COAXIAL CABLE - THE HOSTILE MEDIUM

Archer S. Taylor
Senior Vice President, Engineering

Malarkey-Taylor Associates, Incorporated
Washington, D.C.

ABSTRACT

The cable television industry has not yet acknowledged the practical impossibility of maintaining the 5 - 30 MHz cable spectrum free of non-Gaussian noise. Modem manufacturers and data network architects either are unaware of the ingressive beasts waiting to ambush innocent upstream data, or naively view them as curable afflictions caused by sloppy design, careless construction, and slothful maintenance. The cost of clean-up can be enormous and never-ending. The time required to locate and repair causes of ingress is likely to be intolerable for services like traffic signal control that demand high reliability. Frequency agile modems, exotic modulation schemes, and sophisticated error detection and correction firmware are expensive, and inefficient. Perhaps the time is ripe for the fully switched, star network topology. Whatever the solution, some means must be devised for upstream transmission that is not so vulnerable to ingress interference.

INTRODUCTION

The cable television industry appears to be on the verge of plunging into the highly competitive interactive telecommunications business. The profit potential seems enormously attractive. We already have communications facilities in place, thanks to the FCC back in 1972 for requiring "two-way capability". All we need, we think, is a few modems, a computer of some sort, and a bit of software, and we are in business.

Not so. I leave it to others to talk about the profit and loss issues, and marketing research, and information banks and software, and storage capacity. I want to talk about the second part of the two-way capability, the part that carries messages upstream. I want to alarm you enough to go out and challenge the system designers and the modem suppliers; but, not enough to scare you away from this exciting new frontier of telecommunications.

THE INGRESS PROBLEM

Do you have, or know anyone who does have, a working upstream network actually providing enhanced services, in addition to home security, producing better than 10^{-8} bit error rate 99.95% (or more) of the time? If you say "yes", then I will ask you to prove it, because I am skeptical. Suppose you use the upstream system for home security alarm responses. Of course, you may incur some legal liability if a house burns or is burglarized, or a panic button fails to bring help. But, really, you may ask, how great is the risk, and who will know, if part of your system is down for the few hours or days required to track down the source of ingress that destroyed the return response? After all, you do have telephone dialers for backup.

On the other hand, suppose you are providing the linkage for a computer controlled traffic system. At 5 o'clock one afternoon, the return signals become unreadable because of severe power line noise interference. After several hours of searching, the trouble is identified, using bridger switches, as caused by a corona discharge in a power substation near the trunk cable. Unfortunately, there was a corroded service drop connector on one feeder near the power substation, and a loose cover plate on a tap on another feeder. While hunting for the problem, traffic became totally snarled at three major rush hour intersections, because of the incorrect signals received by the computer. That would not be so easy to indulge.

Or, suppose you were providing a high-speed, high-density data link service, with packet switching. Down time for maintenance or fault location could mean a disastrous back-up in transmissions causing customers to look for a more reliable communication service.

Why, you may ask, is the upstream transmission band considered so hostile?

First, look at the electromagnetic spectrum in the 5 - 30 MHz band. Seven international broadcasting bands are occupied by high powered transmitters, many of which shift from one band to another as the sky-wave "skip" moves up and down through the band. When conditions are right, signals broadcast from thousands of miles away come in loud and clear on the upstream network. Citizen's Band and amateur Radio transmissions are almost certain to be keyed "on" and "off" within a few yards of the cable somewhere, some with considerable power.

These services occupy about 5.4 MHz, or about 22% of the band. The rest of the spectrum, with a very few exceptions, is allocated to Marine and aeronautical, fixed and mobile services, some of which are also high powered.

You may have a "closed system" that generates less than 20 uv/m at 10 feet at any location; but I assure you that is not tight enough to prevent ingress. It does not help much to claim that the distribution plant has been well and carefully constructed, using RFI connectors and metal gasketed housing covers, all properly torqued down, with shrink tubes covering all splices and connectors, and no kinks or cracks or "ripples" in the cable. The problem is in the service drops, thousands of them, all over the system. As fast as you find one corroded, or broken, or improperly installed F-connector, two more bad ones show up.

