Mitigation Techniques to Reduce the Vulnerability of Railway Signaling to Radiated Intentional EMI Emitted From a Train

Marc Heddebaut, Virginie Deniau, Jean Rioult, Christophe Gransart

Mitigation Techniques to Reduce the Vulnerability of Railway Signaling to Radiated Intentional EMI Emitted from a Train

Marc Heddebaut, Virginie Deniau, Jean Rioult, and Christophe Gransart

***Abstract*—This paper evaluates several techniques capable of mitigating the impact of low power radiofrequency jammers that interfere with ground-to-train communications. These radio communications are used for railway signaling, and interfering with these signals can have a negative impact on train operation. Although the commercialization, detention, and use of radiofrequency jammers is strictly forbidden in most countries, they can be easily found on the internet at low cost and unexpectedly switched on by a passenger in a moving train. In this paper we evaluate and compare the ground-to-train radio communication and IEMI received signal powers delivered by roof train antennas to the train control command receiver. This comparison is used to deduce potential zones of interference along the train trajectory and its consequences. Operating at the physical layer, we then propose and evaluate three mitigations techniques that can be used separately or combined to reduce the impact of this type of interference. We show that they can significantly reduce the jamming capability and help maintaining railway full operation.**

***Index Terms*—Electromagnetic compatibility, Cellular radio, Rail transportation communication, Jamming, Antennas.**

I. Introduction

THE theme of cybercrime is now a major challenge for our societies, strongly supported both nationally and internationally. Let us put cybercrime in the context of transport. In Europe, critical infrastructures are described as follows [1]: “Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services.” Other regions of the world have adopted similar definitions [2]. As we can deduce, these critical infrastructures are numerous and play an important role in our daily lives, whether directly or indirectly; some of them can be sensitive to IEMI [3], [4], [5]. For example, the rail infrastructure covers many priority corridors all over the world. These railway lines are a vital means of transport providing both passenger and freight transport. Likewise, the road transport infrastructure is another important example with the expected development of the automated road and the arrival of safety relevant services based on inter-vehicles radio communications. To illustrate this critical aspect in the transportation domain, let us go back a few decades. Many of us remember directly or indirectly from the year 1963 when, at Ledburn England, Glasgow mail train traveling to Euston Station in London was carrying the equivalent of forty-three million pounds to be destroyed by the bank of England. To stop the train, thieves hid the green signal of a traffic light and, using a portable battery, operated the red signal, resulting in the requirement for the train to stop, scrupulously respected by the train driver. Once the train stopped, the bandits jumped on board to detach the locomotive of the first two train cars and stole money. This train robbery, famously, is very illustrative of what a voluntary change in railway signaling may bring in terms of stopping the train "on demand", and is very introductive of what modern techniques of cybercrime could now potentially perpetrate against this critical infrastructure.

Already many years ago, but more recently in 1998, some authors envisaged electromagnetic terrorism as a real danger in [6]. The problem of IEMI against civilian air traffic was addressed in [7], and [8] investigated the vulnerability of an electrified railway system to radiated IEMI. Still in [8], the authors considered the use of a high power microwave source and the scenario of in-band disturbances damaging the communication system connected to the roof train antenna. In this paper, we also address railway signaling and IEMI. However, we evaluate the potential of low power jammers located in the train, for example in a passenger pocket, to interfere with signaling communications, and to stop trains potentially at predetermined locations. This studied scenario is illustrated Fig.1.

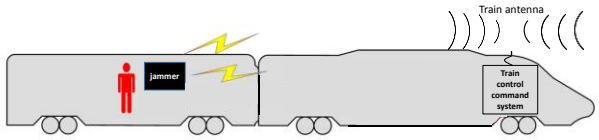

Fig. 1. IEMI signal transmitted from the train to the roof train antenna.

To the contrary of high power sources, using low power IEMI sources leaves no easily detectable damage to the

The research leading to these results has received funding from the European Community’s Framework Program FP7/2007-2013 under grant agreement n°285136.

system. Therefore, they can be more difficult to identify when the jammer has been stopped.

The rest of this paper is organized as follows. Section II describes low power jammer characteristics relevant to the study, analyzes their output signals, and deduces a representative theoretical railway jamming signal. Section III presents a typical dedicated railway ground-to-train cellular communication network and, along this particular network, estimates the received power strength by the moving train. Section IV starts by presenting coupling attenuations between radiofrequency sources located in the train and a train roof antenna; it then compares the jamming signal power and the ground-to-train radio power received by this roof antenna. This comparison is used to deduce interference areas. Section V presents three envisaged mitigation techniques and evaluate their performance, trying to reduce the size of the previously identified interference areas. Finally, section VI presents some perspectives and draws a conclusion.

