Stochastic Study of the Receptivity of Critical Load to Conducted IEMI in a Network

Bing Li, and Daniel Månsson

***Abstract*—In most cases, the electromagnetic disturbance appears somewhat in a stochastic way, which hence probably leads to damages on the critical loads connected to networks, in terms of different extents, being random. Especially when it comes to intentional electromagnetic interference (IEMI), where more human activities are involved, then the traditional electromagnetic topology concept becomes not straightforwardly applicable. In this paper, with respect to the IEMI, we analyze the receptivity of the critical load in a network by using stochastic methods. The statistical results are presented via the complementary cumulative distribution function (CCDF), which intuitively shows the probability in that the critical load can be successfully attacked. The research indicates that, the receptivity can still be large even if the IEMI disturbance source is far away from the critical load, and it depends on the probability of the disturbance accessing the critical load.**

***Index Terms*—Stochastic approach, receptivity, network, IEMI.**

I. Introduction

USUALLY, in realistic scenarios, where the attacker has little or no knowledge of electromagnetic interference, the IEMI attack occurs in a stochastic fashion, in terms of categories, location, duration of the attack [1], [2]. To evaluate the impacts of stochastic IEMI attacks, the concept of receptivity in the EMC field was proposed [3], which describes transfer functions and acts as an important metric for characterizing the susceptibility of a facility.

The location/position of the IEMI disturbance source measures the distance between the disturbance and the critical load, and it is an important factor of affecting the receptivity of critical system/load. However, to the best of our knowledge, the existing work regarding the receptivity in the presence of stochastic IEMI is very limited. In [4], a preliminary study analyses the frequency response of loads in a network with respect to the IEMI, based on the Monte Carlo approach. Here, we mainly investigate the receptivity of critical load in a network, regarding the conducted IEMI appearing in a stochastic position.

The rest of the paper is organized as follows. In Sec. II, we first describe our scenario, which is a multi-junction multi-branch network including a critical load, and is established based on the concept of electromagnetic topology. Then, we elaborate the stochastic approach used for assessing the receptivity of the critical load in the model. In Sec. III, based on the stochastic approach and the modified BLT approach, we calculate the receptivity of the critical load in the model. Moreover, several cases with respect to the probability distribution for accessing different zones are studied, and the resulting impacts by stochastic disturbance are analyzed and discussed. Finally, our work is summarized in Sec. IV.

B. Li is with the Department of Electromagnetic Engineering, Royal Institute of Technology, 100 44 Stockholm, Sweden (e-mail: libing@kth.se).

D. Månsson is with the Department of Electromagnetic Engineering, Royal Institute of Technology, 100 44 Stockholm, Sweden (e-mail: manssond@kth.se).

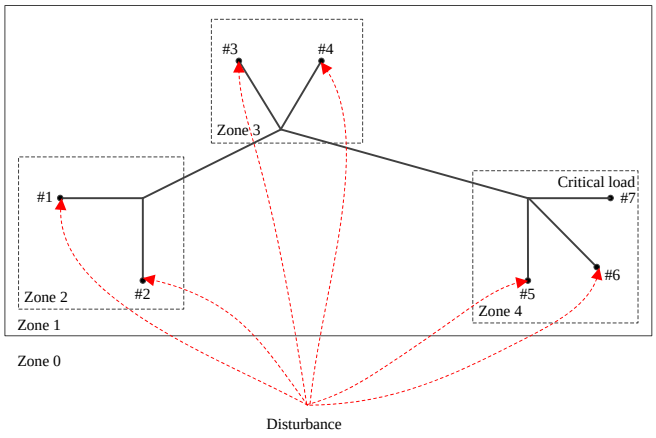

Fig. 1. A multi-junction multi-branch network with several ports distributed in different zones. The electromagnetic disturbance can be injected from any port to attack the critical load at Port 7.

II. Stochastic Approach of Estimating Receptivity

A. Scenario

Commonly, critical loads in distributed systems are protected based on the concept of electromagnetic topology, where zone boundaries are set up according to respective susceptibility. Moreover, the accessibility of a system [3] describes the ability of gaining access to different parts of the system. Regarding the IEMI, due to the intervention of human activities, a portable IEMI source can be carried into different zones with certain probabilities, such that the conventional deterministic zones partitions may not be able to provide effective protections for the facilities. In other words, for a network with loads distributed in different zones, the conducted interference that randomly emerges in different zones can still reach the critical load through the network, and may hence result in damages.

