Intentional Electromagnetic Interference Through Saturation of the RF Front End

Stefan van de Beek[#1], Robert Vogt-Ardatjew[#2], Frank Leferink[*3]

[#]*Telecommunication Engineering, University of Twente*
Enschede, The Netherlands
[1]g.s.vandebeek@utwente.nl
[2]r.a.vogtardatjew@utwente.nl
[*]*Thales Nederland B.V.*
Hengelo, The Netherlands
[3]f.b.j.leferink@utwente.nl

Abstract—**There is an increasing use of wireless applications in today's society. A big disadvantage of wireless communication is the high vulnerability to denial-of-service (DoS) attacks. Intentional electromagnetic interference can saturate, and thereby block and desensitize, the wireless receiver. This mechanism of causing a DoS is different from well-studied jamming attacks. It is important to determine and quantify saturation levels of a receiver. The saturation is quantified by the 1-dB compression point, $P_{1\text{-}dB}$. An experimental method is presented that can determine $P_{1\text{-}dB}$ over a wide frequency band in a fast and accurate way. Results show the need for a high quality front door filter to be robust against out-of-band interference.**

I. Introduction

The use of wireless applications in today's society has increased steeply. Wireless networks are widely being deployed and the dependence of society upon these networks is growing. In a white paper released by Cisco [1], it is estimated that the number of mobile-connected devices has exceeded the world's population in 2014. The obvious advantage of wireless communications is the flexibility it provides to the end user, additionally, it is becoming more affordable. However, a big disadvantage of wireless communication is the high vulnerability to denial-of-service (DoS) attacks.

Wireless communication is very vulnerable to DoS attacks because of the use of antennas and the open access nature of the wireless medium. Antennas are an easy point of entry for electromagnetic interference that disrupts the communication. These type of DoS attacks can be defined as intentional electromagnetic interference (IEMI) [2].

The most obvious attack against wireless communication is an in-band jamming signal that decreases the signal-to-noise ratio (SNR), resulting in masking the information signal such that it cannot be detected by the receiver. There are many different jamming techniques and they have been extensively studied [3]-[6]. The most common anti-jamming technique makes use of spread spectrum technology, such as frequency hopping or direct sequence spread spectrum [7]. Anti-jamming techniques increase robustness, however, it is impossible to make a wireless system completely insensitive against jamming attacks.

A more crude way of disrupting wireless communication is described in [8]. This work is focused on high power IEMI that can damage the receiver. Typically, the RF front end of a receiver is designed to operate on very weak signals received by the antenna. High power interference can relatively easy burn out the low-noise-amplifier (LNA), resulting in permanent damage. Another example of IEMI that can lead to a DoS is the saturation of the RF front end. A strong interferer can result in blocking and desensitization of the receiver [9]. Anti-jamming techniques such as spread spectrum communications are useless against this type of IEMI. In this paper, we will focus on IEMI attacks with the goal of saturating the receiver.

Whereas a jamming signal needs to be in-band of the communication signal to cause a DoS, this is not per se necessary for an interferer that saturates the receiver. For this reason, it is important to know the saturation levels of the receiver over a wide frequency band. In most standards it is required that a receiver must comply with a certain blocking template. For instance, in terrestrial trunked radio (TETRA), it is described in the testing specifications that a desired signal only 3 dB above the sensitivity level should be correctly received; even if accompanied by an out-of-band (OOB) blocker as large as -25 dBm [10]. This test has a pass or fail outcome and gives no information on the power levels at which the receiver starts to cause problems. In this paper, we present an experimental method that can be used to quantify and measure the saturation level of a receiver as a function of frequency in a fast and accurate way. This gives an estimate of the robustness of the receiver against a DoS attack via blocking and desensitization of the receiver.

In the next section, we explain how the saturation of receiver can be quantified and the effect of saturation on the information signal. In Section III, the experimental method we use to measure saturation is explained. Results of measurements performed on a commercial-off-the-shelf (COTS) receiver to estimate its robustness against saturation are presented in Section IV. Finally, conclusions are drawn and recommendations are given.

978-1-4799-6670-7/15/$31.00 Copyright 2015 IEEE

II. Analysis of RF Saturation

Saturation of a wireless receiver can only be achieved with power levels greatly exceeding the power level of the nominal signal power. From an adversary point of view, the advantage of blocking the receiver in comparison with jamming, is that no accurate knowledge of the communication signals frequency is required, and it is not affected by spread spectrum techniques. The high selectivity of a receiver is not at the RF frequencies, so the first components are susceptible in a relatively wide frequency band. The low-noise-amplifier (LNA) or mixer are most often the responsible receiver components for saturation of the front end.

