Energy Leakage from LANs

CHESTER L. SMITH
Harvey Consultants, Inc, Concord, MA

Concerns about energy leakage and information espionage can be eliminated with the proper installation of good-quality cable.

INTRODUCTION

Many Local Area Networks (LANs) used to interconnect work station computers to one another and frequently to a remote mainframe employ some kind of inexpensive coaxial cable. A favorite is RG-59, a quarter-inch, 75-ohm product that is flexible and easy to install. It pulls readily in restricted spaces and above all, it is inexpensive, sometimes costing as little as 10 to 15 cents per foot in upwards of a kilometer length. As an interconnection medium, RG-59 or its close cousin, RG-58 (50 ohms), works very well, indeed. So what is the problem?

The problem is that the outer conductor of these common cables is braided and this causes them to leak energy. Some have raised the question of possible personnel hazards and, indeed, some states have regulations on the subject. For the most part, these rules are based on ANSI C95.1 1982. The levels of leakage are very low, even in a poorly designed installation, so this is not a source of concern.

Information leakage is another matter. Industrial espionage is serious business that tends to remain "under the rug" with most organizations. No one wants to admit having been victimized or having perpetrated the espionage. Pirating information from a leaking LAN is not at all difficult and not particularly hazardous. It is not necessary to physically enter the premises or to "hack" the computer systems of the victim organization. It can be done from a remote location, sometimes as far as a kilometer or more away. A nearby hotel or motel is ideal for such an information pirating base.

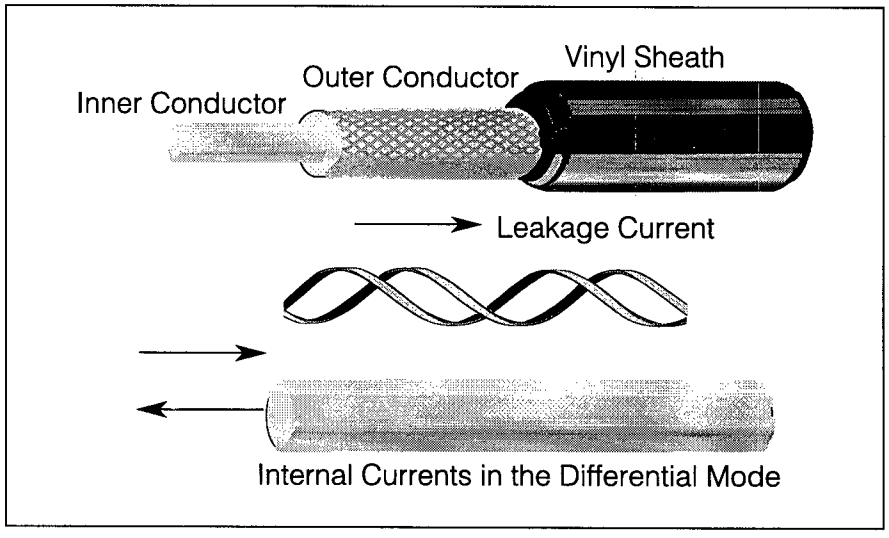

Figure 1. *Leakage Mechanism of Braided Coaxial Cables.*

BRAIDED CABLE

The mechanism responsible for the leakage of braided cable is in the braid itself. The outer conductor is not solid, but somewhat braided (Figure 1). The signal on the cable is in differential mode. Two conductors in close proximity carry the counter currents of a circuit. In the case of an open line, there are local fields, but radiation is nearly completely canceled. In a coaxial cable, one conductor is inside the other and, ideally (e.g., perfect conductors), there is no countering external field, not even the quasi-stationary fields of a typical TV twin-lead. However, in this portion of the universe, there is no such thing as a "perfect" coaxial line. Some so-called "hard lines" come close, but low-cost RG-59 is not one of them.

The braid plays an electronic version of an old children's game called "In and Out the Window." The braid conductors pick up the current and transport it to the outside. Over any given short length, the actual levels on the outside are low. There is a shorting action at every crossover. Furthermore, there is some attenuation from the black vinyl jacketing. The vinyl jacket is deliberately made slightly conductive to prevent static build-up during handling. The jacket has a resistance of about 5 to 10 Mohms per square. If the jacket were not slightly conductive, static electricity generated during installation could arc through the polyvinyl chloride dielectric to the inner conductor and, eventually, breakdown would occur.

In spite of all of these factors, enough energy does reach the outside world to form current loops or "standing waves" along an extended run of cable. These are the "hot spots" where radiation takes place. Whatever information is being passed is also radiated and may

be intercepted. The strongest radiation is at the clock frequencies of the computers, but there can be harmonics as high as tenth or fifteenth order. The radiation pattern is not readily predictable nor is it simple.