II. Jamming signal characteristics

Looking for radio frequency jammers on the internet will return many results recalling jamming prohibition, but also providing technical information and commercial proposals. Indeed, many types of radio jammers are for sale on the market. Some of them can block the signals of only one frequency band; some of them can block up to 5 frequency bands at the same time. They can be battery operated, pocket size, or more powerful. They operate between several hundred MHz, up to a few GHz, delivering their output signal to different output ports, up to external antennas that can be simple quarter wave antennas or more directive arrays. Most of them operate by scanning very quickly the covered frequency band. Thus, we can consider that their instantaneous frequency varies as a linear function of time. In laboratory, the corresponding sweeping sawtooth period, noted T, was measured close to 8 μs on several devices. Therefore, the whole covered frequency band is swept repetitively at this 8 μs period. Such a chirp signal can be generated using

$$x(t) = A\cos(2\pi\ f(t)\,t + \phi_0) \tag{1}$$

Where the time-varying frequency is given by

$$f(t) = \frac{k}{2}t + f_0 \tag{2}$$

With k, the rate of change between the minimum and maximum frequency noted f_1 and f_2 respectively, given by

$$k = \frac{f_1 - f_2}{T} \tag{3}$$

Let us consider the case of a jamming signal operating between 921 and 925 MHz with a continuous wave (CW) output power of 0 dBm. This frequency band is used in some countries as the GSM-R(ailway) downlink band for communicating from ground-to-trains, thereby delivering mandatory signaling data to the trains [9]. Other telecommunication protocols operating at similar frequencies could have been considered. Fig. 2 represents, in dashed line (a), the computed output signal using a CW signal at 921 MHz, and in solid line (b), the same signal swept over 4 MHz, between 921 and 925 MHz.

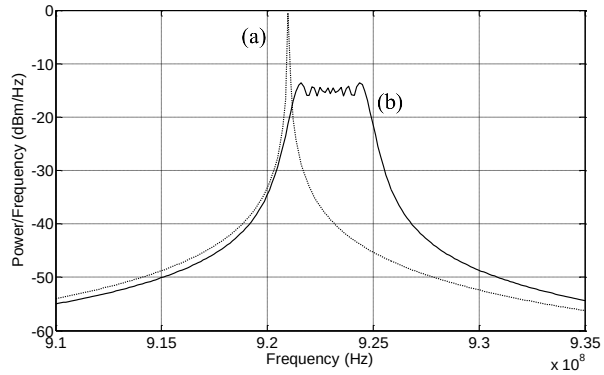

Fig. 2. Jamming signal (a) continuous wave, (b) swept over 4 MHz.

Compared to the CW case, we observe that, sweeping over the 4 MHz band, reduces the power spectral density (PSD) by a factor close to 13 dB, and that the jamming signal is almost constant in the swept band. In the rest of the paper we will use this jamming waveform as a reference and, to facilitate the further analysis, we will also assume that its PSD is constant over the whole swept band i.e., the 4 MHz used for the downlink data transfer.

Now, using the laboratory test bench presented in Fig. 3, we consider a communication established on a specific GSM-R channel, at a central frequency f. We use a GSM-R protocol emulator and analyzer noted CMU connected to a GSM-R mobile station (MS) [10]. On demand, we also inject a variable output power interfering CW signal coming from a radiofrequency signal generator also operating at frequency f. We evaluate its impact on the radio link.

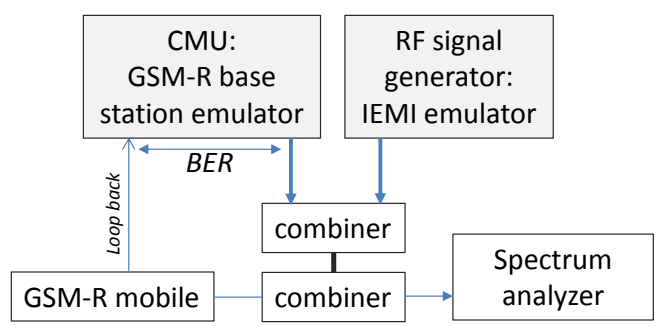

Fig. 3. Jamming impact evaluation test bench.

The measurement results are regrouped in Table I. The power levels delivered by the GSM-R transmitter and the jammer are indicated in columns 1 and 2 respectively. The resulting Signal to Interference Ratio (SIR) is mentioned in column 3 and the corresponding measured Bit Error Rate (BER) of the digital radio link appears in column 4. Loss of communication, noted Loss of com. in table I means that the communication is lost after applying the disturbing signal. No connection, noted no con. means that no connection at all can be established after the jamming signal is applied.