Saturation of a system will often lead to compressive behavior, i.e., decreasing gain for increasing input amplitude. This effect can be quantified by the 1-dB compression point, $P_{1\text{-}dB}$, defined as the input signal power that causes the gain to decrease by 1 dB (10% voltage gain reduction) [11]. In Fig. 1, $P_{1\text{-}dB}$ is graphically explained. At $P_{1\text{-}dB}$ the output power is 1 dB less than its ideal value. The effect of gain compression is larger with amplitude modulation than with phase modulation, since gain compression only affects the amplitude of the signal. The 1-dB compression point of a receiver is often frequency dependent.

In the case of IEMI, a large interfering signal accompanies the desired information signal. The relatively small desired signal is superimposed on the large interferer. The large signal could saturate the receiver, and as a result, the desired signal will experience a reduced gain. This well-known phenomena can be attributed to the third-order nonlinearity of a memoryless system with an input/output characteristic approximated by

$$y(t) \approx \alpha_1 x(t) + \alpha_2 x^2(t) + \alpha_3 x^3(t), \qquad (1)$$

where $y(t)$ is the output signal, $x(t)$ the input signal, and α_1, α_2, and α_3 are the coefficients. Now assume $x(t) = V_1 \cos\omega_1 t + V_2 \cos\omega_2 t$, where the first term represents the desired signal, and the second term the interferer. If we substitute this in (1), and assume $V_1 \ll V_2$, the output at frequency ω_1 appears as

$$y(t) \approx \left(\alpha_1 + \tfrac{3}{2}\alpha_3 V_2^2\right) V_1 \cos\omega_1 \,. \qquad (2)$$

Assuming $\alpha_1\alpha_3 < 0$, it is easy to see from (2) that the gain experienced by the desired signal is a decreasing function of V_2. This effect is called desensitization and it lowers the SNR at the receiver output, e.g., the noise contribution of the following baseband blocks is increased. For a sufficiently large V_2, the gain can even drop to zero and the desired signal is completely blocked. Another important phenomenon with a strong interferer accompanying a desired signal is called cross modulation. It is easily explained by (2) if the amplitude of V_2 is time varying, this variation can be seen in transfer of the desired signal at ω_1.

To protect a receiver from saturation and the accompanying negative effects, it is important to have a high dynamic range, so that it can still properly receive a very small signal, and at the same time a very strong signal can still be accurately processed or filtered in later stages of the receiver chain. Secondly, it is important to have a sharp front door filter to remove OOB interferers before they can reach the electronics. The most often used filter is an external surface acoustic wave (SAW) filter. However, as discussed in [12], a SAW filter is often not preferred for cost reasons and because it has a relative high insertion loss, typically 2 - 3 dB [12].

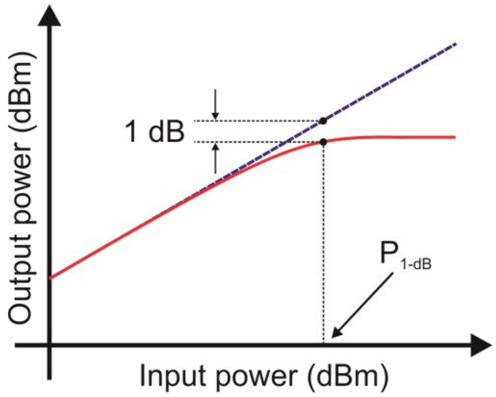

Fig. 1 Graphical representation of $P_{1\text{-dB}}$. The output power is plotted as a function of the input power.

III. Experimental Method

It is important to know the $P_{1\text{-}dB}$ of a receiver over a wide frequency band. This information can be used to estimate the robustness of a wireless receiver against saturation due to IEMI, and it can set requirements upon the front door filter that should be implemented. In this section, we present a method to measure the compression levels of a receiver front end over a wide frequency interval.

At single frequency point, the gain curve of the front end can be measured by directly feeding a continuous wave (CW) signal to the input of the receiver, and measure the output power of the front end using a spectrum analyzer. If we make a power sweep at the input, while monitoring the output power, we can plot the measured gain curve next to the extrapolated small signal curve. The plot will be comparable to Fig. 1 and the $P_{1\text{-}dB}$ can be derived. However, if we want to compute the compression levels over a wide frequency band, this is very cumbersome, since we have to measure the gain curve for every frequency point.

The method we use is based on the requirements for the control of EMI characteristics of electronic equipment described in [13]. The basic concept is to apply OOB signals while monitoring the receiver for degradation, but only a very general test set-up is shown, and it is not specified how to quantify the degradation of the receiver. It is stated that the required test equipment, setup, procedures, and data presentation should be determined on a case-by-case basis. We want to quantify the receiver by measuring $P_{1\text{-}dB}$ for many frequency points.

