Water-Filling for Friendly Wide-Band Jamming

1st Werner Henkel, *senior member, IEEE*
werner.henkel@ieee.org

2nd Lynda W. Mwema
lmwema@constructor.university

3rd M. Ahmed Leghari
m.leghari@jacobs-university.de

Computer Science and Engineering
Constructor University Bremen
Bremen, Germany

***Abstract*—We are deriving "Water-Filling" in the realm of jamming with a power constraint. In contrast to the conventional Water-Filling, not the signal power is distributed given a power constraint, but a jamming power is distributed with a corresponding constraint. Instead of the channel capacity, the secrecy capacity is maximized. Additionally, we also apply a minimum mean squared criterion for jamming power distribution as a counterpart to applying it to equalization and precoding. The jamming power is allocated such that it outperforms a simple flat jamming spectrum.**

As an example, we discuss eavesdropping with a near-field probe. Friendly jamming of this form can reduce leakage to an eavesdropper. To illustrate the procedure, we use USB 2.0 signal spectra, despite of the fact that the independence assumption is violated that one makes use of in Water-Filling. Furthermore, we use the loop of shield and ground to radiate our jamming signal. Later applications that we envisage are, however, on-chip or on-board eavesdropping with dedicated RF designs, also ensuring that interference to other systems will be negligible.

***Index Terms*—Eavesdropping, jamming, TEMPEST, near-field probe**

I. Introduction

As part of our "TEMPEST" [1], [2] (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions) activities, we considered near-field scanning of typical broadband PC signals, trying to classify the type of signal up to synchronizing to it. Near-field probes exist as E-field or H-field counterparts [3]–[5], where the latter is simply a coil with a single turn offering directional properties, picking up signals on a conductor that is in parallel to the direction of the plane of the probe. One may classify the signal, e.g., based on time-frequency representations or special signal properties. The latter can then be used to synchronize to those signals and finally detect them. Intentional (friendly or cooperative) jamming may be used to protect against eavesdropping. One example of such works is [6], where the authors combine legitimate signal and interference, cooperatively, in a way that an eavesdropper is not able to recover the legitimate signal. Other approaches in narrow-band applications use separate spatial dimensions for signal and jamming, putting the jamming signal into the null space of the legitimate channel [7]. In [8], additional to spatial dimensions, includes also correlation properties to maximize secrecy capacity. It also provides a literature review for cooperative jamming in wireless, also regarding options for jamming power allocation. [9] uses mutual information and the MMSE to optimize jamming and signals for radar applications. However, this is not about friendly or cooperative jamming, nevertheless, addresses criteria from Information Theory and Signal Processing, which we do, as well. Bounds and closed-form solutions for MIMO (Multiple-Input Multiple-Output) systems optimizing secrecy capacity are provided in [10].
Otherwise, jamming is, of course, usually applied to disturb the legitimate transmission itself, be it by narrow-band or sinusoidal strong signals or impulsive ones, up to synchronizing to CDMA sequences to appear as a legitimate user (repeat-back jamming). Mostly also this concerns modulated wireless transmission. We, however, consider broadband baseband signals. Directional properties as with the mentioned antenna arrays for RF transmission to direct jamming signals into certain directions, are not an option for broadband signals. Instead, one may use separate conductors to emit jamming fields stronger than the to be protected legitimate signal, still not strongly disturbing the legitimate transmission.

Given a certain amount of power, the question arises, how to shape the spectrum to efficiently make use of it to harm a possible eavesdropper, but less so the legitimate channel. From Information Theory, we know power distribution over independent user channels maximizing channel capacity as "Water-Filling" [11]. For our eavesdropping situation representing Wyner's wiretap channel [12]–[14], we will maximize secrecy capacity. As an alternative, we will also apply an MMSE (Minimum Mean-Squared Error) criterion to define the optimum power distribution.

For illustration – not to propose it for a practical implementation –, we consider a shielded USB cable which has differential lines called D+ and D− plus a pair for power supplies and, of course, the shield. We considered Full (12 Mb/s) and High-speed (480 Mb/s) USB [15]. Usually, the shield is connected to the ground wire, at least, through a capacitor. When comparing the transfer function between the differential wires (D+/D−) to an external H-field probe (see, Fig. 1) and between a ground-shield (GS) loop and the probe, dependent on the probe location, one can observe higher emissions from the GS loop in certain frequency ranges. This allows for higher efficiency of jamming at those frequencies.