The worst of it is that ingress interference may be caused by leakage transfer impedance well below the levels that would show up on the "cuckoo" or even the "Sniffer" monopole.

Even if you spend the time and dedicate considerable manpower to the job, constant vigilance is required to detect and correct the ingress that never stops happening. I am convinced that there is just no practical way to be reasonably confident that the ingress monster will not pop up at any minute and devour unprotected messages.

SOLUTIONS

What to do about it? If you only use the upstream network for status monitoring, ingress is merely an inconvenience. If you use it for home security, you can always back it up with digital dialers, as many operators are now doing. (Parenthetically, one might ask what good is the cable network if half the security subscribers are connected to our friendly telephone competitor's network). If you use it for two-way addressability and pay-per-view, the ingress monster may take a nip at your own bottom line. That could be a problem. But unless you are serious about competing for the interactive telecommunications business, you probably need do little or nothing about ingress, except learn to live with it.

However, if you really want to go after the new revenue potential for transmitting data, the first thing to do is talk to your modem and software suppliers. Don't let them snow you with talk about how well their equipment works at 20 dB carrier-to-noise ratio; they are talking about <u>thermal</u> noise, and that is the least of your problems. Don't worry about bit error rates, either. Practically any equipment will beat 10^{-8} ber under ideal conditions.

You need to find out what kind of error detection and correction protocols are provided in the software. Is either affirmative or negative acknowledgement required before any message can be accepted? Can the modem frequency be shifted to avoid an interfering carrier? If so, is the frequency shift automatically provided in the software? What is the tolerable ratio between the desired carrier level and that of an undesired, interfering discrete carrier? How much impulsive noise (from auto ignition or electrical machinery) can be tolerated before the information is lost?

I hope I am wrong, but I suspect you will get distressing answers. They will tell you that such sophisticated protocols are too expensive and unnecessary; they occupy too much bandwidth, or waste too much time. They will tell you how successfully their simple parity check polling system works, here, there, and the other place. They may even try to tell you that if you build your system "right", and maintain it "properly", you can eliminate ingress interference.

Actually, sophisticated protocols are expensive; they are less efficient because they occupy more bandwidth; and it does take time to acknowledge message receipt and correct errors. One way out might be to transmit the data at slow speed and narrow bandwidth; but what advantage would narrow band transmissions on cable have over ordinary telephone lines, except for security alarms, pay per view, status monitoring, and other internal uses? New revenues are most likely to be realized by offering medium-and high-speed data transmission services, not narrow band.

The most successful commercial data transmission services on cable TV today are provided on special cable networks mostly separate from the subscriber network. The institutional network (I-Net), if properly used, could be a good solution to the problem in some cases. However, users should not be connected with braided cable and F-connectors, and user terminals should be well-shielded and free of direct pickup ingress. Data channels should be allocated to portions of the spectrum with a limited number of identifiable interfering carriers; the TV channels, for example, with one main carrier and two attenuated subcarriers are far more suitable than the 5-30 MHz band.

The I-Net does not, however, solve the problem of providing enhanced services to cable TV subscribers. Several years ago, Jerrold put forth a system to convert the 5-30 MHz carriers at the bridger to higher frequencies for transmission to the headend on a second cable, independent of the subscriber trunk. Perhaps this idea should be resurrected, though I believe it should be modified so that each bridger, or perhaps pair of bridgers, would convert to a different channel. I suspect this would be a better way to use the 500 MHz bandwidth capacity.

The code operated bridger switch (COS) is a successful technique for disconnecting most sources of noise and interference during the upstream transmission. However, communication with a particular terminal would only be possible for the brief interval during which the feeder was connected. Thus, all communication services would have to be synchronized to the switching control cycle. This would be ideal for polling protocols, but would impose an intolerable restriction on other communications.

