Using Narrow Band Data Transmission as an Information Delivery System for CATV Applications

Emory McGinty

Scientific Atlanta

ABSTRACT

The cable industry has in place a highly efficient information delivery system to the home supporting video programming and text. Unknown to many people, the same cable system also delivers one-way data from the cable headend to data receivers in the home disguised as cable TV converters. Many addressable converter systems have been using one-way data over cable for years to address and control the services that are offered by the cable companies. The same technology can be used as a cost effective information delivery system to data subscribers having personal computers in their home.

This paper describes a one-way information delivery system using technology available today. Alternatives to modulation format, addressability and security are presented in detail. In order to help the cable operator better understand the impact of encryption on the cable system, many encryption methods are described along with their impact on the cable operator and cable subscriber. Finally, an addressable system with encryption is described which provides the best trade off between addressability, security and cost.

BACKGROUND

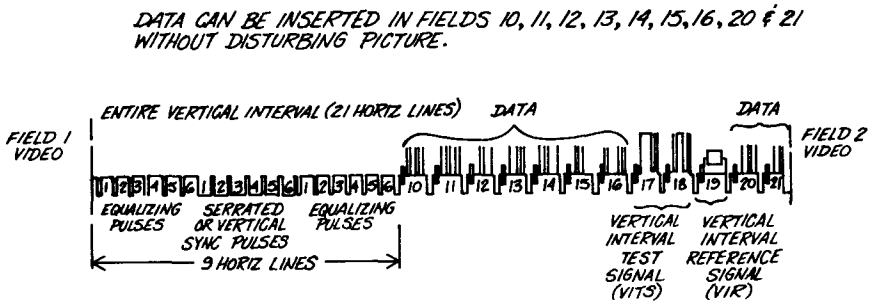
As long as TV's have been available to the budget conscious public, people have been looking for ways to deliver printed information along with the video programming. Early attempts included pointing TV cameras at words printed on a large piece of paper. Technology continued to advance and character generators replaced the cameras and printed page for on-screen text. Now text can be typed directly into a machine and converted directly to a TV signal for broadcast. Computers have found their use in this area by providing large amounts of text storage and by letting the computer decide what text is displayed and when.

WEAK POINTS

Character generators are still used today because they are relatively inexpensive for the cable operator to use and the subscriber only needs a TV to watch both the video programming and text. However, the system has some serious weak points. First, the subscriber must be watching at the time the particular text that he is interested in appears on the screen . Watched video bulletin boards can be very frustrating as page after page of information must be read before information of interest appears. Second, the text uses 6MHz of bandwidth. Now on-screen text must compete with video programming in order for the cable operator to see any merit in its use. Finally, the data is updated very slowly since the user must read through all the information before he finds what interests him. The more text that is displayed, the slower the text can change. And the changing text must accommodate even the slowest reader. Due to the tendency of viewers to lose interest in slowly advancing text, character generated text has had success only with brief messages.

VERTICAL BLANKING INTERVAL

In order to overcome some of these disadvantages, engineers found ways to hide data in the Vertical Blanking Interval ,VBI, of the video programming. The term TELETEXT usually refers to information sent in this manner. An example of data using the VBI is shown in figure 1. The TV paints a picture on the TV screen from top to bottom. When it is finished with one picture it moves the paint brush, or electron beam, to the top of the picture again. The VBI is the time needed for the electron beam to go from the bottom of one picture to the top of the next picture. The VBI has been used for many purposes over the years and no standard has been adopted for its use with



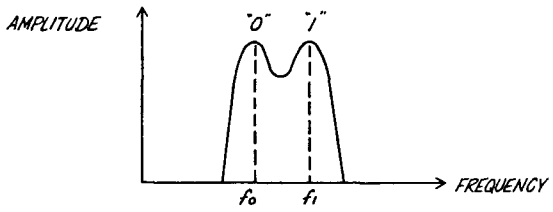
VERTICAL BLANKING INTERVAL WITH DATA

FIGURE 1

data. Using the VBI, thousands of characters of information can be sent in one picture. Unfortunately, the circuitry needed to send and receive information in the VBI is relatively expensive. The data must be separated from the video signal and is coming so fast that it must be stored until it can be seen. And once collected and stored, the subscriber must find some way to display the information.