A PIRATE SYSTEM

Even though the radiation is low level, it is in the portion of the high frequency (HF) spectrum where even very low level signals have astonishing carrying capability. These computer signals, if not suppressed, can be detected kilometers away. A block diagram of a simple system is shown (Figure 2). The basic system consists of a converter to map the LAN leakage onto a blank TV channel, which is available in every major television market. The TV set only needs to be modified by replacing the raster oscillator with a tuneable one that can be used to lock onto the screen display being transmitted. A phase lock loop will keep it on track once the signal is acquired. A more sophisticated system is possible involving a computer.

The directional antenna is not absolutely necessary — a simple whip will do — but the directional properties will help pick out particular signals and discriminate against others. A well-designed loop antenna has a steerable null that can be useful in controlling undesired signals. The video recorder is another accessory useful for recording material for future study.

CAUSES

One question that niggles at the edge of this issue is why anyone would go to so much trouble. No doubt there are some who will do it just for kicks. The most probable motive would seem to be to obtain intelligence about competitors' plans in areas of conflict or overlap. Quite often, given the convenience of computer technology, proposal data is prepared on or exchanged over the LAN. While the unethical competitor would never admit to it, a knowledge of what some rival(s) might be considering would be a major advantage in a close competition. As the economy tightens, more of these desperate measures may be seen.

CURES FOR THE LANS

It may seem like a platitude, but the best cure is a proper installation in the first place. The "hard lines" have attenuation levels approaching the dB loss to the nearest stars when properly installed and terminated. They also cost ten to fifteen times as much as RG-58 or -59. If the information to be handled is sufficiently critical, the cost can be justified.

Fiber optical lines are also a good choice for the initial installation, but this type of interconnection requires special converters at each end. Converters have their own problems.

Several manufacturers make a line of double-braided cables that are much better than the low-cost types. One manufacturer claims leakage attenuation levels of 90 dB/m. However, they are being modest. The author has measured some of their products at over 110 dB/m. This compares favorably with the 60 to 70 dB for single braid cables. The shielding effectiveness of braided cable is a function of how tight the braiding is. In some inexpensive varieties of cable the coverage is only 70%. As is often the case, buying for price alone is poor economy.

When a cable is extended, the net attenuation drops quite rapidly. For example, if the attenuation is 70 dB/m, a two meter-long piece loses 3 dB and is only 67 dB. Every time the run is doubled, another 3 dB is lost. To be sure, it never goes to zero. An asymptotic limit, typically around 11 to 14 dB, is reached based upon the ratio of the cable ground impedance and any lossy material within the cable sheath.

CAN IT BE FIXED?

Once the installation is in, it is generally an expensive proposition to replace. All is not lost, however, as it is possible to suppress most of the radiation. The pattern of current loops on the outside of the LAN lines is illustrated (Figure 3). Wherever the current is relatively high, the radiation takes place. These points of high leakage current are not hard to find. They tend to appear at zones delimited by points of discontinuity. A "point of discontinuity" can be any of a number of things. A sharp change of direction is a common one, as is a Tee.

While these fields are not sufficient to be a personnel hazard, they are radiators. It is necessary to attenuate the external current. By placing a lossy ferrite clamp at the center of the current loop, the radiation will be attenuated. The ferrite material must have a high value of μ and a large magnetic loss tangent. A device of this sort is modeled as an inductance shunted with a resistance placed at the point where the current is at its peak (Figure 4).

If the suppressors are added at each principal frequency node, lower level but significant radiative loops may appear generated by some of the harmonic content. Digital data strings are rich in harmonics due to the square-

