device's susceptibility levels distributions obviously overlap. In security and safety contexts, this kind of restriction may reduce analysis soundness, since *Gaussian* approximations are known to fail in accurately modeling rare events that are the most critical ones in our applications. It has been shown that the extremal type theorem [6], and more precisely the *excess model* [7], is a useful tool to avoid the underestimation of the critical extreme events level for a given probability. Recently applied in electromagnetic compatibility (EMC) studies [8], it has been shown that the level of extreme events can be well estimated.

In this study, the excess model [7] is derived in order to extrapolate the very high level of voltages and currents induced by an information system in the power distribution network. The benefits of the excess model in the context of the electromagnetic security (EMSEC) will be highlighted.

The paper is organized as follows: in Section 2, the methodology applied for the modeling of the power network will be described. In Section 3, the Generalized *Pareto* Distribution will be presented. Thanks to the combination of the excess model and a Monte Carlo simulation approach, the very high levels of the spurious end-current magnitude induced by a computer in the power network will be computed. It will be shown how risk management accuracy can be enhanced using the excess model.

2. Power-grid modeling

The propagation of the electromagnetic wave in the power network has been modeled thanks to the CRIPTE Code [9] developed by ONERA. It aims at resolving the *Baum, Liu* and *Tesche* (BLT) equation in order to estimate the currents and voltages induced by external sources in topological networks. The low-voltage network under study is depicted in Fig. 3.

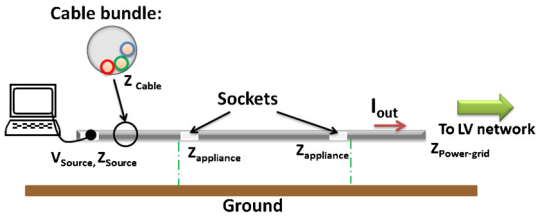

Fig. 3. Low-voltage test network.

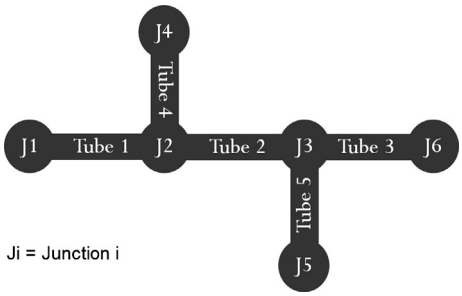

Fig. 4. Topological description of the low-voltage network under analysis.

The electromagnetic topology [10] consists in the decomposition of a non-uniform complex network into a set of connected uniform sub-networks by means of tubes and junctions. The topological description of the low-voltage network depicted in Fig. 3 is given in Fig. 4. The tubes represent the transmission lines (Tubes 1 to 5) and the junctions denote either perfect transitions (J2 and J3) or the connected loads impedance (J1, J4, J5, and J6). Each variation (cable cross-section variability, power sockets) has been taken into account in the topological model.

The common-mode spurious end-current magnitude $|I_{\text{out}}|$ will serve as the observable in this study. It can be assumed that it relates to the following equation:

$$|I_{\text{out}}| = \alpha\left(V_{\text{Source}}, Z_{\text{Source}}, \left([Z_{\text{cables}}]\right), Z_{\text{Power-grid}}, (Z_{\text{Appliances}}), f\right) \tag{1}$$

where V_{Source} and Z_{Source} are respectively the voltage source and the impedance of the computer connected, which induces the electromagnetic noise in the network. The parameter $Z_{\text{Appliances}}$ is the set of the input impedances of the connected electronic equipments (printer, computer...), the parameter $[Z_{\text{Cable}}]$ denotes the set of characteristic impedance matrices associated with each tube. Each characteristic impedance matrix is itself a function of the diameter of the conductors, of their height above the ground, and of their position in the electric raceway. The network is supposed to be connected to a large power network represented by the impedance $Z_{\text{Power-grid}}$ measured on a large power-grid. f refers to the working frequency (from 1 MHz to 100 MHz).

In this section, the tools applied for the characterization of the tubes and the junctions will be described.

2.1. Tubes: cable modeling

The single-phase low-voltage network is based on cables composed of three copper wires named phase, neutral, and ground. Assuming that the height of conductors above the ground is smaller than the shortest wavelength and that the dielectric losses are negligible, the Multiconductor Transmission Line Theory can be applied.

In our analysis, it is assumed that the conductors have a 1.5-mm^2 cross-section and that their length is equal to 3 m. The mean height of the electrical sockets above the ground is 5 cm and the electrical raceway diameter is 3.5 cm (both parameters are considered as EM transparent in this study). Based on physical considerations, it is assumed that the propagated mode in the modeled test network is a quasi-TEM one.