MODULATED DATA CARRIERS

Modulated data carriers is an alternative to using the VBI. On a modulated carrier, the amount of bandwidth used is a function of how fast the information needs to get to the subscriber. The more the information, the more bandwidth is used [7]. The most popular modulation format for data is Frequency Modulation, or FM. In an FM modulated data signal the data is either a "1" or a "zero", represented by one of two frequencies, see figure 2. The bandwidth is a function of how fast one must switch between the two frequencies and how far apart the two frequencies are set. The circuitry needed to transmit and receive an FM signal is relatively inexpensive.



FREQUENCY MODULATION

FIGURE 2

Computers can talk to one another over telephone lines using this type of modulation. FM modulation also works well on cable TV systems because of its low cost and the small bandwidth it requires. An inexpensive demodulator for receiving 9600 bits-per-second data might use only 200KHz of bandwidth. Less bandwidth is possible by using more costly filters.

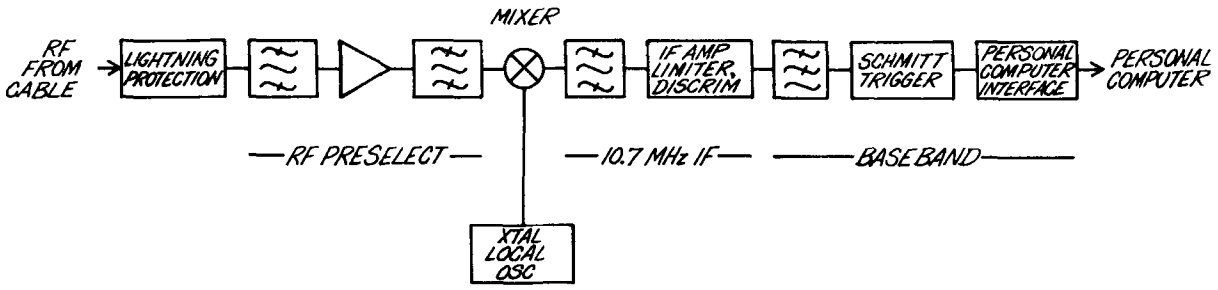
TRANSMISSION RELIABILITY

In addition to data speed and bandwidth, transmission reliability is also important. Different data formats have varying degrees of sensitivity to errors during transmission. VBI is most prone to errors since the information is transmitted as amplitude modulation and is susceptible to many types of noise such as lightning, ingress or poor connections. FM modulation is relatively insensitive to the types of noise typically found on cable systems since the information is sent as alternating frequencies. Limiters in the receiver strip away any influence noise might have prior to data detection. Only noise that interferes with the transmitted frequencies will affect the receivers performance. Addressable converters have demonstrated the high reliability of sending data over cable using Frequency Modulation despite extreme environmental conditions.

Non-addressable Delivery System

NON-ADDRESSABLE SYSTEM FIELD TESTED

Figure 3 shows a demodulator that is being used to receive data over cable. The same design can be applied to data rates up to 64 Kbps by adjusting filter bandwidths and carrier frequencies. Cost and performance were the central goals in the demodulator design. The circuitry uses readily available parts and the performance, measured using a bit-error-rate test set, averaged one error in 10^9 bits with a carrier-to-noise ratio of 20dB. The circuit can be built in an area about the size of a pack of matches. The same circuit was used over the past 12