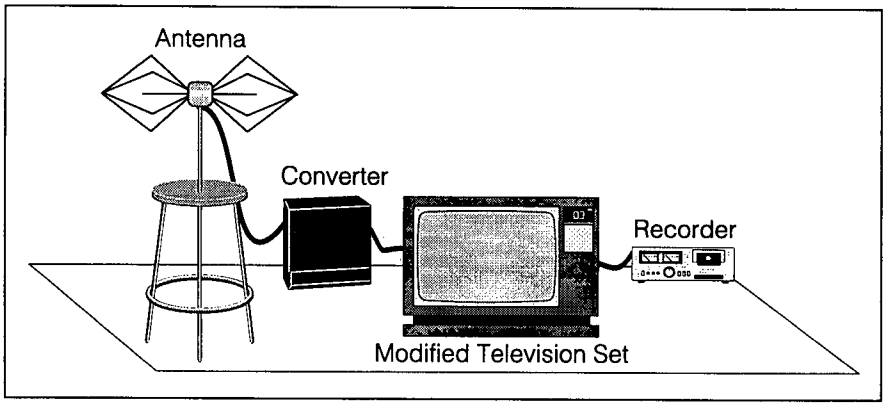

Figure 2. *A Pirate System for the Detection of LAN Leakage.*

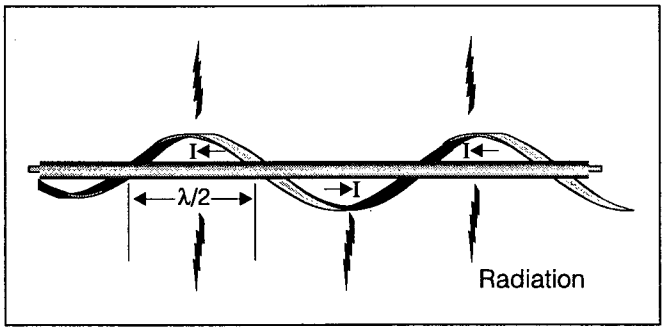

Figure 3. *Radiative Current Loops on the Outside of a Coaxial Cable.*

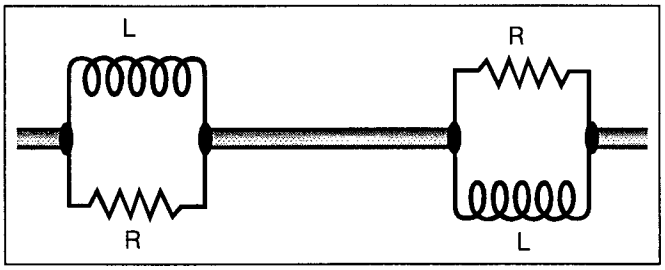

Figure 4. *The Equivalent Circuit for a Line Loaded with Lossy Ferrite.*

wave nature of the pulses. If these higher frequency loops are still serious, they too will require suppression. These harmonics can be manipulated to recover the primary data just as in the case of the fundamental. They are more trouble to intercept and analyze. Better or more sophisticated equipment than that indicated in Figure 2 would be necessary.

ELECTROMAGNETIC INTERFERENCE

Unintentional leakage, however, may pose a potential for interference to licensed users of the spectrum and will have to be suppressed for that reason. One investigation revealed a computer that was putting out a strong fifteenth harmonic on the two-meter amateur bands (144-148 MHz). It was energetic enough that a mobile operator could not access a repeater fifteen miles away. Rearranging cables and some shielding solved the problem.

EMISSIONS AND IMMUNITY

PC-type computers do not emit strongly by themselves. They must conform to FCC Rules, Part 15, Subpart J, Type B. The Communications Act of 1934 was modified in 1982 to authorize the Federal Communications Commission to stipulate immunity standards, but it did not mandate that it do so. Due to pressure from international markets and foreign governments this issue is finally being addressed by the ANSI C63 Committee 5. It will be some time before their work is finished and adopted by the FCC. The new standard is expected to call for immunity against noise fields on the order of 1 V/m.

What is not being addressed is impulsive noise being conducted into the local computer via the power cords and the LANs. Power cords can be filtered both for common mode and differential mode noise. The latter can be taken out by a lowpass filter. Differential mode filtering on the data line is more difficult as there is the possibility of destroying the desired signal, or at least attenuating it significantly. Computers like nice square waves with fast rise and fall times, but these are incompatible with filters as the ideal square wave has frequency components from the fundamental to nearly "daylight." Filters tend to erase the higher frequency components and serve up a round-shouldered pulse that may have to be differentiated and regenerated before the computer can handle it. Systems of this sort are available, but they add cost to the network.

COMPOUNDING FACTORS

There are two trends in computer design that exacerbate the local area network problem. First, higher and higher clocking frequencies are touted as the key features of future computers. The shielding effectiveness of braided cable drops off as frequency is increased. This implies that there will be more "hot" zones along a cable run. The second design trend, related to higher speeds, is lower thresholds between the switched states. This makes the local area network more susceptible to disturbances. The latter issue is not a problem for piracy, but it is for network stability.

SUMMARY

Local area networks leak unless the interconnecting cables are either hard line or double-braided with metallized Mylar film. The leaked energy is radiated away and may be intercepted. Any information contained can be captured. Personnel hazards from LAN leakage is minimal, but may need to be "proved" if challenged.

Leakage from LANs can be suppressed sufficiently to provide adequate security against unsophisticated apparatus. If leakage is a problem or is suspected, tracking down and suppressing the radiation will, in general, be more costly than using good quality cable or fiber optical lines in the installation phase.

After service during WWII in the Army Signal Corps, ***CHESTER L. SMITH*** *returned to the University of Utah to complete his BSEE. His career included work at the Douglas Company, Raytheon, GTE Sylvania, and the MITRE Corporation. The work at MITRE involved evaluation of shielding and the application of MIL-STD-461 to various projects. He has published a number of papers. Chester is a registered engineer and certified by NARTE. He has a M.S. degree in mathematics and physics from Northeastern University and a Ph.D. from Clayton. He is an ordained American Baptist minister and until recently served the North Billerica Baptist Church as Associate Pastor. He serves a number of denominational committees, including the Committee on BiVocational Ministries. This committee is concerned with ministers who divide their time between denominational/church and secular jobs such as engineering, medicine, etc. (617) 275-0598.*