RC75 Jeffrey, I., LoVetri, J., Kordi, B. (2004) *Hardware Invariant Protocol Disruptive Interference*, Proceedings of 2004 IEEE International Symposium on Electromagnetic Compatibility, Vol. 2, pp. 703 - 707, Aug. 9-13.

Hardware Invariant Protocol Disruptive Interference

Ian Jeffrey Joe LoVetri Behzad Kordi
Department of Electrical and Computer Engineering
University of Manitoba
Winnipeg, Manitoba, Canada R3T 5V6
ijeffrey@ee.umanitoba.ca, lovetri@ee.umanitoba.ca

Abstract--**In this paper we consider that the target of intentional interference is a communication channel and we attempt to find interference capable of degrading communication throughput. The goal is to achieve disruption independent of hardware implementation while maintaining hardware functionality. We call such interference HIPDI and parameterize it using a concept called *hardware aperture*, as defined by the protocol of the channel. We show that simple CW and AM interference is capable of halting throughput for 100BaseTX Ethernet networks for all hardware configurations considered.**

I. Introduction

The problem of maximizing energy transfer to a hardware device caused by a remote disturbance is commonly addressed using a topological approach [1]. Typically, this approach uses time or frequency norms to maximize the energy coupling from one level of the topology to another. Surface and boundary interactions can be simply modeled in the frequency domain while the energy contained in resonant waveforms is easily quantified in either domain [1], [2].

A slight modification of the electromagnetic interaction problem unveils a novel and interesting new idea: consider that *instead of a hardware device, a communication channel is the* interference target. We ask, is it possible to produce energy in the channel that will disrupt (reduce or halt) communication throughput regardless of the hardware used to interpret the communication protocol, all the while maintaining hardware functionality? If such interference were to exist, it would pose a severe threat to the integrity of existing communication channels.

We use the name *Hardware Invariant Protocol Disruptive Interference* (HIPDI) to describe this theoretical interference. The purpose of this research is to parametrize HIPDI as a function of the protocol parameters. Herein, we do not consider the physics of the coupling problem. Obviously, for a wired channel, the spatial orientation of the cable may be such that limited coupling is possible at various frequencies. We assume that sufficient power is available to overcome this problem and consider only the effect of sufficiently-coupled energy.

It is useful to consider the theoretical existence of HIPDI for an arbitrary protocol and communication channel. If it were possible to produce energy in the channel indistinguishable from data, then the *hardware interpreters* (the hardware responsible for transmitting and receiving information) would be disturbed by the coupled energy. An important question is: How dissimilar from valid data can HIPDI be and what are the minimum sufficient parameters required of a HIPDI waveform? E.g, are simple CW and AM waveforms sufficient?

One theoretical approach leading to parameter extraction of the required interference is the concept we refer to as the *hardware aperture* of the protocol. It is clear that *any* hardware used to implement a communication protocol *must* be sensitive to valid signals of that protocol. The parameters of such valid signals are the hardware aperture of the protocol. Signals outside the hardware aperture can be protected against by physical means, such as the use of chokes on wired channels, without disrupting the normal operation of the link.

In order to apply the HIPDI concept, we must consider a specific protocol. In this paper we consider the 100BaseTX Ethernet protocol for which we parameterize possible HIPDI based on a theoretical analysis. We then perform experiments on a point-to-point communication link to validate our findings.

II. 100BaseTX Ethernet Protocol

The 100BaseTX Ethernet protocol is a wired communication standard typically applied over CAT-5 unshielded twisted pair (UTP). Such cables have an operating frequency up to 100 MHz. While there exist shielded twisted pair (STP) cables for this protocol, we have selected UTP based on its wide implementation in local-area networks (LANs) and residential broadband connections. In a 100BaseTX implementation, the hardware interpreters are commonly referred to as Network Interface Controllers (NICs). This physical channel allows us to conclude that for HIPDI to exist it must have frequency components less than 100 MHz because the upper frequency of the hardware aperture does not need to be more than 100 MHz.

Given a logical bitstream with desired transmission rate of 100 Mbps, the 100BaseTX Ethernet protocol uses differential baseband signalling with two encoding schemes: 4b/5b and MLT-3, to create a 125 Mbps bitstream with a maximum fundamental frequency component of only 32.5 MHz. (Details are available in [3], [4].) For any data transfer, the bit period is 8 ns and the bit amplitude takes discrete values at -1, 0 and 1V for the bit period.