TABLE I
JAMMING SIGNAL IMPACT - MEASUREMENT RESULTS

P_Signal	P_Jammer	SIR	BER_*f1*
-38 dBm	-36 dBm	-2 dB	Loss of com./ No con.
-38 dBm	-37 dBm	-1 dB	12.5
-38 dBm	-38 dBm	0 dB	5.5
-38 dBm	-40 dBm	2 dB	2.1
-38 dBm	-42 dBm	4 dB	0.7
-38 dBm	-44 dBm	6 dB	0.2
-38 dBm	-46 dBm	8 dB	0.1

In these experimental conditions, we obtain that using similar received powers for the useful radio signal and for the interfering jamming signal leads to severe communication problems. Moreover, the transition zone between a satisfactory radio link and a loss of connection is abrupt, comprised in less than 2 dB in this experiment. This conclusion remains valid using various power levels instead of the -38 dBm reference signal power considered in Table I, column 1. Communication can be re-established after the jamming signal is stopped but it necessitates initiating a new connection. No damage to the test equipment was ever detected. Then, a fast sweeping signal of equivalent PSD in the communication channel used is selected instead of the CW signal. We obtain similar results when both jamming and useful signals have similar powers. A strong link deterioration quickly followed by a loss of connection are obtained at SIR lower than 0 dB. In this case also, communication can be re-established after the jamming signal is stopped but it necessitates initiating a new connection, and no damage to the test equipment was ever experienced. Following these experiments we will assume that, when the SIR level degrades and becomes negative, then a severe degradation quickly occurs for the tested radio protocol, including a complete loss of connection. Moreover, in the case of a connected communication mode, both downlink and uplink communications are lost simultaneously.

Otherwise, in [11], the author indicates that using the particular settings exploited on the presented railway network, losing the ground-to-train communication for more than 20 s, leads to an automatic activation of the emergency brake. Trains stop because no fresh data, including authorized speed setpoints at the current train location, are received. Moreover, in case where an emergency braking occurs, then an inspection must be launched to establish the origin of the incident. This will immobilize the train for a significant amount of time, including the fact that the IEMI origin of the problem could be difficult to establish afterwards. In the rest of this paper, we will consider this particular delay of 20 s after losing the connection to activate an emergency braking.

III. EVALUATION OF THE TRAIN RECEIVED POWER LEVELS

Although similar to a public cellular radio architecture, a dedicated railway cellular radio infrastructure presents a deployment only performed along the track. Fig. 4 represents such a longitudinal deployment using a succession of cells.

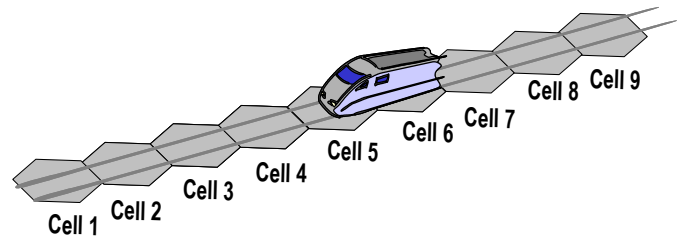

Fig. 4. Railway cellular radio deployment.

Base Stations (BSs) manage the ground-to-train communication in each cell. Medium power transmitters associated to directive Yagi antennas beaming to the direction of the track are used to maintain a sufficient radio coverage all along the railway infrastructure. Usually, spacing between two consecutive BSs ranges from 6 km to 12 km depending on the local radio clearance conditions and on the selected radio planning. For example, instead of using single Yagi antennas pointed at the following BS and covering the cell from one extremity, directive head to tail Yagi antennas can be installed on the same BS antenna mast, at the centre of the cell, to extend the radio coverage to both sides of the BS [12].

The frequency of GSM-R networks can differ slightly from country to country. In Europe, the 876 MHz to 880 MHz band is used for the uplink i.e, communication from the trains to the ground BSs, and the 921 MHz to 925 MHz bands for the downlink i.e., from the ground BSs to the trains. Channel spacing is 200 kHz [9]. In the previous section II, we have considered the case of a jamming signal operating between 921 and 925 MHz, therefore potentially jamming all the allocated downlink channels.

Railway EIRENE specifications [13] indicate that a minimum received power level of -92 dBm at a height of 3 m above the track must be maintained. Handover to the following BS is triggered by the network when the train is far from the communicating BS, and consequently when the received signal becomes of this low order of magnitude. Deployment techniques for an effective implementation of a dedicated railway cellular radio system are described in [12], and a dedicated railway ground-to-train radio propagation model is presented in [14]. However, for the purpose of this study, a simplified propagation model represented Fig. 5 is used.

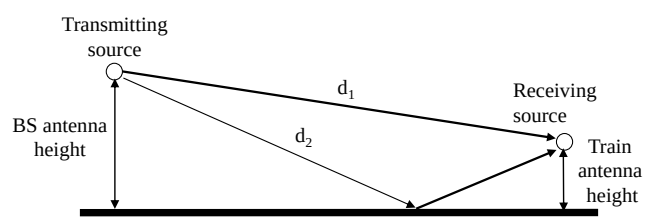

Fig. 5. 2 ray propagation model.