The conductors are randomly arranged in the raceway, therefore defining the boundary conditions, which are the maximal and minimal admissible distances between the conductors in the electrical raceway. Two hundred random 2D cross-sections have been generated; three of them are depicted in Fig. 5. The tubes can then be characterized by the computed per-unit-length parameters of the cable cross-sections with respect to the metallic ground.

2.2. Junctions: appliances

The characterization of appliances connected to the low-voltage network is of fundamental interest since the propagation of electromagnetic waves is highly influenced by them [11]. The available connectors of measurement equipment are N-type connectors, an adaptor between a 50-Ω-N type connector and a female power socket has been designed in order to measure the reflection coefficient of electronic devices.

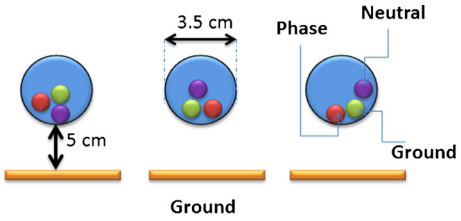

Fig. 5. Examples of random cable cross-sections.

Table 1
Correspondence between the load reference and the tested devices.

Load reference	Appliance
L1	alarm's clock
L2	battery charger
L3	computer speakers
L4	printer
L5	light
L6	computer

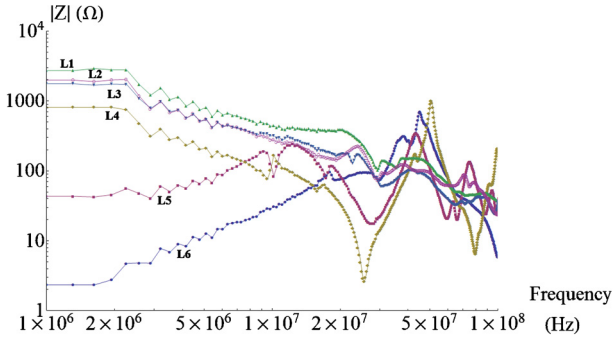

Fig. 6. Measured impedance of loads L1 to L6.

Using a *de-embedding technique* [12], six classical appliances, representative of those usually found in an office, have been characterized. The resulting impedances (L1 to L6, related to Table 1) are depicted in Fig. 6.

Moreover, using statistical tools [12], from each measured appliance, ten samples of loads have been derived, taking into account the errors in the measurement process. Additionally, the open-circuit load and the large power network impedance have been included in the database. The set of impedances is involved in the model for characterizing end-junctions (J1, J4, J5, and J6) in the topological model of the power network.

3. The generalized *Pareto* distribution

The study focuses on the probability that a spurious signal excesses a defined threshold. For such a purpose, the excess model approach [7] (also called *peak-over-threshold* approach) is applied in order to estimate the extreme tendencies of the physical quantity under study ($|I_{out}|$). This methodology consists in the determination of the samples above a high-enough threshold in a set of observations and more precisely the statistical distance between the remaining samples and the threshold, called excesses. The appropriate distributions can be chosen within the generalized *Pareto* distribution family.

In this section, the definition of the generalized *Pareto* distribution is given. Then, statistical methods that can be applied for the adjustment of a generalized *Pareto* distribution are also provided. Finally, the extreme values of the spurious end-current magnitude are analyzed. The results obtained thanks to the Gaussian model are compared to the excess model results.

Note that an event is hereafter considered as an extreme one if its level is above an estimated threshold, which is defined as the 90th quantile of the dataset $Q(p = 0.9)$ given for the probability p by:

$$Q(p) = F^{-1}(p) \tag{2}$$

where F^{-1} refers to the inverse of the cumulative distribution function F.

Table 2
Estimated shape and scale parameters using Eq. (4).

f (MHz)	Threshold (mA)	Shape	Scale (mA)
3.8	0.53	0.58	0.33
63.8	2.18	−0.17	0.52
90.7	6.19	0	1.15

Table 3
Estimated quantiles using the *Gaussian* model (Ga), GPD model and Empirical one (Em).

f (MHz)	Q_{Em} (mA)	Q_{Ga} (mA)	Q_{GPD} (mA)
3.8	4.50	1.55	4.58
63.8	9.09	2.97	9.14
90.7	19.70	7.55	19.71

3.1. Definition

The generalized *Pareto* distribution (GPD) has been first introduced by Pickands et al. in 1975 [7]. It is commonly presented as a two-parameter distribution, i.e. scale and shape parameters. The GPD has a cumulative distribution function given by:

$$F_{\beta,\xi}(x) = \begin{cases} 1 - (1 + \frac{\xi}{\beta}x)^{-\frac{1}{\xi}}, & \xi \neq 0 \\ 1 - \exp[-\frac{x}{\beta}], & \xi = 0 \end{cases} \tag{3}$$

where β and ξ are respectively the scale and the shape parameters.