NON-ADDRESSABLE DATA RECEIVER
FIGURE 3

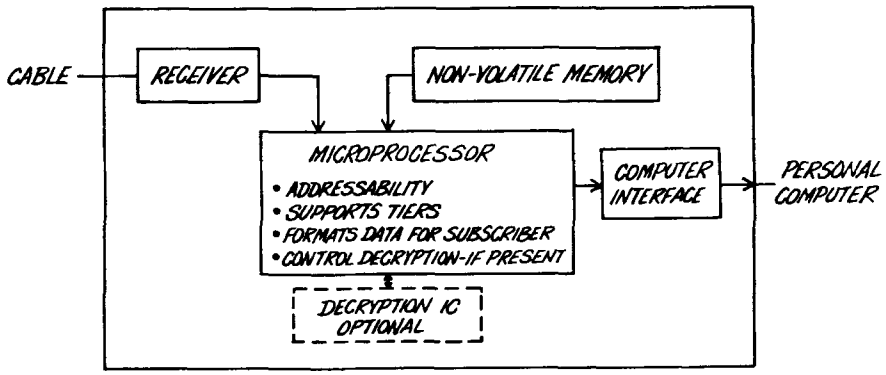
months in several cable systems. The data modulators received data from satellite receivers and modulated the data over cable in the FM band. The data receivers connected directly to the cable and had RS232 interfaces allowing them to be connected to personal computers in the home. Through the system, data was distributed over cable systems to data subscriber's home and the information was collected and displayed on the subscriber's personal computer.

Addressable Information Delivery System

ADDRESSABILITY - PRO'S AND CON'S

For any service provided by a cable operator, the operator must feel confident that he controls who receives the service. This is particularly true when service to a particular subscriber needs to be discontinued. In an addressable receiver, access to the service can be controlled by the cable operator. Once the receiver is deauthorized, the receiver becomes useless until it is authorized once again. Addressability has two major advantages: the cable operator can easily change services or terminate service and the cable operator can charge for tiers of service. Unfortunately, this ability does not come for free. First, the cable operator needs the necessary equipment at the head end to control the receivers, to keep track of who has what authorization levels, and to implement a more complex billing system. Also the cable must be capably of supporting the increased bandwidth needed to pass authorization information along with the data to subscribers. The more authorization and control information that must be sent, the less useful data can be sent to the subscriber.

The main difference between an addressable receiver and a non-addressable receiver is the addition of a microprocessor, (figure 4). The microprocessor does not have to be expensive. Its task is to watch the data as it comes by and look for data addressed to that subscriber. Control data addressed to this receiver is used to load



ADDRESSABLE RECEIVER
FIGURE 4

the authorization tables in the receiver. All authorized non-control data is passed to the subscriber. The same mechanism is present in addressable cable converters and has been for many years. The technology is tested and proven.

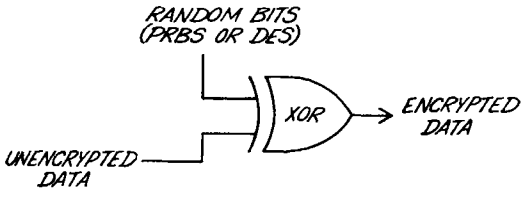
IMPORTANCE OF DATA FORMAT

However, the format of the control data is very important. It must be capable of supporting all the cable operator's current and future needs while keeping the amount of control information to a minimum. Control information gives the cable operator control and flexibility but has no benefit to the subscriber. In fact, it reduces the amount of information he can receive. The amount of control information can be minimized by carefully studying what control is necessary and by using both individually addressed and global commands to the data receiver.

ADDRESSABLE SYSTEM WITH ENCRYPTION

Even with the most sophisticated addressable system, as long as the information is available on cable, people will try to steal it. To prevent data theft, encryption can be used so any information that is received in an unauthorized way is of no use.

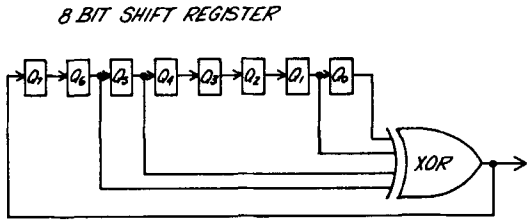
There are several methods used to secure data over cable. The most popular technique relies on using a data format that is so unique that no one could "figure it out" or could they? Some manufacturers use unusual modulation formats, others rearrange the bits that are transmitted in a fixed format that is difficult to figure out. Unfortunately, these techniques do not take into account the "hacker" who delights in these types of challenges. And the worst part is that they publish their findings in user club journals and the secret is no longer a secret. Another form of security is by "exclusive ORing" random 1's and 0's with the data before transmission. This is called encryption and is shown in figure 5. The receiver must know how to remove the random data so it can correctly interpret the data it received.