The schematic of the test set-up we use to measure the compression levels over a wide frequency band is given in Fig. 2. It is a conducted susceptibility test to get accurate results. The description of the method is as follows: generator 2 generates the in-band desired signal while generator 1 generates the EMI. The power of the desired signal should be well within the linear region of the amplifier. To determine $P_{1\text{-}dB}$, first, generator 2 is transmitting a low power continuous wave (CW), which is the desired signal, and the output power of the front end is measured with a spectrum analyzer, in this case spectrum analyzer 2. Next, generator 1 is switched on and starts transmitting a CW, the interferer, at the frequency of interest. The power of the interfering signal is gradually increased until the output power of the desired signal measured by spectrum analyzer 2 is decreased by 1 dB, i.e., 1-dB compression. The $P_{1\text{-}dB}$ is determined by measuring the input power of the interfering signal with spectrum analyzer 1. The procedure is repeated for every frequency point of interest, and as a result, we get the $P_{1\text{-}dB}$ as a function of frequency.

It is important to verify that the signals at the input of the front end are only the intended signals. For this reason the set-up includes filters, 6-dB attenuators, and a directional coupler. The filters are connected, if necessary, to the output of the generators to filter the possible spurious harmonics generated in the signal generators. The generators are connected to the 6-dB attenuators, which function as wideband isolators, to prevent unwanted reflection affecting the signals. Dedicated isolators are often not suited for this measurement, because they are narrowband and the measurements we perform can be extremely wideband. A resistive splitter can be used as a wideband combiner. The resistive splitter we use has a loss of 6 dB from one port to another, whereas a 3-dB combiner only has 3-dB loss. Again, a 3-dB combiner is often not suited for this measurement, because they are narrowband and are therefore unable to combine two signals with a large frequency difference. Finally, a directional coupler is used to verify that the signals appearing at the input of the front end are actually the intended signals, and to monitor the power of the interference.

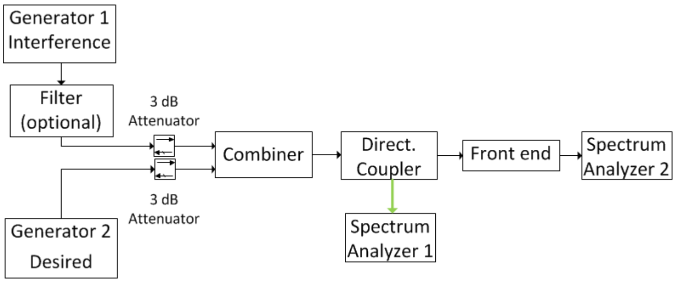

Fig. 2 Measurement set-up for determining $P_{1\text{-dB}}$.

IV. Experimental Results

For demonstration purposes the 433 MHz evaluation kit of the MAX1470 superheterodyne receiver has been purchased and evaluated [14], [15]. This type of receiver finds its application in remote keyless entry systems, garage door openers, remote controls, and more. It is a low cost heterodyne receiver tuned to 433.92 MHz to demodulate on-off-keying (OOK) modulated signals. Further information on a superheterodyne receiver architecture can be found in [11]. This receiver has an image-reject mixer that mixes the signal to an intermediate frequency (IF) of 10.7 MHz. It is stated in the data sheet that because of the image-reject mixer the need for a costly front end SAW filter is eliminated. The evaluation kit only has a series inductor (L) and capacitor (C) tuned to 433.92 MHz at the input of the receiver prior to the LNA. The lack of a front end filter makes this receiver vulnerable to saturation for signals over a wide frequency band.

The MAX1470 evaluation kit makes it possible to measure the transfer from the input of the receiver to the output of the mixer. Thus, compression measurements were performed over the cascaded LNA and mixer. First, the gain curve was measured at 433.92 MHz. The input power of the receiver was increased with steps of 1 dB from -90 dBm up to -25 dBm. The output power was monitored with a spectrum analyzer. The result is depicted in Fig. 3. As can be seen, the output power flattens from approximately -35 dBm input power. The power gain shows the compressive behavior as expected.

Compression measurements over a wide frequency interval were conducted according to Fig. 1. The $P_{1\text{-}dB}$ was determined from 80 MHz up to 670 MHz. For higher frequencies the signal generator did not have enough power to bring the receiver into saturation. The in-band desired signal had a power of -60 dBm at the input of the receiver. The small signal gain of the front end is 20 dB, so for this input signal we measured an output signal of -40 dBm. The compression was monitored over this output signal, while the interference frequency and power was being swept. The results of the measurements are depicted in Fig. 4. It can be seen that the receiver has a valley in $P_{1\text{-}dB}$ from 425 MHz to 435 MHz. This is expected because the receiver is tuned to this frequency range. However, we can also see that the OOB compression levels are relatively low, e.g, -15 dBm at 200 MHz. These type of results are very well suited to determine vulnerability against OOB interference, and determine attenuation levels of a receiver.