3.2. Maximum log-likelihood function

Several statistical tools have been proposed in order to estimate the parameters of the GPD. In our study, the classical maximum log-likelihood method has been applied:

$$l(\beta,\xi) = -n\ln\beta - \sum_{i=1}^{n} \frac{\xi+1}{\xi} \ln\left(1 + \frac{\xi x_i}{\beta}\right) \tag{4}$$

where x_i denotes a sample of the ith observations above a defined threshold.

In the case of the GPD, there is no analytical solution that allows the maximization of Eq. (4). As a result, an iterative numerical algorithm has been applied using Matlab for the estimation of β and ξ.

3.3. Extreme values of spurious compromising emanations

Using a Monte Carlo simulation approach, 10^5 random networks have been generated using the random cable cross-sections and the derived impedances. Both parameters (position of conductors and connected appliances) are considered as equiprobable.

First, the threshold, defined as the 90th quantile is computed. Then, the shape and scale parameters of the excess model are estimated using Eq. (4). The results are summarized for a frequency of 3.8 MHz, 63.8 MHz, and 90.7 MHz in Table 2.

Finally, the 95th quantiles of the inferred distributions have been computed using the *Gaussian* model (Q_{Ga}) and the GPD model (Q_{GPD}) as well as the empirical one. Results are provided in Table 3. It can be observed that the excess model allows a better evaluation of the spurious compromising current magnitude for a given probability. It can be pointed out that, based on the classical *Gaussian* model, the common-mode end-current magnitude is always underestimated.

4. Conclusion

In this paper, it has been shown that the excess model is a well-suited tool for the estimation of high-level electromagnetic interferences. The Generalized *Pareto* Distribution has been applied for the computation of very high levels of the spurious compromising emanations induced by an information system in the power network.

The comparison between the classical *Gaussian* and excess models allows concluding about the benefit of the GPD formalism for the information security risks management, since appropriate protections (such as filters, shields) can be designed. Threats of electromagnetic interferences related to the susceptibility of devices to high-power electromagnetic attacks can be reduced and the emissivity of devices vulnerable to electromagnetic intelligence can be lowered.

References

[1] F. Brauer, F. Sabath, J. ter Haseborg, Susceptibility of IT network systems to interferences by HPEM, in: IEEE International Symposium on Electromagnetic Compatibility, EMC 2009, 2009, pp. 237–242.
[2] W.V. Eck, N. Laborato, Electromagnetic radiation from video display units: an eavesdropping risk, Comput. Secur. 4 (1985) 269–286.
[3] Y. Parfenov, L. Zdoukhov, W. Radasky, M. Ianoz, Conducted IEMI threats for commercial buildings, IEEE Trans. Electromagn. Compat. 46 (3) (2004) 404–411.
[4] D. Mansson, R. Thottappillil, M. Backstrom, Propagation of UWB transients in low-voltage power installation networks, IEEE Trans. Electromagn. Compat. 50 (3) (2008) 619–629.
[5] International Organisation of Standardization, Guide to the expression of uncertainty in measurement, 2000.
[6] R.A. Fisher, L.H.C. Tippett, Limiting forms of the frequency distribution of the largest or smallest member of a sample, Math. Proc. Camb. Philos. Soc. 24 (1928) 180–190.
[7] J. Pickands, Statistical inference using extreme order statistics, 3 (1975) 119–131.
[8] C. Kasmi, M. Darces, M. Hélier, E. Prouff, Generalised Pareto distribution for extreme value modelling in electromagnetic compatibility, Electron. Lett. 49 (2013) 334–335.
[9] J.-P. Parmantier, P. Degauque, Topology based modeling of very large systems, in: J. Hamelin (Ed.), Modern Radio Science, Oxford University Press, 1996.
[10] C.E. Baum, Generalization of the BLT equation, in: Interaction Notes, vol. 511, 1995, pp. 131–136.
[11] C. Kasmi, M. Darces, M. Hélier, Statistical analysis of a spurious signal level in a low voltage PLC network, in: International Symposium on Electromagnetic Compatibility (EMC EUROPE), 2012, pp. 1–5.
[12] C. Kasmi, M. Darces, M. Hélier, E. Prouff, HF input impedance measurement based on a de-embedding technique, in: Ultra Wideband Short Pulse 10, 2014, Part IV: Measurement Techniques, 2014, pp. 393–401.