ENCRYPTION
FIGURE 5

TYPES OF ENCRYPTION

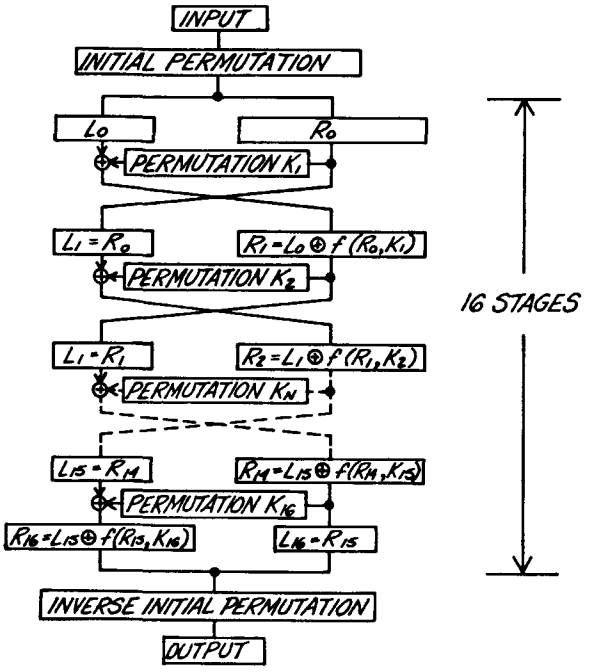
There are two types of encryption algorithms commonly used for data transmission: Pseudo-Random Binary Sequences (PRBS) [1,4] and the Data Encryption Standard (DES) [2,5]. The PRBS method of encryption, figure 6, can provide an affective method of encryption when the data changes often and its importance does not warrant an unauthorized subscriber using computers to attack the encryption. Data that has great value such as electronic fund transfer or non-delayed stock quotes require more protection than PRBS



PSEUDO RANDOM BINARY SEQUENCE
FIGURE 6

provides. The National Bureau of Standard adopted the DES algorithm, figure 7, for these types of applications. The algorithm can be implemented in either microprocessor software or a single Integrated Circuit containing the DES algorithm. This algorithm is gaining popularity for use in data distribution due to its availability in a single IC. Information Providers wishing to deliver data over cable want as much protection of their data as is available. Even if the DES algorithm is more security than is warranted, the information provider will often ask for it because they equate the name with security. One information provider might require multiple levels of encryption for many tiers of data to the subscriber.

Readers should be aware that the DES IC's are difficult to use. From a list of available DES IC manufacturers [2] we selected one based on its speed and flexibility. A bread board has been built using this chip for applications where security of data is of primary concern. The intent was to design a system where encryption can be added economically as it becomes necessary.



DATA ENCRYPTION STANDARD

FIGURE 7

ENCRYPTION KEYS

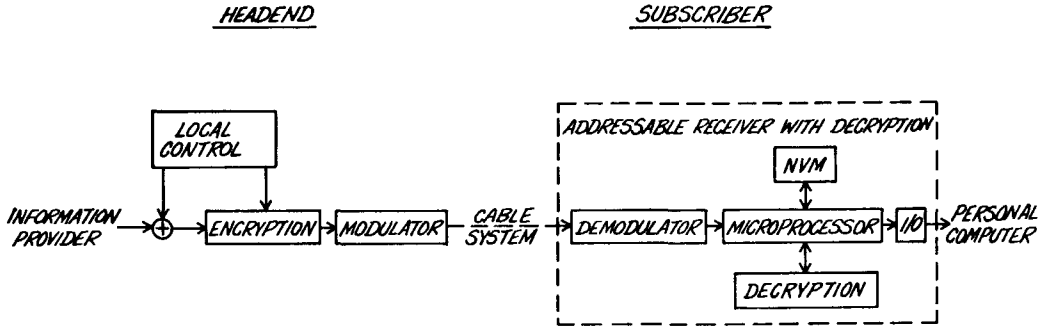
No matter which encryption algorithm is chosen, the data is protected only as much as the encryption key used to create the data [3,6]. Just as a house key provided to a crook bypasses all the locks and window bars, the encryption key unlocks access to the data. Unfortunately, the receiver needs to know the key that was used in the transmitter so it can decrypt the data. So, keys must be sent down the cable to the appropriate receivers. The keys must be encrypted using keys known by both the transmitter and receiver. They should be changed as often as practical. One method used for sending keys requires future keys to be sent encrypted with current keys. Then at some predetermined time or as a result of a global command the future key becomes the current key and the process continues. Both the transmitter and receiver always know which key to use to decrypt data.