We gratefully acknowledge funding by the Federal Ministry for Economic Affairs and Energy (BMWi) under the ZIM program

We will derive the optimum power allocation of a jamming signal minimizing the mutual information to the eavesdropper. We are not (yet) optimizing jamming towards other signal properties, especially not targeting header sequences or the special common mode component in the packet ends of Full-speed USB.

In the following Section II, we will outline the involved channels and determine the secrecy capacity, followed by its optimization in Section III. Results for our USB illustration example are shown in Section IV. The alternative MMSE-based treatment follows in Section V, and we conclude with Section VI.

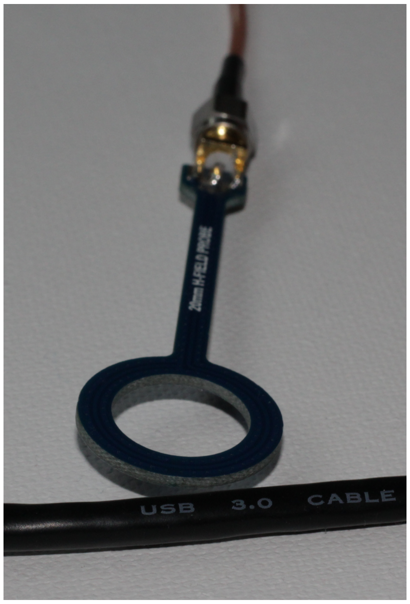

Fig. 1. H-field probe at USB cable

II. Jamming wiretap channel and secrecy capacity

As shown in Fig. 2, let us consider transmission between Alice and Bob with a transfer characteristic, described by the convolution Toeplitz matrix $\mathbf{H}_{AB}$, likewise the channel to Eve as $\mathbf{H}_{AE}$. Jamming to Bob and Eve experiences the channels $\mathbf{H}_{JB}$ and $\mathbf{H}_{JE}$, respectively.

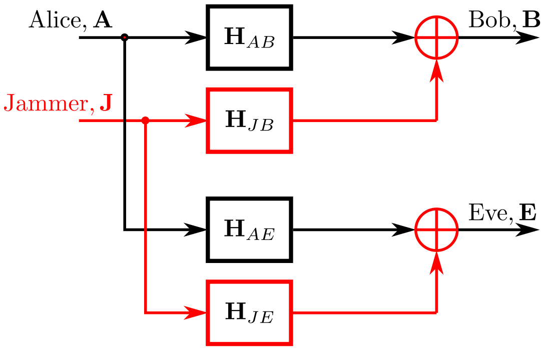

Fig. 2. Jammer and Wiretap channels

We neglect additional noise that would be added at all terminals. We essentially obtain Wyner's wiretap channel [12]–[14] with the corresponding secrecy capacity

$$C_s = \max_{P_a}[I(A;B) - I(A;E)]. \tag{1}$$

After addressing the complete secrecy capacity expression in (1), we will also simplify to minimizing $I(A;E)$ (maximizing $-I(A;E)$), the leakage to Eve, alone. Hereto, the assumption is that the jamming effect onto the legitimate channel is not significant. This will require corresponding designs and is actually not valid for our chosen USB illustration example.

For N independent channels, from (1), we obtain

$$C_s = \sum_{i=1}^{N} \max_{P_{a_i}}[I(A_i;B_i) - I(A_i;E_i)]. \tag{2}$$

Assuming the channels to be AWGN,

$$\begin{aligned} C_s \;=\; & \sum_{i=1}^{N} \frac{1}{2}\log\left(1 + \frac{S_i|H_{AB_i}|^2}{N_{J_i}|H_{JB_i}|^2 + N_{\beta_i}}\right) \\ & -\frac{1}{2}\log\left(1 + \frac{S_i|H_{AE_i}|^2}{N_{J_i}|H_{JE_i}|^2 + N_{\epsilon_i}}\right), \end{aligned} \tag{3}$$

where H_{AB_i} and H_{AE_i} are the transfer functions for the twisted pair cable channel between Alice and Bob and the probing channel from Alice to Eve, respectively, and H_{JB_i} and H_{JE_i} are transfer functions from the Jammer to Bob and Eve, respectively. N_{J_i} are the jamming power contributions.