In this paper, a network with seven ports distributed in different zones is studied, as shown in Fig. 1. Here, for simplifying illustration, we assume that the critical load is connected to port 7. The disturbance is injected randomly into any one of other six ports. Then, excluding the ports for the

critical load and disturbance injection, respectively, other ports are connected to random loads. Without loss of generality, we assume the probabilities of accessing Zone 2, 3 and 4 are different. Particularly, we define Zone 4 as the "critical zone", since the critical load is located there, and by accessing Zone 4, the attack is most likely to succeed. However, it is worth noting that, the attack is still likely to succeed if the probability of accessing Zone 2 or 3 is large. Therefore, it is essential and valuable to investigate the receptivity of the critical load regarding the stochastic IEMI.

B. Stochastic Approach

Regarding the critical load in a network, the receptivity (transfer function) from all possible ports to the critical load should be checked [3]. In our specific model, the receptivity associated with different ports is shown in Fig. 2. Considering that the access probabilities of the IEMI attacker to different zones may be different, we use P_2, P_3 and P_4 to represent the accessing probabilities for Zone 2, 3 and 4, respectively, and $P_2 + P_3 + P_4 = 1$ holds for any P_2, P_3 and P_4. Note that, for a network with multiple junctions and branches, it is difficult to obtain the closed-form transfer function from one port to another. Therefore, we alternatively use a stochastic approach to evaluate the receptivity of critical load in the probabilistic sense, by considering the voltage on the load. The statistical results are presented in terms of the CCDF.

In statistics [5], for any random variable X, the cumulative distribution function (CDF) is defined as

$$F_X(x) = P(X \leq x)$$

which characterizes the events that X does not exceed the given x in probability. Thus, for the contrary events, i.e., X exceeds the given x, the resulting probability is characterized by the CCDF, which is given as

$$\bar{F}_X(x) = P(X > x) = 1 - F_X(x).$$

The purpose of presenting the results via the CCDF is that, we focus on the probability that the receptivity is higher than some certain value, e.g., threshold.

III. Receptivity of Critical Load

A. Receptivity Calculation

In this section, we calculate the receptivity of the critical load, based on the model proposed in Sec. II-A. Regarding the calculation, we follow the method proposed in [6], for dealing with the problem of multi-reflection between junctions. The method is derived based on the BLT approach, and its high accuracy has been verified by [7]. The main idea of the method is to divide a multi-junction network into several one-junction networks. When the disturbance is injected from a different port, the resulting decomposition is different, which plays an important role in the subsequent calculation. To be more precise, for the network shown in Fig. 3a (equivalent to the network in Fig. 1), when the disturbance injection happens at Zone 2, i.e., injected from Port 1 or 2, the decomposition is shown in Fig. 3b. Then, the one-junction network that

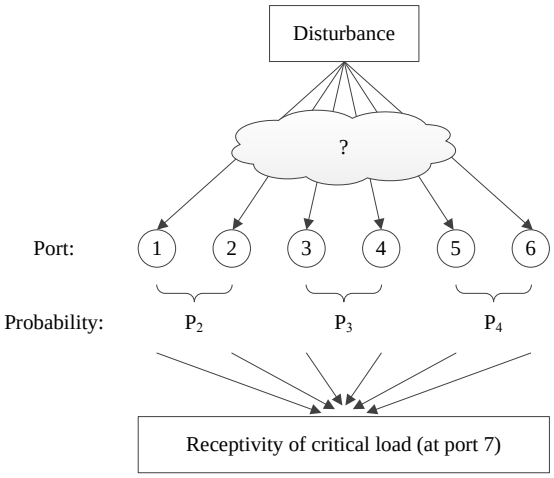

Fig. 2. Illustration of the stochastic disturbance injection, where P_2, P_3 and P_4 denotes probabilities of accessing Zone 2, 3, and 4, respectively, and Port i, $1 \leq i \leq 6$, is the potential port for injection.