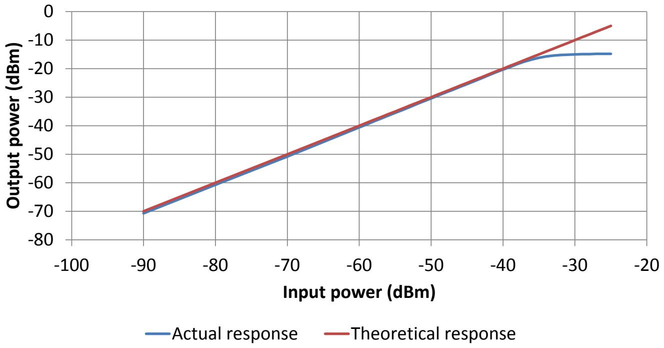

Fig. 3 Gain curve of the MAX1470 front end at 433.92 MHz.

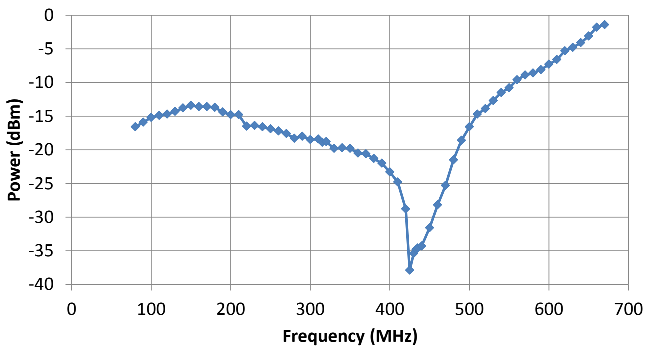

Fig. 4 $P_{1\text{-}dB}$ of the MAX1470 front end as a function frequency.

V. Conclusions

In this paper, we discussed the effect of an IEMI attack that aims at saturating the receiver. This type of attack can cause DoS by blocking the receiver and the mechanism is different from a jamming attack. Spread spectrum techniques do not improve robustness against strong interferers that desensitizes the receiver.

The experimental method presented can give a good estimate of the saturation levels of a receiver. This can be quantified by the 1-dB compression levels over a wide frequency band. As long as the power of the interference is below the $P_{1\text{-}dB}$ the interferer can be processed or filtered in later stages of the receiver chain. The results give an estimate of the robustness of the receiver against this type of IEMI attack.

Hardening a wireless receiver from saturation is only possible with a high dynamic range, and a strong attenuation of OOB signals. For this reason high quality front door filters are necessary, but for cost reasons they are not always incorporated in the receiver.

Acknowledgment

The research leading to these results has received funding from the European Union Seventh Framework Programme under grant agreement number FP7-SEC-2011-285257.

References

[1] *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2018*, white paper, Cisco, 2014.

[2] S. van de Beek, R. Vogt-Ardatjew, and F. Leferink, "Robustness of remote keyless entry systems to intentional electromagnetic interference," *in Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on*, 2014, pp. 1242-1245.

[3] W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," *MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp.*, 2005, pp. 46–57.

[4] X. Wenyuan, M. Ke, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *Network, IEEE*, vol. 20, pp. 41-47, 2006.

[5] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *Communications Surveys & Tutorials, IEEE,* vol. 11, pp. 42-56, 2009.

[6] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," *Communications Surveys & Tutorials, IEEE*, vol. 13, pp. 245-257, 2011.

[7] R. A. Poisel, *Modern Communications Jamming Principles and Techniques, Second Edition*. Norwood: Artech House, 2011.

[8] D. Mansson, R. Thottappillil, M. Backstrom, and O. Lunden, "Vulnerability of European Rail Traffic Management System to Radiated Intentional EMI," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 50, pp. 101-109, 2008.

[9] R. G. Meyer and A. K. Wong, "Blocking and desensitization in RF amplifiers," *Solid-State Circuits, IEEE Journal of*, vol. 30, pp. 944-946, 1995.

[10] ETSI EN 300 394-1, V3.1.1, *Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 1: Radio,* 2007.

[11] B. Razavi, *RF Microelectronics Second Edition.* Upper Saddle River: Pearson Education Inc., 2012.

[12] H. Darabi, "A blocker filtering technique for SAW-less wireless receivers," *Solid-State Circuits, IEEE Journal of,* vol. 42, pp. 2766-2773, 2007.

[13] MIL-STD-461E, *Department of Defense Interface Standard – Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment*, 1999.

[14] "MAX 1470 Superheterodyne Receiver data sheet," Maxim Integrated Products, Sunnyvale, CA, USA.

[15] "MAX 1470 Evaluation Kit data sheet," Maxim Integrated Products, Sunnyvale, CA, USA.