The model considers a direct path linking the transmitter to the receiver, and a second path corresponding to the signal reflected over a flat surface. The received power as a function of the distance d can be written according to [15]

$$P_r(d) = \frac{P_t\, G_t\, G_r\, h_t^2\, h_r^2}{d^4} \tag{4}$$

where P_t is the transmitted power, h_t and h_r are the heights of the transmit and receive sources respectively, and G_t and G_r are the gains of the transmitting and receiving antennas respectively. We selected $P_t = 8$ W i.e., +39 dBm, $G_t = 15$ dBi for the gain of the BS antenna gain in the direction of the track, and $G_r = 3$ dBi in the horizontal plane, for the gain of the train antenna. The BS antenna is situated at $h_t = 18$ m and the train MS antenna is located 3 m above ground. These values were considered representative of typical in situ conditions [12]. Moreover, both BS and train antennas are vertically polarized, and roof train antennas are almost omnidirectional in the horizontal plane. Therefore, we do not consider the effective presence of the train or a particular terrain model. Fig. 6 represents a simulation result obtained at 923 MHz. The minimum operationally acceptable received power of -92 dBm is also indicated by a horizontal dashed line.

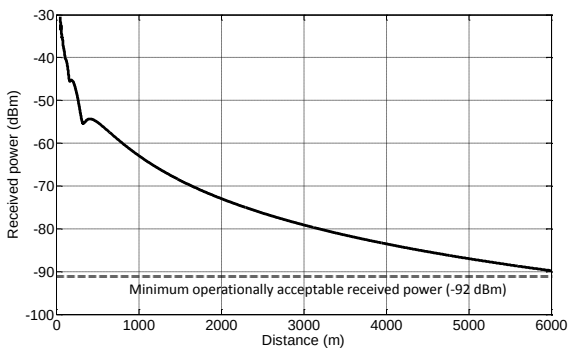

Fig. 6. Received power as a function of the train to BS distance.

We obtain a signal decreasing from the BS area down to the minimum operationally acceptable signal after 6 km. This simplified model cannot represent the fading conditions due to the interactions of the radiofrequency signal with a real railway environment.

We now consider the signal generated by the in-train jammer and received by the train roof antenna as depicted in Fig. 1. To estimate the received power, we use a simplified method associated to in situ measurements. We consider a 1 W or +30 dBm output power jammer. This may correspond to battery operated discreet equipment that can be activated in a pocket. Taking into account the results presented and discussed Fig. 2, we obtain that scanning over a 4 MHz band reduces the jammer power spectral density by a factor 13 dB that leads to a reduced +17 dBm PSD value all over the band. We also consider a jammer gain antenna of 3 dBi. With our theoretical scanning jamming signal and our preceding assumptions, we produce an equivalent jamming power of +20 dBm in any radio communication channel of the considered 4 MHz band. Moreover, since the jammer is inside the train, we also consider that we have steady coupling conditions between the in-train jammer and the train roof antenna, not affected by the train movement, passenger displacements, and other local perturbations. As previously, we consider that the train antenna gain is also 3 dBi in the direction of the jammer. To evaluate the overall coupling loss between the jammer and the train antenna, we first evaluate the free space coupling loss using the Friis transmission equation:

$$P_r = P_t\, G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 \tag{5}$$

Where P_t is the transmitted power, G_t and G_r are the gains of the transmitting and receiving antennas respectively, λ the considered wavelength and d the transmitter to receiver distance. At 923 MHz, for different train antenna to jammer equivalent free space distances, we obtain the values indicated in Table II, column 2. In this table, a minimum distance of 10 m is selected. At 923 MHz, this corresponds to more than 30 λ in the air, and the far-field, plane wave conditions, necessary to apply the Friis formula are considered to be verified. At this frequency, in situ measurements were also performed using a CW source associated to a vertically polarized omnidirectional antenna operating in the train. The received power from this signal is measured at the train roof antenna port. By moving the transmitting in-train antenna through the doors and windows from the inside to the outside of the train, we estimate the supplementary attenuation of the signal due to the shielding effectiveness of the train structure. We have tested different trains, different cars, and different locations in a car corresponding to several passenger seat locations. For each measurement, the outside location of the train antenna is selected to be as much as possible in a clear area at the roof train antenna height, and in line of sight of the train roof antenna. Although somewhat dependent of the train mechanical characteristics, we obtain a supplementary attenuation close to 20 dB, not really depending on the selected antenna location inside successive similar train cars. This constant figure is indicated in column 3. So, the total estimated coupling loss is now deduced by adding the free space loss and the supplementary train shielding effectiveness attenuation. These values are mentioned in column 4. Considering the output power of the jammer i.e., 20 dBm, and the train antenna gain i.e., 3 dBi, the corresponding estimated received jamming power by the train roof antenna is indicated in column 5.

TABLE II
JAMMER TO TRAIN ANTENNA ESTIMATED COUPLING LOSS

Jammer to antenna distance (d)	Free space loss	Additional train coupling loss	Total considered coupling loss	Train antenna received jamming power
10 m	51.7 dB	20 dB	71.7 dB	-48.7 dBm
50 m	65.7 dB	20 dB	85.7 dB	-62,7 dBm
100 m	71.7 dB	20 dB	91.7 dB	-68,7 dBm
200 m	77.7 dB	20 dB	97.7 dB	-74.7 dBm

We obtain that all these figures are much higher than the minimum operationally requested radio received power of -92 dBm. Therefore, jamming conditions will be severe over a more or less long part of the 6 km communication range represented Fig. 6.