0-7803-8443-1/04/$20.00 © IEEE.

The protocol is defined such that, in the absence of data transmission, an idle signal is transmitted between NICs to monitor link integrity. This idle signal operates at the maximum protocol frequency of 32.5 MHz. Any other data transmitted is guaranteed to have fundamental frequency lower than 32.5 MHz. In addition, the Ethernet protocol senses the activity on the cable, prior to transmission, to ensure that the channel is free. A final important feature of the protocol is that synchronization between NICs is extracted from the data stream itself. This could play a role in the development of HIPDI as sufficient jitter in the data could cause synchronization to fail.

Therefore, there are two predominant ways to disrupt communication: we can sufficiently corrupt valid data or we can make the channel inaccessible to the transmitting NIC because it falsely appears that the channel is occupied (i.e. an induced collision).

III. Time Domain and Frequency Domain Protocol Characteristics

Fig. 1 depicts a short segment of a simulated 100BaseTX Ethernet bitstream in the time domain, acquired by framing and encoding an arbitrary computer file (approximately 1 kB in size). The corresponding 4b/5b encoded bitstream is:

[1 0 1 1 1 1 0 1 1 0 1 0 0 1 1 1 0 0 1 0].

Fig. 2 shows the frequency information obtained from the bitstream by using the Fast Fourier Transform (FFT) to calculate the Fourier spectrum of the data with a sample period of 0.08 ns.

From the spectrum of the encoded data we see that for this particular bitstream, the largest frequency component is at approximately 16 MHz. This suggests that perhaps this is a good candidate for the frequency of interference. Unfortunately, the relative magnitude of this component is not large enough to suggest that interference at this frequency will be capable of reducing or halting data throughput. Moreover, the time domain waveform itself is insufficient to indicate the required interference parameters with the exception of the signal amplitude. It is clear that any hardware implementation will not be damaged by differential energy having a magnitude of ±1 V. The time- and frequency-domain information of the protocol gives us limited parameters on which to construct a HIPDI. We can gain more information by using a mixed time-frequency domain transform: the Continuous Wavelet Transform (CWT).

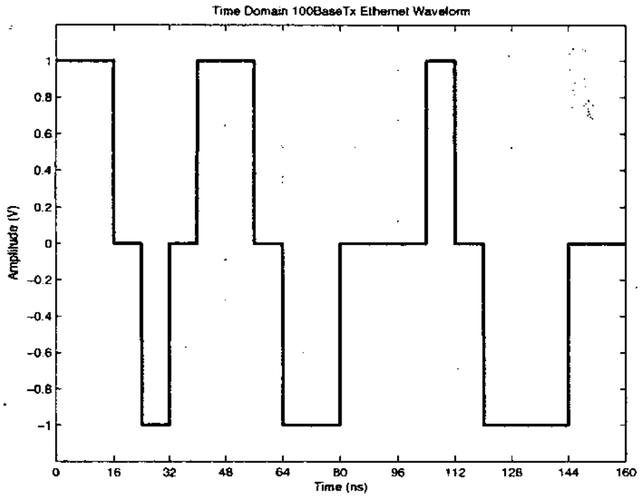

Figure 1. Simulated 100BaseTX bitstream

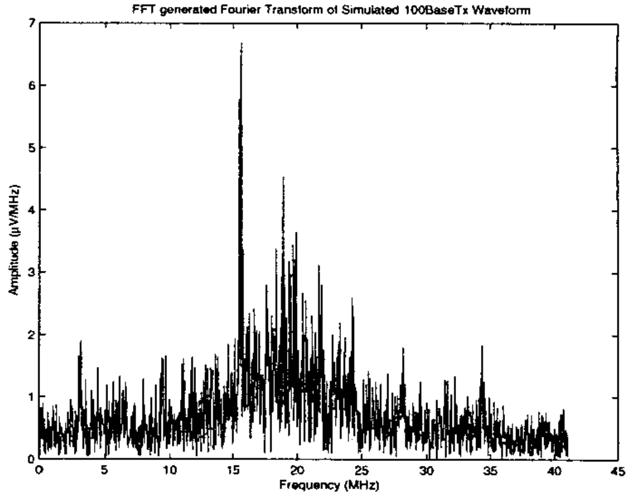

Figure 2. FFT of simulated 100BaseTX bitstream scaled to (µV/MHz)