III. Jamming power distribution

In the following, we constrain the overall jamming power to be P_J to be distributed among the channels (frequencies) to minimize leakage to the eavesdropper.

$$\sum_{i=1}^{N} N_{J_i} = P_J. \tag{4}$$

For simplicity, we replace $\log$ by $\ln$ in (3) and neglect the background noise contributions N_{β_i} and N_{ϵ_i}.

$$\begin{aligned} \text{maximize}: \; & \sum_{i=1}^{N} \frac{1}{2}\ln\left(1 + \frac{S_i|H_{AB_i}|^2}{N_{J_i}|H_{JB_i}|^2}\right) \\ & -\frac{1}{2}\ln\left(1 + \frac{S_i|H_{AE_i}|^2}{N_{J_i}|H_{JE_i}|^2}\right) \\ \text{subject to}: \; & P_J - \sum_{i=1}^{n} N_{J_i} = 0. \end{aligned} \tag{5}$$

To obtain N_{J_i}, we determine

$$\begin{aligned} & \frac{\partial}{\partial N_{J_i}}\left[\sum\nolimits_{i=1}^{N} \frac{1}{2}\ln\left(1 + \frac{S_i|H_{AB_i}|^2}{N_{J_i}|H_{JB_i}|^2}\right)\right. \\ & \left. -\frac{1}{2}\ln\left(1 + \frac{S_i|H_{AE_i}|^2}{N_{J_i}|H_{JE_i}|^2}\right) + \lambda\left(P - \sum_{i=1}^{n} N_{J_i}\right)\right] = 0. \end{aligned} \tag{6}$$

From Eq. (6), we obtain

$$\begin{aligned}&\frac{|H_{AE_i}|^2 S_i}{2|H_{JE_i}|^2 \cdot \left(\frac{|H_{AE_i}|^2 S_i}{|H_{JE_i}|^2 N_{J_i}} + 1\right) N_{J_i}^2} \\ &- \frac{|H_{AB_i}|^2 S_i}{2|H_{JB_i}|^2 \cdot \left(\frac{|H_{AB_i}|^2 S_i}{|H_{JB_i}|^2 N_{J_i}} + 1\right) N_{J_i}^2} - \lambda = 0\end{aligned} \tag{7}$$

One recognizes a quadratic equation in N_{J_i}, but refrain from rewriting it into the typical form to avoid another lengthy expression, but instead will formulate the solution as

$$\begin{aligned}N_{J_i} =& \frac{1}{4|H_{JE_i}|^2|H_{JB_i}|^2} \cdot \\ &\cdot \left\{ \left[\frac{4|H_{JE_i}|^2|H_{JB_i}|^4 S_i}{\lambda} |H_{AE_i}|^2|H_{AB_i}|^2| \right.\right. \\ &+ 4S_i^2 \left(|H_{JB_i}|^2|H_{AE_i}|^2 + |H_{AB_i}|^2|H_{JE_i}|^2\right)^2 \\ &\left. - 8S_i^2|H_{AB_i}|^2|H_{JE_i}|^2|H_{JB_i}|^2|H_{AE_i}|^2 \right]^{\frac{1}{2}} \\ &\left. - 2|H_{JB_i}|^2|H_{AE_i}|^2 S_i - 2|H_{AB_i}|^2|H_{JE_i}|^2 S_i \right\}\end{aligned} \tag{8}$$

Applying a simple search for a “suitable” λ that fulfills the side condition (4) and picking those solutions with positive square root arguments and positive N_{J_i} deliver the final jamming power distribution. One may, of course, go for search algorithms like, e.g., Nelder-Maed Downhill Simplex or Differential Evolution with some modification to avoid moving outside valid regions.

In case, one would only consider the leakage to Eve, i.e., the 2nd term in (3), one can apply the Newton method for finding the optimum. The corresponding derivation steps will be outlined in the sequel.