Indeed, the Table II, column 1, 10 m jammer-to-train antenna distance could seem unrealistic since no passenger are

usually present in the locomotive, and train cars are situated farther than 10 m behind the train roof antenna. However, this distance merits attention if the passenger is on a platform, waiting for the train to start, and therefore sufficiently close to a locomotive. Moreover, in these conditions, the supplementary coupling loss due to the shielding effectiveness of the train structure should also be reduced since almost line of sight communication is realized. This 10 m distance could also be considered if, instead of a train, we consider the case of a tram or a subway train also receiving signaling data over radio. Indeed, in public transport vehicles, passengers can be very close to the driving cabin and associated antennas.

In this section, we have estimated the ground-to-train received signal as a function of the distance to the nearest BS. We have also evaluated the jamming power received by the train antenna as a function of the distance to the jammer. In the preceding section II we have shown that, if both jamming and useful signals are of similar powers, then the radio communication link can be severely affected and the train could stop because no updated control command data are received. We can now determine some critical communication areas corresponding to this condition, and evaluate several mitigation techniques.

IV. Evaluation of Critical Railway Zones

To visually evaluate these critical zones, we superimpose results similar to those presented in Fig. 6 and the constant jamming powers indicated in Table II, column 5. Let us consider the scenario of a jammer situated 100 m away, in the train. Fig. 7 presents the corresponding result.

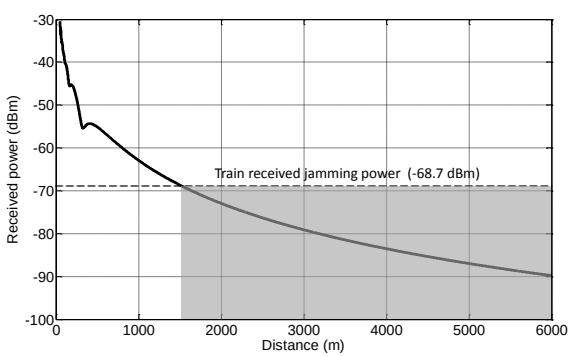

Fig. 7. Perturbed radio communication zone – No mitigation technique

We observe that the SIR is positive for the first part of the evaluated communication range, up to 1.5 km, and then becomes negative at longer communication ranges included in the grey zone. Therefore, 1.5 km after passing the BS, the communication becomes heavily impacted by the jamming signal, and the radio link could be interrupted. Moreover, if we recall the previous section II conclusion indicating that, as the SIR decreases, the transition zone between a satisfactory radio link and a loss of connection is abrupt i.e., in less than 2 dB then, the radio link could be broken very quickly after this critical 1.5 km distance.

Let us now consider a train running at a constant speed of 200 km/h and the particular railway network settings mentioned at the end of section II in which, after a 20 s time interval following a loss of communication, the train starts an emergency braking because of the loss of sufficiently recent control command data. At 200 km/h, the train will travel 1.1 km in 20 s. A realistic train braking deceleration value is 1 m/s^2. Using such speed and deceleration parameters, a train needs 55 s to stop. Within 55 s the train travels 1,512 m. Using these values, we estimate that the train could stop at the predictable distance of $1.5+1.1+1.5=4.1$ km after a jammer has been switched on in the vicinity of a BS. These values are recapitulated in Table III.

TABLE III
INITIAL BREAKDOWN OF DISTANCES BEFORE THE TRAIN STOPS

Jammer to antenna distance	Critical BS-train distance	Distance before braking	Braking distance	Train stopping distance from the BS
100 m	1.5 km	1.1 km	1.5 km	4.1 km

We conclude that mitigation techniques are necessary to avoid an emergency stop of the train. Different countermeasures can be envisaged. In the next section we will evaluate some of them operating at the physical layer.

V. Mitigation Techniques

In this section, we discuss the effectiveness of three different techniques. The first one considers a local increase in the ground-to-train transmitted power, locally triggered to increase the SIR. The second solution considers switching from the train front antenna to the train rear antenna to benefit from a larger attenuation between the train antenna and the jammer. The third one evaluates the effectiveness of using a high front-to-back ratio train antenna to reject in-train IEMI.

A. *Increasing locally the BS radiated power*

Adaptive power control schemes based on the optimization of transmitter power are used in any cellular radio system. They are exploited particularly to limit interference in the neighboring cells. In case of interference, the power used is increased to optimize the SIR. So, our first mitigation technique consists in improving the SIR level by increasing the useful signal level i.e., the BS transmitted power. Let us consider the same jamming condition than the one presented in the preceding Fig. 7. We evaluate the impact of a 6 dB increase in the BS output power. In our selected conditions, this corresponds to an output power of 45 dBm instead of 39 dBm. We obtain the result presented Fig. 8.