THE STAR NETWORK

A much better long-range solution, in my judgment, at least for new systems, is the star distribution network topology. To old-timers, this is simply a fancy name for the "switched system" promoted 10 or 15 years ago in Britain by Rediffusion, Ltd. as "Dial-a-Program", and in the U.S. by Ameco as "Discade". The C-COR and Texscan off-premises converters, and the Times Fiber Mini-Hub could also be called star networks, using remotely switched converters instead of baseband or R.F. switches.

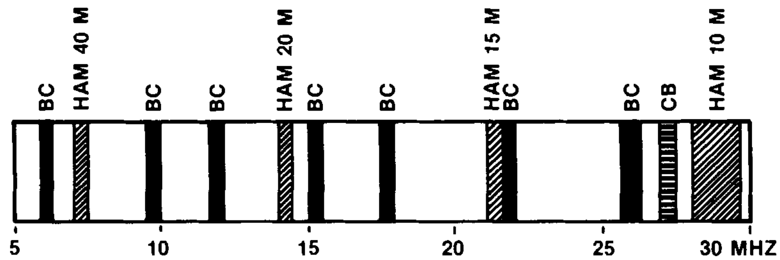
The star network has many advantages (and a few disadvantages) for distribution of television programming to subscribers. But the decisive advantage for interactive message service is that individual subscriber data channels can be switched at the hub to protected trunk channels. The tree-and-branch network is basically a party-line, always open to the noise and ingress picked up by many subscriber service drops. The star configuration, with hub switching, can provide private line protection for individual messages. Concentrators at the star hubs would convert low speed data on the subscriber service drop to high speed data for time division multiplexing on the trunk. Depending on the traffic load, therefore, each data channel on the trunk could serve many subscribers.

To the best of my knowledge, none of the presently available off-premises equipment includes data switching facilities. Digital switching hardware is available in the telephone industry, and could be readily adapted to cable distribution in the star configuration.

The Times Fiber Mini-Hub, using optical fibers for the service drop, is potentially a major advance over off-premises systems using coaxial drops. The fiber is much more difficult to tap illegally; it is almost immune to ingress interference; and its losses are low enough to permit much longer drops.

The most often cited disadvantage of the star (or off-premises converter) network is the psychological hazard of marketing a service which, like telephone service, requires a separate drop for each fully independent outlet. We do have an advantage over the telephone facility in that it is technically feasible to multiplex two, and perhaps more,

UPSTREAM CABLE SPECTRUM



White Spaces assigned to Marine and Aeronautical Fixed and Mobile

separate channels on either coaxial or fiber drops. In most places, for example, Channels 2, 3, or 4 are available for the first service outlet; Channels 5 or 6 would be equally available for a second outlet.

Until optical splitters are available at reasonable loss and manageable price, the Times Fiber system requires two fibers, one upstream, the other downstream. The upstream fiber is quite capable of carrying not only the remote channel selection signals but digital messages as well.

CONCLUSION

After you have worked night and day for months, and spent hundreds of thousands of dollars trying to make your system tight, free from ingress - or reasonably so - I think you will understand what I mean by the "hostile medium".

In my opinion, if we intend to offer "two-way interactive" data services in competition with MCI, Bell, AT&T, and others, we simply cannot fool around with ingress at 5-30 MHz. NASA is still in communication with Pioneer 10 as it passes the planet Neptune, notwithstanding nearly three billion miles of hostile outer space; so far, in fact, that it takes 4 hours for a message to make the trip, each way. Protocols and technology are now available for successful transmission through the interference in our hostile coaxial cables, and the costs, although higher, are probably not prohibitive. Moreover, several more forgiving configurations of the network topology are also available that avoid the accumulation of ingress. Maybe we need both; but we need something fast.

We can no longer afford to play with rubber band airplanes while our competition is building jets.

Malarkey-Taylor Associates
1301 Pennsylvania Avenue, N.W. Suite 200
Washington, D.C. 20004