IV. Protocol Characteristics from the Continuous Wavelet Transform

Some relevant theory regarding the CWT can be found in [5], and a recent application to EMC in [6]. In general the CWT sacrifices some of the frequency information obtained from the FFT in order to preserve time domain information. We have numerically applied various wavelet transforms to both a 100BaseTX idle signal (10 kB) as well as the encoded bitstream corresponding to a 1 kB data file. It was found that a 10th order Complex Gaussian Wavelet utilizing 60 frequency points from 1 MHz to 150 MHz provides an acceptable time and frequency resolution within a reasonable computation time.

In Fig. 3 we depict the CWT of the idle signal, while in Fig. 4 we show the CWT of the bitstream simulated data. We see clearly from Fig. 3 that the MLT-3 encoded idle signal has a fundamental frequency of 32.5 MHz as expected. The CWT shown in Fig. 4 demonstrates that the range of frequencies of any simulated bitstream shifts down to approximately 15 MHz with the majority of components existing below 30 MHz. Taking the sum of the absolute value of the complex CWT coefficients through time for a given frequency value, as shown in Fig. 5, confirms that the majority of the signal energy is between 15 and 30 MHz.

What can we extract from Figs. 3-5? If the hardware aperture of the protocol is truly sensitive up to 100 MHz then Fig. 5 suggests one of two possibilities for HIPDI: Interfere with the protocol where the energy is lowest thereby reducing the signal to noise ratio or interfere with the protocol where the energy is highest in order to confuse the hardware interpreter with interference highly correlated to data.

In summary, because of the specification of the CAT-5 cable, the hardware aperture of the protocol is no greater than 100 MHz. It may well be substantially lower than 100 MHz, given that the majority of the frequency content is between 10 and 30 MHz. This depends on how sensitive the hardware aperture is with respect to signal risetime. It is unclear how to ascertain this dependency from the protocol itself. In the remainder of this paper it will be assumed that the hardware aperture of the protocol includes all frequencies up to 100 MHz. Actual tests performed on particular hardware implementations to be presented in the next two sections show that disruptive interference exists at various frequencies throughout this bandwidth.

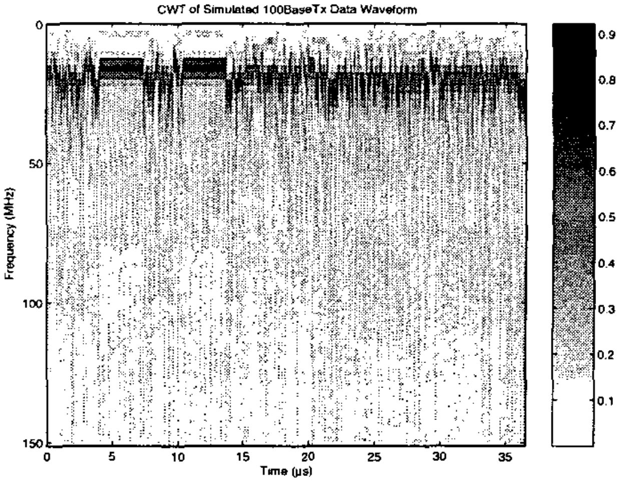

Figure 4. CWT of simulated 100BaseTX waveform.

V. Experimental Setup

Experiments were performed by radiating Ethernet cables via a GTEM cell [3]. Because we are not concerned with the cable coupling problem, direct injection of differential interference onto the cable is all that is required. On the other hand, field coupling experiments via GTEM radiation give us some indication of the field levels required to disrupt communication.

A point-to-point 100BaseTX communication link between two computers was established such that one computer was continuously transmitting data to the other. The throughput (data packets received per second) was measured in the absence of interfering radiation as a benchmark. Experiments were performed by subjecting three pairs of NICs (one NIC of each pair in each computer), to continuous wave (CW) and amplitude modulated (AM) radiation. These radiation types were selected due to their availability. We will refer to the results of the experiments in accordance to the NIC pair used (i.e. A, B, C). The throughput was monitored remotely via a third computer, but lost packets were not.