Equation (7) will then simplify to

$$\begin{aligned}&\frac{S_i|H_{AE_i}|^2}{2({N_{J_i}}^2|H_{JE_i}|^2 + S_i|H_{AE_i}|^2 N_{J_i})} - \lambda = 0 \,, \\ &{N_{J_i}}^2 + \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} N_{J_i} - \frac{S_i|H_{AE_i}|^2}{2\lambda|H_{JE_i}|^2} = 0 \,.\end{aligned} \tag{9}$$

We would then obtain N_{J_i} as

$$\begin{aligned}N_{J_i} =& -\frac{1}{2} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} \\ &+ \sqrt{\frac{1}{4}\left(\frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}\right)^2 + \frac{1}{2\lambda} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}},\end{aligned} \tag{10a}$$

$$N_{J_i} = \frac{1}{2} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} \left[-1 + \sqrt{1 + \frac{2}{\lambda} \cdot \frac{|H_{JE_i}|^2}{S_i|H_{AE_i}|^2}}\right]. \tag{10b}$$

By Eq. (10a), Eq. (4) is written as

$$\begin{aligned}&\sum_{i=1}^{N} -\frac{1}{2} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} + \\ &+ \sqrt{\frac{1}{4}\left(\frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}\right)^2 + \frac{1}{2\lambda} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}} = P_J \,.\end{aligned} \tag{11}$$

Rewriting Eq. (11) yields

$$\begin{aligned}&\sum_{i=1}^{N} \sqrt{\frac{1}{4}\left(\frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}\right)^2 + \frac{1}{2\lambda} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}} = \\ &\qquad = P_J + \sum\nolimits_{i=1}^{N} \frac{1}{2} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} \,.\end{aligned} \tag{12}$$

Equation (12) can be approximated as

$$\begin{aligned}&\sum_{i=1}^{N} \frac{1}{\sqrt{2}} \left[\frac{1}{2} \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} + \sqrt{\frac{1}{2\lambda} \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}}\right. \\ &\qquad \le P_J + \sum_{i=1}^{N} \frac{1}{2} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} \,,\end{aligned} \tag{13}$$

having used

$$\sqrt{a^2 + b^2} \ge \frac{1}{\sqrt{2}}(|a| + |b|) \,, \tag{14}$$

a lower bound obtained from the Cauchy-Schwarz inequality. From Eq. (13), one obtains

$$\begin{aligned}&\sum_{i=1}^{N} \frac{1}{2\sqrt{2}} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} + \sqrt{\frac{1}{4\lambda}\left(\frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}\right)} \\ &\quad \le P_J + \sum_{i=1}^{N} \frac{1}{2} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} \,, \\ &\sum_{i=1}^{N} \sqrt{\frac{1}{4\lambda} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}} \\ &\quad \le P_J + \sum_{i=1}^{N} \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2} \,, \\ &\frac{1}{\sqrt{\lambda}} \sum_{i=1}^{N} \sqrt{\frac{1}{4} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}} \\ &\quad \le P_J + \sum_{i=1}^{N} \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}.\end{aligned} \tag{15}$$

This results in a lower bound for λ.

$$\sqrt{\lambda} \ge \frac{\sum_{i=1}^{N} \sqrt{\frac{1}{4} \cdot \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}}}{P_J + \sum_{i=1}^{N} \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) \frac{S_i|H_{AE_i}|^2}{|H_{JE_i}|^2}} \tag{16}$$

Using this lower bound as a starting point for Newton’s method, one can obtain the exact value of λ that delivers the

N_{J_i} that minimize $I(A_i; E_i)$ given the power constraint. We iteratively use

$$\lambda_{n+1} = \lambda_n - \frac{f(\lambda_n)}{f'(\lambda_n)} \ , \tag{17}$$

where we use the expression for N_{J_i} from Eq. (10b) such that

$$f(\lambda_n) = \sum_{i=1}^{N} \frac{1}{2} \cdot \frac{S_i |H_{AE_i}|^2}{|H_{JE_i}|^2} \cdot \left[-1 + \sqrt{1 + \frac{2}{\lambda} \frac{|H_{JE_i}|^2}{S_i |H_{AE_i}|^2}} \right] - P_J \tag{18}$$

and

$$f'(\lambda_n) = \sum_{i=1}^{N} -\frac{1}{2\lambda^2} \left[1 + \frac{2}{\lambda} \frac{|H_{JE_i}|^2}{S_i |H_{AE_i}|^2} \right]^{-\frac{1}{2}} . \tag{19}$$