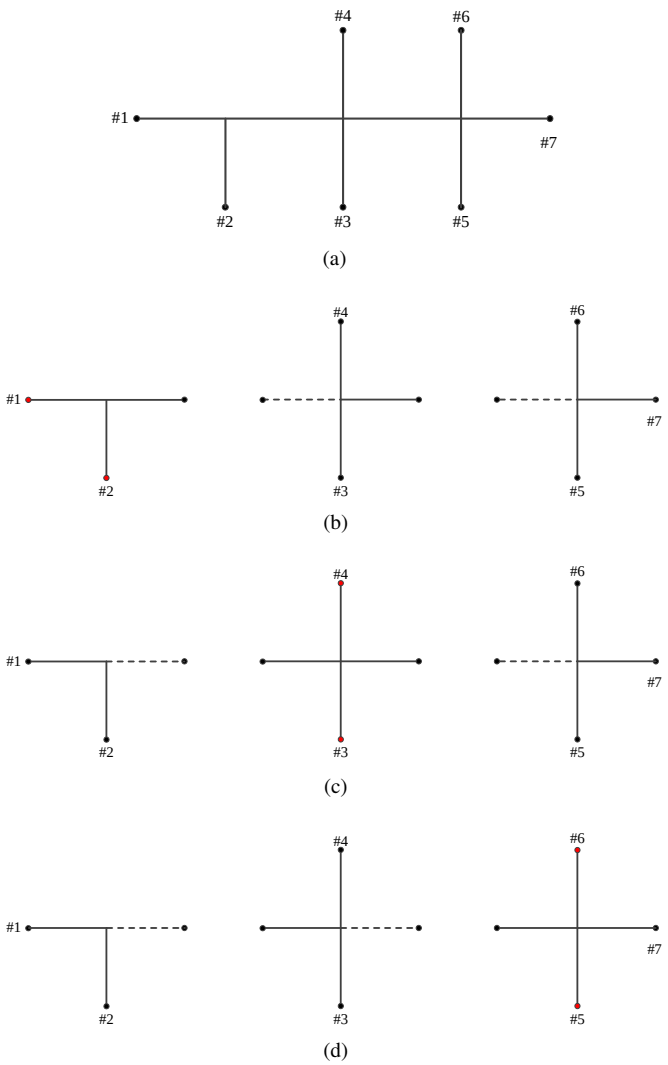

Fig. 3. Decomposition of the network, where red markers point out the injection port. (a) network; (b) case of injected from Zone 2; (c) case of injected from Zone 3; and, (d) case of injected from Zone 4.

contains Port 5, 6 and 7 is termed as the "super load" of the adjoining network shown in the middle. Recursively, the one-junction network that contains Port 3 and 4 can also be treated as the super load of the leftmost network. Likewise, for the case that the disturbance is injected from Zone 3 or Zone 4, the decomposed networks are shown in Fig. 3c and Fig. 3d, respectively.

Previous results [8] indicates that, for networks in which the medium between conductors is lossless or low-loss (as for the insulation in normal power cables), the frequency response of frequency-independent load (i.e., purely resistive load) is periodic in the frequency domain (see the example in Fig. 4). Moreover, it is suggested that, to protect critical loads in networks, one mainly needs to focus on the frequency response of the critical load within one period in the frequency domain. That is, due to the periodicity, there are potentially multiple frequencies at which the IEMI can result in serious damages to critical loads in networks. In this sense, from the perspective of protection, it is necessary to consider typical frequencies associated with the period of frequency response. Here, we calculate the frequency response of the critical load, i.e., the load connected to Port 7 in Fig. 3a, when the disturbance is located in Zone 2, 3 or 4. The parameters for the network under investigation are given in Table I. Let L_0 denote the length of the line connected two junctions, and L_b denote the length of the branch. V_s represents the voltage of the disturbance injected into the network. Z_L and Z_c represent the load impedance and characteristic impedance of the lines, respectively. Thus, the lengths of two lines for connecting adjacent junctions are both 15 m, all branches have the identical length, i.e., 10 m, and the impedance of all loads are all 100 Ω. The results are given in Fig. 4. It is shown that, wherever the disturbance is injected from, the resulting frequency response emerges in the periodical manner, i.e., with a period of 20 MHz in the frequency domain (see Fig. 4). Thus, in what follows, we only consider the frequency responses within one typical period, i.e., frequency band $0 \sim 20$ MHz.

For a more realistic study, we consider the amplitude of loads $|Z_\mathrm{L}|$ ranges from 0 to 1000 Ω, and the phase ϕ_{Z_L} ranges from $-\pi/2$ to $\pi/2$. In the calculation, we sweep the frequency of the disturbance V_s from 0 to 20 MHz, and focus on the maximum of the receptivity of the critical load within the frequency range. For statistical analysis, we generate 1×10^4 groups of random data for the injection position (port) of the disturbance and impedance of loads connected to the rest ports. We consider several distinct probability distributions for P_2, P_3 and P_4, as given in Table II, where the case with $P_2 = P_3 = P_4$ is particularly taken as a reference. Then, the resulting CCDFs according to different probability distributions are compared. The receptivity of the critical load is written as V_7/V_s, and the CCDF results of different cases are given in Fig. 5.