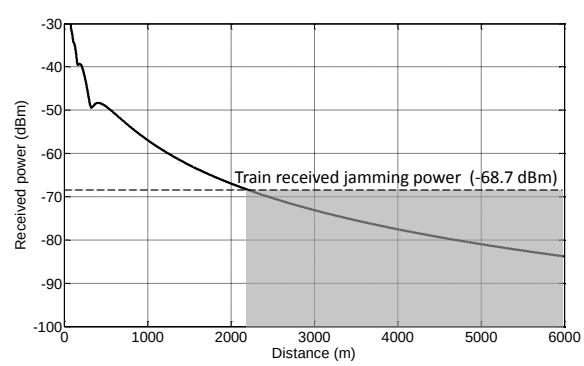

Fig. 8. Perturbed radio communication zone – Increasing the BS power.

We get a significant benefit, pushing the BS to train critical distance to 2.2 km, instead of 1.5 km without increasing the BS output power. The new breakdown of distances is displayed in Table IV.

TABLE IV

INCREASING THE BS OUTPUT POWER - BREAKDOWN OF DISTANCES

Jammer to antenna distance	Critical BS-train distance	Distance before braking	Braking distance	Train stopping distance from the BS
100 m	2.2 km	1.1 km	1.5 km	4.7 km

We conclude that this measure is effective if the jamming condition is detected sufficiently early to rapidly increase the BS output power, before the radio connection is lost. Interference in the neighboring cells due to this temporary increase of power should also be managed. Alternatively, more BSs could be installed with a smaller spacing between each of them. This would enable a minimum operationally received power higher than the low -92 dBm requirement indicated in the EIRENE specifications [13]. This alternative solution is considered to be costly.

B. *Switching from the front to the rear train antenna system*

Trains are often equipped with a locomotive at each extremity of the rolling stock. Using this architecture the train can be easily driven alternatively in either directions. Both locomotives are identically equipped. We can take benefit from these characteristics to select the train receiving equipment and associated antenna that produces the best SIR. Let us consider the example of a 300 m long train and a jammer located, as previously, 100 m from a train antenna. Therefore, the other train antenna is situated 200 m away. Using the Table II results we obtain that the jamming received power is -68.7 dBm at the nearest antenna and -74.7 dBm at the farthest antenna. We compute the new corresponding critical communication zone. This result is presented Fig. 9.

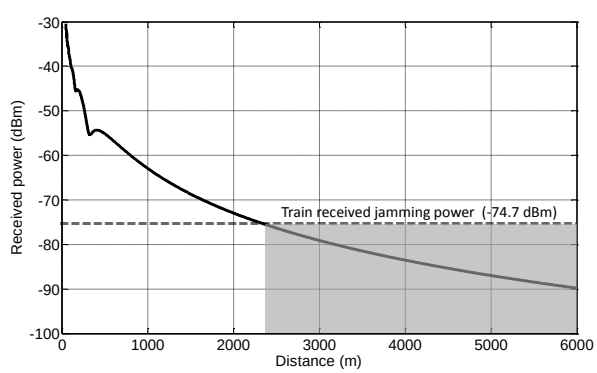

Fig. 9. Perturbed radio communication zone – Switching the train antenna.

Compared to Fig. 7, we obtain a significant benefit pushing the critical BS to train distance to 2.4 km, instead of 1.5 km. The new breakdown of distances is displayed in Table V.

TABLE V

SWITCHING THE TRAIN ANTENNA - BREAKDOWN OF DISTANCES

Jammer to antenna distance	Critical BS-train distance	Distance before braking	Braking distance	Train stopping distance from the BS
100 m	2.4 km	1.1 km	1.5 km	4.9 km

In this case also, the countermeasure is effective but does not fully solve the problem alone. As indicated, this countermeasure is only applicable in the case of trains equipped with a locomotive at each extremity of the rolling stock. This technique can also be exploited to facilitate the handover procedure between two consecutive BSs. Indeed, both train front and end equipment can be used to limit data loss during the switching between consecutive BSs.

C. *Using a high front-to-back train antenna*

Smart antennas have been widely deployed in modern wireless communication systems. They are used to improve the signal to interference/noise level and increase the frequency reuse rate effectively [16], [17]. They are also exploited to attenuate interference and jamming signals affecting satellite navigation receivers [18], [19]. We can select a smart antenna technique to mitigate the impact of an in-train jammer. Train roof antennas are generally vertically polarized along the vertical z axis and have an almost omnidirectional radiation pattern in the horizontal plane. They present a classical far-field, free space, toroidal shape radiation pattern in the horizontal plane. Although the roof of the train is generally not fully metallic, antennas are mounted on a metallic plane a few side wavelengths working as a reference plane. Since the jammer is situated in the train, we can try to attenuate the interfering signal by using, on demand, a high front-to-back (F/B) ratio train antenna at the rear of the train, receiving signals from the preceding BS, or inversely, a high F/B front train antenna, receiving signals from the next BS. This will attenuate the IEMI coming from the back of the antenna, in the direction of the train. This will also increase the received power from the communicating BS. Trains are generally running on large radius of curvature turns so, a broadly attenuated rear radiation lobe is sufficient.