The cable inside the GTEM cell was oriented so as to maximize the differential-mode pick-up while minimizing the common-mode: the cable was oriented parallel to the septum in the cross-sectional plane of the GTEM. In addition, to increase differential-mode coupling, a 1 m length of cable was untwisted. With this setup, data transfer occurred normally in the absence of interference and we therefore concluded that the effects of untwisting were negligible. Finally, common-mode chokes were used to minimize the amount of common-mode energy reaching the NICs and the portion of cable outside of

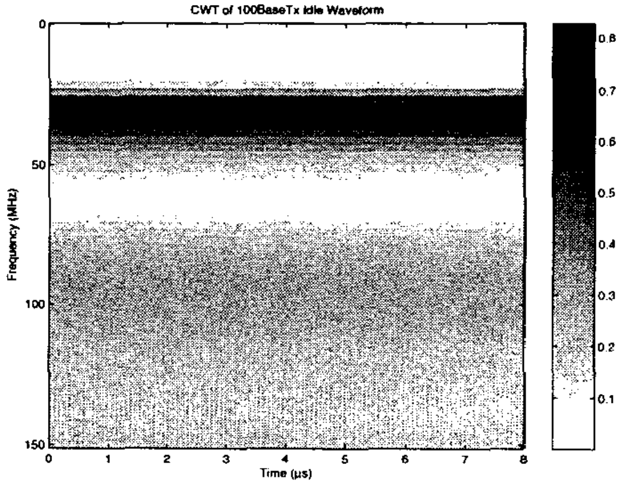

Figure 3. CWT of 100BaseTX idle signal.

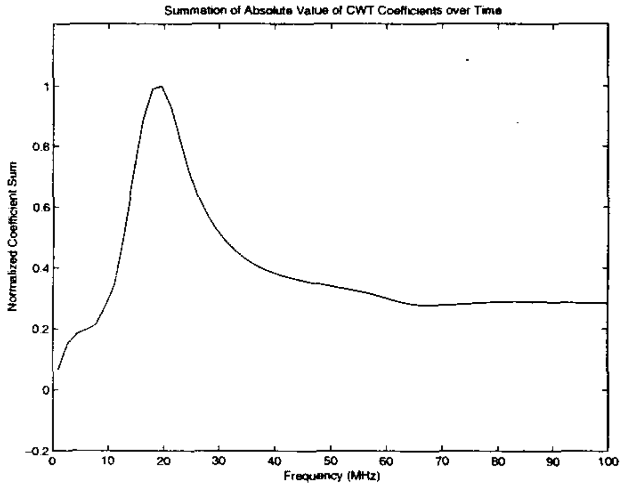

Figure 5. Normalized sum of CWT coefficients.

the cell was shielded to minimize the re-radiation of coupled energy.

After measuring throughput in the absence of radiation, the network cable was subjected to varying levels of radiation at discrete frequencies from 1 to 100 MHz in 1 MHz steps. This choice of frequencies was made based on the frequency response of the CAT-5 cables as well as preliminary tests which involved frequencies up to 1 GHz for which little, if any, throughput reduction was achieved above 100 MHz. Both CW and AM radiation were used for the various NIC pairs. In the case of AM radiation, a 15 kHz modulation frequency with 100% modulation was used. The modulation frequency was quite arbitrary, as preliminary test results showed little variation due to a modulation frequency from 1 to 20 kHz.

A signal generator was used to produce the CW and AM interference and this signal was amplified using a wideband RF amplifier. The maximum output power of the amplifier was approximately 120 W (a maximum field level of 78 V/m at the cable). Measurements of the radiated power were taken as a percentage of the forward power of the amplifier.

VI. Experimental Results

Figs. 6 and 7 show the results for NIC pair A under both CW and AM interference. The results show percent network throughput as a function of frequency (horizontal axis) and as a function of the forward radiated power (vertical axis). The dark regions of Figs. 6 and 7 correspond to reduced or zero throughput while lighter regions correspond to full or 100% throughput. A comparison of the two figures shows that throughput reduction occurs more readily for AM interference than for CW. One possible explanation for this is that the wider spectrum of the AM interference more closely resembles the spectrum of the data than CW interference.

Without further investigation of the mode of the coupled energy, we can draw little conclusions directly from the plots as they do not show the actual differential-mode coupled to the cables. Therefore, measurements were taken in the absence of data transfer of the differential- and common-mode interference at some frequencies of interest.