IV. USB on-shield jamming water-filling

We consider the spectral shape of USB 2.0, 12 and 480 Mb/s transmission with rectangular pulse shape as an example. The spectra with such a pulse shape are shown in figures 3 and 4 as "S". Practical measurements indeed sometimes show steep signal slopes. Such a signal does, of course, not provide the required independence of the different channels over frequency, but it provides some illustration with actually measured channel characteristics. H_{AB} is the legitimate differential D+/D− channel. H_{AE} is the transfer function from the D+/D− wire pair to the eavesdropping H-field probe. H_{JE} denotes the transfer function between the Ground-Shield loop and the probe. Finally, H_{JB} means the transfer function between the Ground-Shield loop into the Alice-Bob connection. The jamming power allocation N_{J_i} is shown as stars in both figures. Their spikes are nicely following H_{JE_i} notches. Note that we had to weaken the legitimate channel significantly to obtain illustrative results. One should note that the jamming transfer function from Ground-Shield to the legitimate one is very strong. Practically, one would have to do a proper design for the jamming elements on circuit boards, connectors, or cables. For this paper, USB was just chosen to obtain some illustrative results. The actual application of such jamming methods are thought to protect from on-chip or on-board eavesdropping. This will require corresponding RF designs. This dedicated jamming will then also not have a strong outside effect that could influence other services.

For the described simplification, when ignoring effects on the legitimate channel, corresponding results for the USB cases are also shown in figures 5 and 6.

V. Trade-off MSE for legitimate transmission and eavesdropping

Instead of, but in line with the secrecy capacity, one could also look into the mean-squared error for the legitimate receiver compared to the one for the eavesdropper. We are using some weighting factor μ for defining the trade-off between both.

From Fig. 2, we obtain the error for the legitimate channel using this weighting factor in determining a trade-off PSD S_Δ.

$$\begin{aligned} S_\Delta(j\omega) \quad &= \quad S_A(j\omega) \cdot |H_{AB}(j\omega) C_L(j\omega) - 1|^2 \\ &\quad\;\; + N_J(j\omega) \cdot |H_{JB}(j\omega) C_L(j\omega)|^2 \\ &- \quad \mu \cdot \left[S_A(j\omega) \cdot |H_{AE}(j\omega) C_E(j\omega) - 1|^2 \right. \\ &\quad\;\; \left. + \ N_J(j\omega) \cdot |H_{JE}(j\omega) C_E(j\omega)|^2 \right] \end{aligned} \tag{20}$$

The first part is the normal MMSE expression, where the jamming noise contribution is provided by the second summand, neglecting additional noise. The expression after μ is the what an eavesdropper would experience. C_L and C_E denote the equalizers used at the legitimate receiver (Bob) and the eavesdropper (Eve), respectively.

To optimize jamming, the S_A contributions are not relevant. We now rewrite the expression (20) using frequency samples labeled by i. We are hence maximizing

$$\sum_i N_{Ji} \cdot \left[\mu \cdot |H_{JEi} C_{Ei}|^2 - |H_{JBi} C_{Li}|^2 \right] \ . \tag{21}$$

We are abbreviating the bracketed term as F_i, simplifying the maximization as

$$\text{maximize} \ \sum_i N_{Ji} \cdot F_i \ \text{with} \ \sum_i N_{Ji} = P_J \ . \tag{22}$$

Rewriting this in vector format, summarizing the components N_{Ji} as a vector $\mathbf{n}_J$ and F_i as $\mathbf{f}$, yields

$$\mathbf{n}_J^T \mathbf{f} = k \cdot \hat{\mathbf{n}}_J^T \mathbf{f} \ , \tag{23}$$

where we chose $||\hat{\mathbf{n}}_J|| = ||\mathbf{f}||$ introducing some constant k. We then conclude

$$\mathbf{n}_J^T \mathbf{f} = k \cdot \hat{\mathbf{n}}_J^T \mathbf{f} \leq k \cdot \mathbf{f}^T \mathbf{f} \ , \tag{24}$$

leading to the maximum when $\hat{\mathbf{n}}_J = \mathbf{f}$.