To simulate such a modification, we choose to add reflectors behind the existing antenna. Two reflectors are considered located $0.15\,\lambda$ behind the vertical radiator and spaced $0.2\,\lambda$ from each other. They are adjusted to have a length of $0.35\,\lambda$ providing a broad and significant front-to-back ratio. We also extend the corresponding metallic reference plane to a square wavelength. At 923 MHz, using a NEC simulator [20], we get the radiation far-field patterns presented Fig. 10. We obtain a broad front radiation lobe and also a broad attenuated rear lobe.

With this directive antenna, the simulation computes a maximum front gain of 7.5 dBi and a front-to-back ratio of 19 dB, exactly to the rear of the antenna.

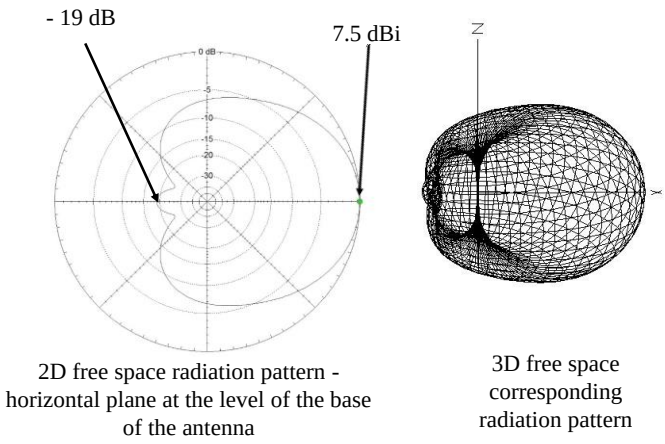

Fig. 10. 2D and 3D train antenna high F/B radiation patterns.

To evaluate conservative figures, we consider a forward gain limited to 3 dB and a front-to-back ratio limited to 15 dB. Thus, the signal is increased by a factor 3 dB and the interference is reduced by a factor 15 dB. Therefore, the jamming power received by the train antenna is now reduced to -83.7 dBm. We obtain the new results presented Fig. 11.

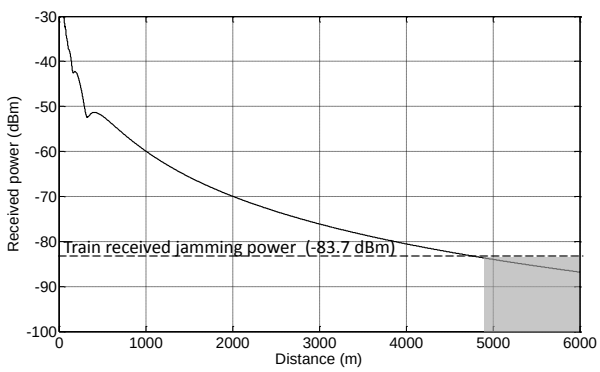

Fig. 11. Perturbed radio communication zone – Directive train antenna.

With these values, the jamming impact is largely reduced and the critical zone now only appears after 4.9 km. Table VI indicates the new breakdown of distances.

TABLE VI
MODIFYING THE TRAIN ANTENNA - BREAKDOWN OF DISTANCES

Jammer to antenna distance	Critical BS-train distance	Distance before braking	Braking distance	Train stopping distance from the BS
100 m	4.9 km	1 km	1.5 km	7.4 km

Looking at Table VI and using our selected parameters, we obtain that a train emergency braking could be triggered after an equivalent distance of 5.9 km after the BS i.e., in the vicinity of the following BS, 6 km from the previous one considering our selected BS spacing. Locally, this new BS delivers a stronger signal to the train antenna, providing a sufficient SIR to prevent any significant jamming. In this area, the communication with this next BS may continue if a successful handover between the two consecutive radio cells has been achieved adequately, despite interference, or, alternatively, if a new successful connection has been initiated. However, still in this case, if an emergency braking was triggered ahead, then the train will stop and an inspection of the train will be necessary. This will immobilize this train and successively all the following trains along the line, for a significant amount of time.

As we can deduce from these three different scenarios, the countermeasure using high front-to-back train antennas, or, more generally, smart antennas provides the best results. However, we have obtained that none of the considered mitigation techniques can separately fully solve the jamming problem studied. Accurately considering the operator specific implementation along its railway network, a cost effective combination of technical countermeasures inspired by the techniques proposed associated to adequate operational procedures can certainly be realistically implemented in order to efficiently harden the radio link.

VI. CONCLUSION AND PERSPECTIVES

Critical infrastructures must be strongly protected, and some of them are sensitive to IEMI. In this contribution, we have shown that low power IEMI can affect the railway infrastructure, notably by perturbing the ground-to-train radio communication link. Depending on the settings along his infrastructure chosen by the railway operator, low power IEMI can stop trains and an estimation of the stopped train location can be predicted. Different countermeasures developed to increase the SIR were evaluated. They can provide separately or combined significant improvements. Railway operators are now considering more and more this IEMI threats, and a whole set of relevant methodology, operational and engineering recommendations is discussed and presented in [21].