Table 1: Differential- and Common-Mode Interference Levels for Immediate Throughput Reduction

Frequency	Differential-Mode (mV pk-pk)	Common-Mode (V pk-pk)
18	300	3
33	330	2.6
65	140	0.5
86	180	0.5

From the plot for CW radiation we see that for various frequencies there exist three kinds of responses to interference. First there are frequencies at which total throughput reduction is achieved immediately for 10% forward power (22 V/m). These are in the vicinity of 18, 33, 65 and 86 MHz. Second, there are frequencies in which the onset of throughput reduction does not occur until the power has been increased substantially. These are 55, 67 and 81 MHz. Finally, there are regions in which no throughput reduction occurs at all. These are 38, 58 and 92 MHz. The measured differential- and common-mode energy present on the cables at these frequencies for each of the throughput reduction trends is summarized in Tables 1 through 3 respectively. It is also important to note that in all of the experiments, the computers functioned normally for all levels of interference.

Of primary interest of the results presented in the above tables is that at 65 MHz, 140 mV pk-pk of differential-mode interference is capable of completely halting network throughput. (All voltage measurements are reported as pk-pk.) Present on the line is a mere 0.5 V of common-mode

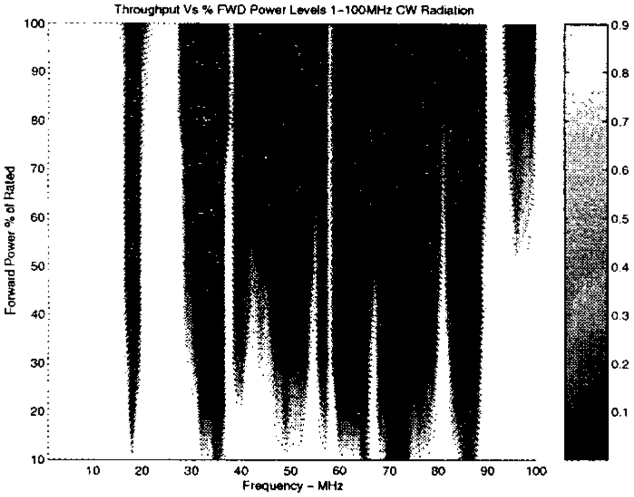

Figure 6. Percent throughput vs. NIC pair A under CW radiation.

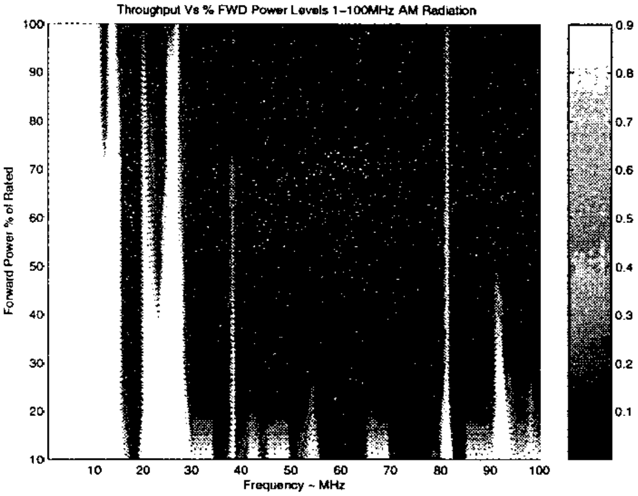

Figure 7. Percent throughput vs. NIC pair B under AM radiation.

TABLE 2: DIFFERENTIAL- AND COMMON-MODE INTERFERENCE LEVELS FOR THROUGHPUT REDUCTION REQUIRING MORE THAN 10% FORWARD POWERS

Frequency	Differential Mode (mV pk-pk)	Common-Mode (V pk-pk)
55	330	0.7
67	330	1.72
81	340	0.7

TABLE 3: DIFFERENTIAL- AND COMMON-MODE INTERFERENCE LEVELS FOR NO THROUGHPUT REDUCTION AT 100% FORWARD POWERS

Frequency	Differential Mode (mV pk-pk)	Common-Mode (V pk-pk)
38	930	9.3
58	260	4.5
92	800	0.9

interference. Note that this frequency corresponds to the second harmonic of the fundamental of the idle signal (32.5 MHz). From Fig. 3 we see that, due to the nature of the idle waveform, there is a null at this frequency. This leads us to believe that frequencies near this value result in good interference as they represent harmonics of the fundamental signal in a situation where no harmonics are expected to exist.