With the side-condition in (4), (22) can be expressed in vectorial form as

$$\mathbf{1}^T \mathbf{n}_J = P_J \ = \ k \mathbf{1}^T \hat{\mathbf{n}}_J \Longrightarrow k = \frac{P_J}{\mathbf{1}^T \hat{\mathbf{n}}_J} \ , \tag{25}$$

where $\mathbf{1}$ is an all-ones column vector. We obtain the optimum jamming PSD as

$$\mathbf{n}_J = k \hat{\mathbf{n}}_J = \frac{P_J}{\mathbf{1}^T \hat{\mathbf{n}}_J} \hat{\mathbf{n}}_J = \frac{P_J}{\mathbf{1}^T \mathbf{f}} \mathbf{f} \ . \tag{26}$$

For illustration, we again take the example with a USB cable and H-field probe and plot a result for $\mu = 50$ in Fig. 7. The vertical transitions mark the areas of negative N_J components, which would, of course, then be zero.

VI. Conclusions

We investigated two approaches to determine the jamming power allocation over a frequency range, where, on the one hand, we started from the secrecy capacity expression. We do this under a total power constraint. One may see this as a jamming water-filling. Unlike the well-known water-filling solution for the transmit power, however, for jamming, the

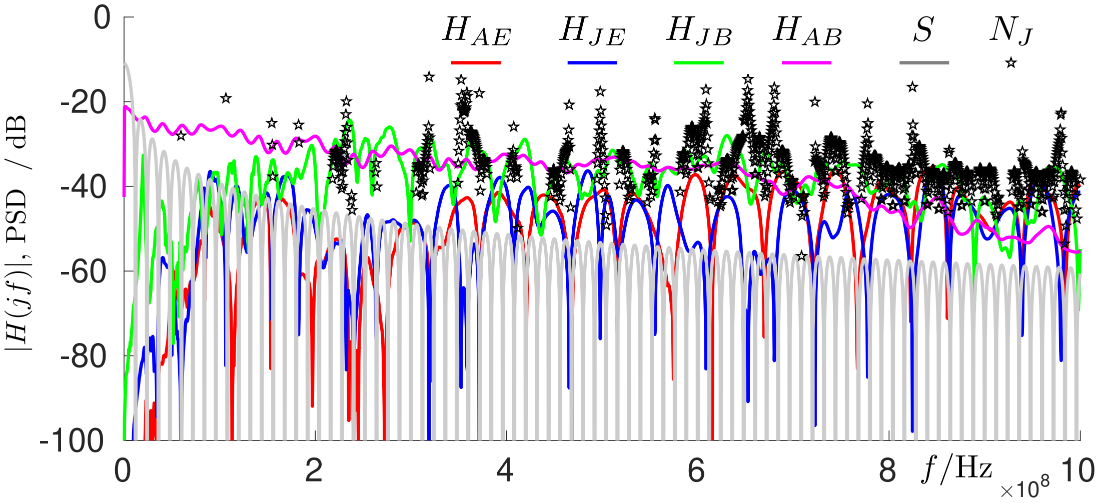

Fig. 3. Jamming power spectral distribution for 12 Mb/s USB spectrum shape

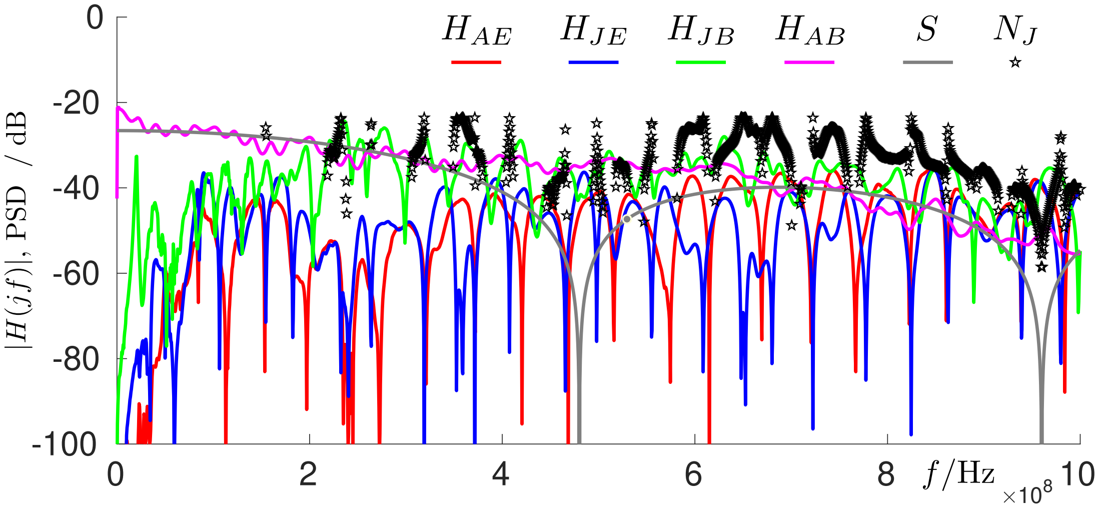

Fig. 4. Jamming power spectral distribution for 480 Mb/s USB spectrum shape

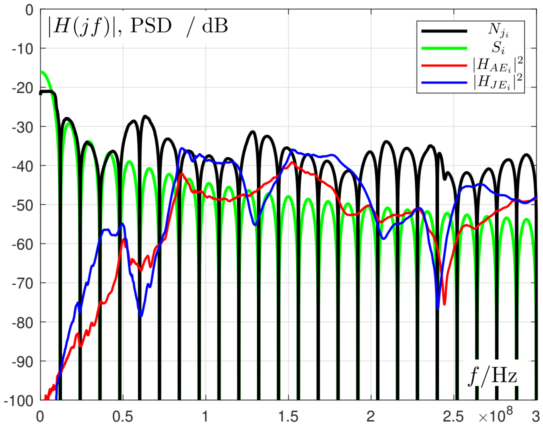

Fig. 5. Jamming power spectral distribution for 12 Mb/s USB spectrum shape disregarding effects on the legitimate channel

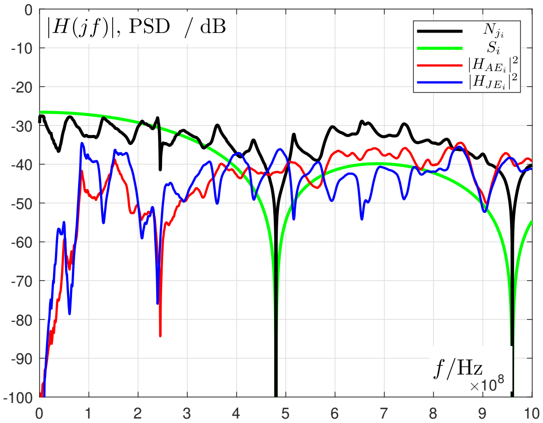

Fig. 6. Jamming power spectral distribution for 480 Mb/s USB spectrum shape disregarding effects on the legitimate channel

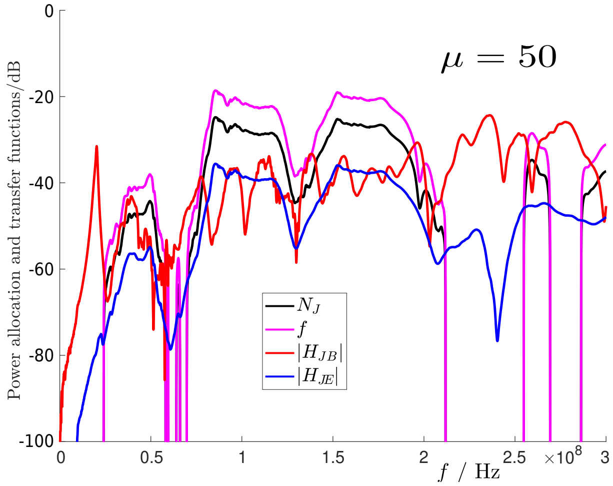

Fig. 7. Jamming power distribution without equalization dependent on the transfer functions between the Jammer towards Bob or Eve; weighting factor $\mu = 50$

Lagrange factor has to be determined by a search checking for valid solutions that lead to positive jamming power contributions.