B. Discussion

From Fig. 5, it can be seen that, generally, the receptivity ranges mainly from 0 to 1.6. We notice that, for all curves, the values of the CCDFs are considerable when V_7/V_s is larger than 1, which is believed to be due to the superposition of the incoming waves at the critical load. Compared to the reference case, i.e., Case 0, the CCDFs of Case 1, 3 and 5 yield higher probabilities, while the others yield lower probabilities. This finding indicates that, the probability of successful IEMI attacks can be significantly reduced by restricting the access to the critical zone, i.e., decreasing P_4, and this is consistent to what we can expect. However, it is worth to note that, despite that the value of P_4 in Case 5 is lower than that in Case 0, the CCDF of Case 5 is always higher than the reference CCDF. It implies that, when the value of P_2 is large enough, the critical load is still exposed to a considerable threat of being attacked, even though the value of P_4 is decreased. Furthermore, comparing Case 2 with Case 5, in which the values of P_4 are the same, it is surprising to find that, the

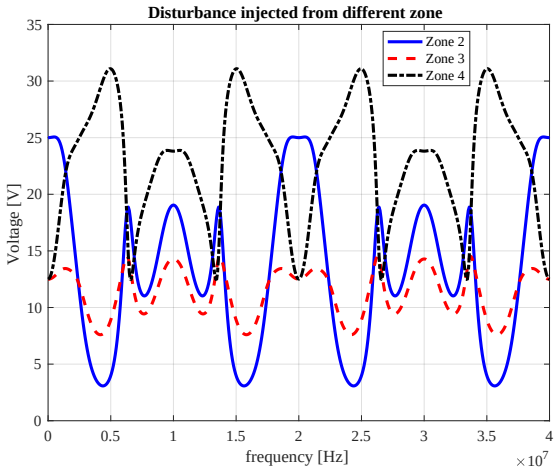

Fig. 4. Periodicity of the frequency responses of the critical load for the case of injected from Zone 2, 3 or 4, when the impedance of all loads in the network shown in Fig. 3a are 100 Ω, and the values of other parameters are given in Table I.

TABLE I
PARAMETERS FOR THE NETWORK SHOWN IN FIG. 3A.

Parameter	L_0 (m)	L_b (m)	V_s (V)	Z_L (Ω)	Z_c (Ω)
Value	15	10	100	100	50

TABLE II
PROBABILITY DISTRIBUTION.

	P_2	P_3	P_4
Case 0	1/3	1/3	1/3
Case 1	0.1	0.3	0.6
Case 2	0.1	0.6	0.3
Case 3	0.3	0.1	0.6
Case 4	0.3	0.6	0.1
Case 5	0.6	0.1	0.3
Case 6	0.6	0.3	0.1

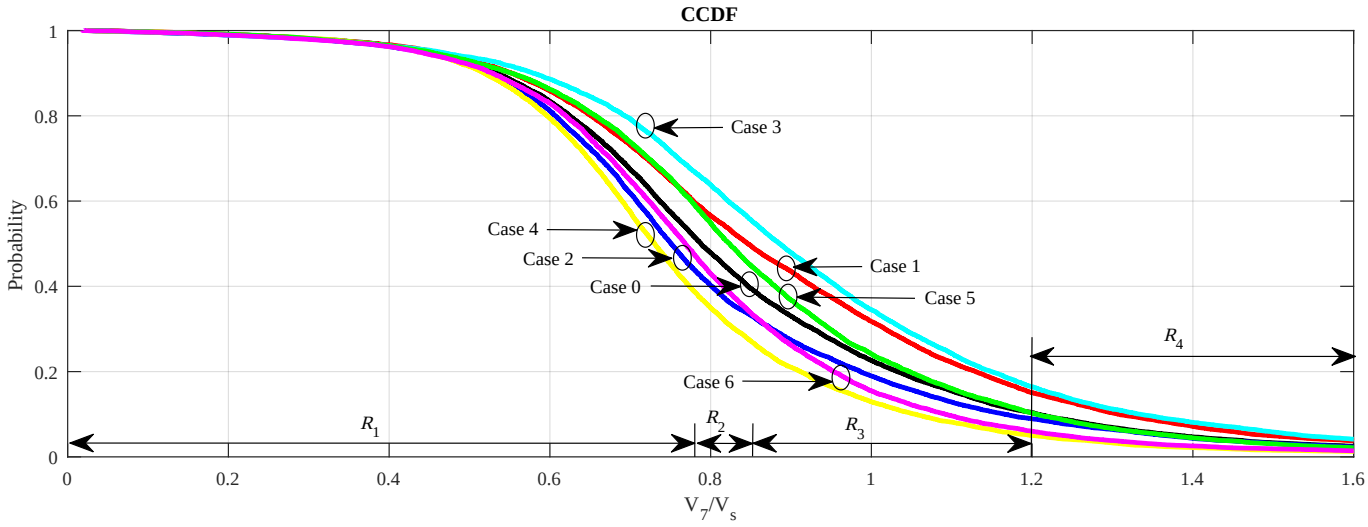

Fig. 5. The CCDFs under the cases in Table II. According to V_7/V_s, the CCDFs are divided into four regions, R_1, R_2, R_3 and R_4.