At 18 and 33 MHz it seems that approximately 300 mV of differential interference is required to halt transmission but in this case the common-mode is quite high, around 3 V.

When we consider the results of Table 2 we see that throughput reduction once again occurs at around 300 mV of differential-mode as in Table 1. Note that in these cases, the common-mode interference is reduced to around 1V pk-pk.

The results of Table 3 show the anomaly that at 38 MHz, even with 930 mV pk-pk of differential mode, no throughput reduction was achieved. On the other hand this result shows that even though a very large common-mode signal of 9.3 V pk-pk is present, no throughput reduction occurred. This reinforces our belief that in the cases of throughput reduction, the common-mode itself is not responsible for hardware failure and that it is indeed differential mode, protocol interference that is occurring. One reason why 930 mV of differential-mode at 38 MHz does not affect data transmission may be that it simply does not posses sufficient *data-like* features to confuse the hardware interpreters.

Various other tests were performed using NIC pairs B and C and it was found that throughput reduction occurred at similar frequencies. Differences were apparent, but this is expected because different manufacturers use different hardware technologies. The interesting thing from the point of view of HIPDI is the commonalities between the different NIC responses. Specifically, throughput reduction occurred in all cases tested for frequencies from 28-35 MHz under simple CW radiation. In general, AM modulation consistently increased the amount of disturbance.

VII. CONCLUSIONS AND FUTURE WORK

The purpose of this research has been to introduce the novel and interesting problem of Hardware Invariant Protocol Disruptive Interference--HIPDI. Moreover it has been an attempt to theoretically parameterize such interference based on the 100BaseTX Ethernet protocol. Based on the theoretical analysis of this protocol, we have shown that possible HIPDI parameters are: low-power, differential-mode interference operating in the frequency band up to 100 MHz. In addition, based on the Continuous Wavelet Transform of the 100BaseTX idle signal we suggest that 32.5 and 65 MHz are good HIPDI candidates.

Via experimentation we have demonstrated that simple CW and AM interference in this bandwidth is capable of terminating communication while maintaining computer functionality. It was found that 33 MHz, CW or AM, caused failure in all cases investigated while 65 MHz shows promise in requiring the least amount of differential-mode power. We have also shown that AM modulation simply increases the effectiveness of the interference and we conclude that this fact is due to the broader spectrum of AM interference as it more closely resembles data. Finally, it is very encouraging to note that for all network configurations considered, total throughput reduction was possible at frequencies predicted by our approach.

The research conducted so far has focused on CW and AM interference because of its simplicity. It is highly likely that more complicated data-like modulation schemes will be more effective as HIPDI (i.e. require less power). We are currently investigating such modulation schemes.

ACKNOWLEDGMENT

The authors wish to thank Mr. Colin Gilmore and Mr. Greg Siemens for their contributions to this work.

REFERENCES

[1] C. E. Baum, "Maximization of Electromagnetic Response at a Distance," *IEEE Trans. on EMC*, Vol. 34, No. 3, August 1992, pp 148-153.

[2] C. E. Baum, "A Time-Domain View of Choice of Transient Excitation Waveforms for Enhanced Response of Electronic Systems," *Interaction Notes*, Note 560, September 2000.

[3] I. Jeffrey, C. Gilmore, G. Siemens and J. LoVetri, "Hardware Invariant Protocol Disruptive Interference for 100BaseTX Ethernet Communications", To appear in *IEEE Trans. on EMC*, Special Issue on High Power Electromagnetic (HPEM) Disturbances and Intentional EMI, 2004.

[4] IEEE std 802.3-2002, "IEEE Standard for Information Technology--Telecommunications and Information Exchange Between Systems--Local and Metropolitan Area Networks--Specific Requirements--Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications."

[5] T.K. Sarkar and C. Su, "A tutorial on wavelets from an electrical engineering perspective, part 2: the continuous case," *IEEE AP Mag.*, 40, 6, pp. 36-49, Dec. 1998.

[6] B. Kordi, J. LoVetri, and G. Bridges, "Using Wavelets to Characterize Time-Frequency Features of Electromagnetic Coupling Problems," *Proceedings of ANTEM'2002*, pp. 115-120, St.-Hubert, Québec, Canada, July 31 - August 2, 2002