On the other hand, we also used a corresponding Mean-Squared Error formulation, where one could weight the jamming effect onto the legitimate receiver and the eavesdropper. In a vectorial description, we find that the jamming power allocation is determined by the direction of those weighted terms.

The common problem of all such approaches is, of course, the assumption to know the channel to the eavesdropper, at least, to some extent. One may have to model this channel. Furthermore, for the MSE formulation, equalizer terms are included, also assuming some knowledge or guessing of the applied equalizer approaches.

Despite of the practical constraints, it is still interesting to determine water-filling for jamming to protect from eavesdropping and be aware, how a corresponding MMSE solution would look like.

For illustration, we used a somewhat modified transfer functions from a USB cable to an H-field probe, applying the jamming signal to the loop consisting of ground and shield. As expected, from our water-filling, at low frequencies, jamming is turned off, since the legitimate cable channel has a low-pass characteristic and the coupling function between the jamming channel and the legitimate one is stronger than towards the eavesdropper.

The MMSE approach allowed for a trade-off between disturbing the eavesdropper versus the legitimate receiver.

The illustration using measurements from a USB connection is, of course, not necessarily meant as an application domain. Especially, here, the legitimate user is disturbed significantly from a ground-shield loop, more than the eavesdropper. It should just serve as an example that such additional loops could be used for friendly jamming purposes.

So far, we have only studied the power distribution over frequency. However, to hinder synchronization, one would also consider hiding synchronization patterns and the clock itself by jamming with certain time patterns, dedicated sequences, and spectra, especially targeting the clock recovery at the eavesdropper side.

References

[1] “An introduction to TEMPEST.” https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981. Accessed: Oct. 13, 2017.

[2] M. A. Leghari, S. M. Pralle, S. F. Peik, S. Luetje, and W. Henkel, “Classification of PC baseband signals from wireless egress,” in *WSA & SCC 2023; 26th International ITG Workshop on Smart Antennas and 13th Conference on Systems, Communications, and Coding*, pp. 1–6, 2023.

[3] D. Baudry, C. Arcambal, A. Louis, B. Mazari, and P. Eudeline, “Applications of the near-field techniques in EMC investigations,” *IEEE Transactions on Electromagnetic Compatibility*, vol. 49, pp. 485–493, Aug 2007.

[4] Y. Liu and B. Ravelo, “Fully time-domain scanning of EM near-field radiated by RF circuits,” *Progress In Electromagnetics Research*, vol. B57, pp. 21–46, January 2014.

[5] M. Spang, M. Albach, and G. Schubert, “Calibration of probes for EMC near-field scanning,” in *CST User Group Meeting 2010*, 2010.

[6] Z. Li, Y. Zhu, and K. G. Shin, “iCoding: Countermeasure against interference and eavesdropping in wireless communications,” in *2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2021.

[7] R. Negi and S. Goel, “Secret communication using artificial noise,” in *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.*, vol. 3, pp. 1906–1910, 2005.

[8] Y. Wu and Y. Huo, “A survey of cooperative jamming-based secure transmission for energy-limited systems,” *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–11, 2021.

[9] L. Wang, L. Wang, Y. Zeng, and M. Wang, “Jamming power allocation strategy for MIMO radar based on MMSE and mutual information,” *IET Radar, Sonar & Navigation*, vol. 11, no. 7, pp. 1081–1089, 2017.

[10] S.-H. Tsai and H. V. Poor, “Power Allocation for Artificial-Noise Secure MIMO Precoding Systems,” *IEEE Transactions on Signal Processing*, vol. 62, no. 13, pp. 3479–3493, 2014.

[11] T. M. Cover and J. A. Thomas, *Elements of information theory (2nd ed.)*. Wiley, 2006.

[12] A. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[13] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[14] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[15] Compaq et al., “Universal serial bus specification, rev. 2.0,” 2000.