CCDF of Case 2 is definitely smaller than that of Case 5. More exactly, with respect to the critical zone (Zone 4), despite that Zone 2 is more distant than Zone 3, the critical load is under attack with higher probability when P_2 is sufficiently larger than P_3. This finding indicates that, from the perspective of protection, one cannot ignore the impact of the disturbance even from the "far-away" injection port, and all injection positions that potentially result in serious damages should be aware of and well investigated.

Specifically, the CCDFs can be roughly divided into four regions according to V_7/V_s, i.e., R_1, R_2, R_3 and R_4, as shown in Fig. 5. The CCDFs of the cases in each region are sorted as follows.

R_1: Case $3 > \underline{5} > \underline{1} > 0 > 6 > 2 > 4$
R_2: Case $3 > \underline{1} > \underline{5} > 0 > \underline{6} > \underline{2} > 4$
R_3: Case $3 > 1 > 5 > 0 > \underline{2} > \underline{6} > 4$
R_4: Case $3 > 1 > 5 \approx 0 \approx 2 > 6 \approx 4$

From R_1 to R_4, there are two obvious changes, as the underlined case number shown above. More precisely, we assume that there is a threshold V_T, such that the critical load gets damaged due to disturbance once V_7/V_s is larger than V_T. Elevating V_T from R_1 to R_2, we find that the CCDFs of Case 5 and Case 1 are swapped. It similarly happens to the scenario when V_T increases from R_2 to R_3, where the CCDFs of Case 6 and Case 2 are swapped. As analyzed above, increasing the value of either P_2 or P_4 will increase the risk of being attacked for the critical load. However, both of the two swaps above reveal a common point that, when increasing threshold V_T, the value of P_4 plays a dominant role, instead of P_2.

IV. Conclusion

We consider a multi-junction multi-branch network in the presence of randomly injected conducted IEMI. The receptivity of the critical load is analyzed, where a stochastic method in terms of the CCDF is used to characterize the probabilistic damages. By calculating the frequencies response of the critical load, statistic results are obtained via injecting the disturbance randomly in different zones and ports with various probability distributions. Results show that:

- The probability of successful IEMI attacks can be largely reduced by restricting the access to the critical zone.
- Disturbance by "remote" injection (i.e, a large distance between the point of injection and critical load), but with large accessing probability, may also lead to serious damages. The position/port of disturbance injection and the corresponding zone-accessing probability are important factors on the receptivity of the critical load, and hence also deserve careful considerations.
- To reduce the potential threat to the critical load, it is essential to consider the accessibility (related to probability of accessing zones), and the susceptibility (related to the receptivity and tolerance threshold), jointly.

References

[1] E. Genender, H. Garbe, and F. Sabath, "Probabilistic risk analysis technique of intentional electromagnetic interference at system level," *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 1, pp. 200–207, 2014.

[2] F. Sabath and H. Garbe, "Concept of stochastic modeling for high-power electromagnetics (hpem) risk analysis at system level," in *Electromagnetic Compatibility (EMC), 2013 IEEE International Symposium on*. IEEE, 2013, pp. 401–406.

[3] D. Månsson, R. Thottappillil, and M. Bäckström, "Methodology for classifying facilities with respect to intentional EMI," *IEEE Transactions on Electromagnetic Compatibility*, vol. 51, no. 1, pp. 46–52, 2009.

[4] B. Li and D. Månsson, "Frequency Response Analysis of IEMI in Power Line Network by Using Monte Carlo Approach," in *electronic environment 2016*. Electronic Environment, 2016.

[5] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education, 2002.

[6] B. Li, D. Månsson, and G. Yang, "An Efficient Method for Solving Frequency Responses of Power-Line Networks," *Progress in Electromagnetics Research B*, vol. 62, pp. 303–317, 2015.

[7] J. Carlsson, T. Karlsson, and G. Undén, "EMEC-an EM simulator based on topology," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 353–358, 2004.

[8] B. Li and D. Månsson, "Effect of Periodicity in Frequency Responses of Networks From Conducted EMI," *IEEE Transactions on Electromagnetic Compatibility*, 2017.