REFERENCES

[1] European Commission, "Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the fight against terrorism," Available: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52004DC0702

[2] US Official website of the Department of Homeland Security, "Critical Infrastructure Security," Available: https://www.dhs.gov/what-critical-infrastructure

[3] R. Rambousky, A. Bausen, S Lange, F. Sabath, "IEMI-testing of electronic systems in critical infrastructure surrounding," in *IEEE Int. Symposium on Electrom. Comp.*, Dresden, 2015.

[4] S. Runke, V. Hansen, J. Streckert, M. Clemens, K.-U. Rathjen, S. Dickmann," IEMI analysis of critical infrastructures by simulations using a multi-method coupling strategy," in *IEEE Int. Symposium on Electrom. Comp.*, Gothenburg, 2014.

[5] W. A. Radasky, C.E. Baum, M. W. Wik, "Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)", *IEEE Trans. Electromagn. Compat.*, vol. 46, no. 3, pp. 314-321, Aug. 2004.

[6] R. L. Gardner, "Electromagnetic Terrorism: A Real Danger," in *Proceedings of the XIth Symposium on Electromagn. Compat.*, Wroclaw, Poland, June 1998, pp. 10-14.

[7] D. J. Serafin , D. Dupouy, "Potential EIMI Threats Against Civilian Air Traffic," in *Proceedings of the URSI XXVIIIth General Assembly*, New Delhi, India, Oct. 23-29, 2005.

[8] D. Månsson, R. Thottappillil, M. Båckström and O. Lundén, "Vulnerability of European Rail Traffic Management System to Radiated Intentional EMI pulses," *IEEE Trans. Electromagn. Compat.*, vol. 50, no. 1, pp. 101–109, Feb. 2008.

[9] C. Beckman, K. Nilsson, "The Technical and Economic Consequences of Protecting GSM-R in Sweden," in *IEEE Vehicular Techn. Conf. (VTC Spring)*, Nanjing, 15-18 May 2016.

[10] M. Heddebaut, V. Deniau, J. Rioult, G. Copin, "Method for detecting jamming signals superimposed on a radio communication - Application to the surveillance of railway environments," in *IEEE Int. Symposium on Electrom. Compat.*, Dresden, 16-22 Aug. 2015.

[11] J. Cellmer, "Le réseau GSM-R de RFF," *Revue de l'Electricité et de l'Electronique* Vol. 3 Available https://www.see.asso.fr/fichier/4243_reseau-gsm-r-rff, 2012.

[12] L. M. Nemţoi, C. Mihail, A. L. Mureşan, "GSM-R radio planning for the Bucureşti - Constanţa railway corridor - Case study", in IEEE 16th Int. Symp. for Design and Technology in Electronic Packaging (SIITME), 23-26 Sep. 2010.

[13] European Union Agency for Railways, "GSM-R System Requirements Specification", Mandatory specification v16.0, 15 Jun. 2016. Available: http://www.era.europa.eu/Document-Register/Pages/Set-1-and-2-and-3-EIRENESRS.aspx

[14] Y. Ma, P. Du, X. Mao, Ch. Long, "On-line and Dynamic Estimation of Rician Fading Channels in GSM-R Networks," in *Int. Conf. on Wireless Commun. & Signal Proc. (WCSP)*, Oct. 2012.

[15] T. S. Rappaport, "*Wireless communications, principles and practice*," Prentice Hall, 1996.

[16] A. El-Zooghby, "*Smart Antenna Engineering*," Norwood", MA, Artech House, 2005, pp. 8-11.

[17] A. Osseiran and A. Logothetis, "Smart antennas in a WCDMA radio network system: Modeling and evaluations," *IEEE Trans. Ant. and Propag.*, Vol. 54, no. 11, pp. 3302–3316, Nov. 2006.

[18] S. Durrani, M. E. Bialkowski, "Interference rejection capabilities of different types of array antennas in cellular systems, *Electronics Letters*, Vol. 38, Issue: 13, pp. 617– 619, 2002.

[19] X. H. Wang, X. W. Shi, P. Li, Y. F. Bai, B. Liu, R. Li, H. J. Lin, "Smart antenna design for GPS/GLONASS anti-jamming using adaptive beamforming", in *Int. Conf. on Microwave and Millimeter Wave Techn. (ICMMT)*, Chengdu, 8-11 May 2010.

[20] J. E. Richie, H. R. Gangl, "EFIE-MFIE hybrid simulation using NEC: VSWR for the WISP experiment," *IEEE Trans. on Electrom., Compat.*, Vol. 37, Issue 2, May 1995.

[21] "Security of railways against electromagnetic attacks," White paper, Available http://www.secret-project.eu/IMG/pdf/white_paper_security_of_railway-against_em_attacks.pdf