ENCRYPTION ON CABLE

An addressable data system with encryption can be added to any cable system as shown in figure 8. The receiver, figure 4, consists of many of the parts that are already in most addressable cable converters. The method of encryption can be any of those already discussed.

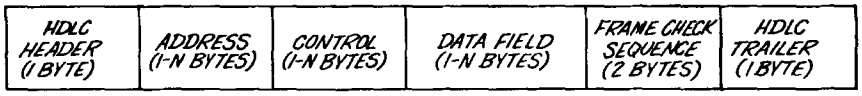
ENCRYPTION DATA FORMAT

The data format, shown in figure 9, supports both global and individual commands for controlling authorization, tiers and encryption. It is compatible with the High-level Data Link Control, HDLC, data format. The address information is not sent encrypted so the receiver can identify its data on power up when encryption keys have not been sent. The data field including the authorization data and future key is encrypted using the current key. The address information can be extended by setting the most-significant-bit in the address field or any control field indicting that the next byte is part of the current field. DES was chosen for our method of encryption for maximum protection of data during transmission. The system shown can accommodate a modular evolution from non-addressable to addressable to addressable with encryption.



ADDRESSABLE DATA DELIVERY SYSTEM WITH ENCRYPTION

FIGURE 8



ADDRESS	CONTROL FIELD	DATA FIELD
ALL '1' = GLOBAL ALL OTHERS = NONGLOBAL	ENCRYPTED FUTURE KEY	FUTURE KEY ENCRYPTED WITH CURRENT KEY
	ENCRYPTED AUTHORIZATION	AUTHORIZATION LIST ENCRYPTED WITH CURRENT KEY
	ENCRYPTED DEAUTHORIZATION	NONE (ALL AUTHORIZATION TABLES DELETED IN RECEIVER)
	ENCRYPTED NEW USER	CURRENT KEY ENCRYPTED WITH USERS SERIAL NUMBER FOLLOWED BY AUTHORIZATION LIST ENCRYPTED WITH CURRENT KEY
	NONENCRYPTED AUTHORIZATION	AUTHORIZATION LIST WITHOUT ENCRYPTION

ADDRESSABLE FORMAT WITH ENCRYPTION
FIGURE 9

CONCLUSION

As cable operators seek additional sources of revenue from their cable system, delivery of digital data to the home can be a benefit to both the cable operator and subscriber. Information providers continue to explore new ways to deliver their information and the technology is available to use cable as the next frontier. Knowledge of digital transmission methods and encryption techniques can help the cable operator take advantage of the opportunities unfolding in this new digital data frontier.

BIBLIOGRAPHY

[1] F. Jesse MacWilliams, Neil J. A. Sloane, "Pseudo-Random Sequences and Arrays," Proceedings of the IEEE, December 1976, PP 1715-1729.

[2] C. R. Abbruscata, "Data Encryption Equipment," IEEE Communication Magazine - September 1984, Vol. 22, No. 9, PP 15-21.

[3] Daniel Fidlow, "A Comprehensive Approach to Network Security," Data Communication, April 1985, PP 195-219.

[4] V. K. Bhargava, D. Halcoun, R. Matyas, P. Nospl, "Digital Communication by Satellite," John Wiley and Sons, New York, PP 275 -280.

[5] Carl H. Meyers, Stephen M. Matyas," Cryptography: A New Dimension in Computer Data Security," John Wiley and Sons, Ney York, PP 113-189.

[6] Carl H. Meyers, Stephen M. Matyas," Cryptography: A New Dimension in Computer Data Security," John Wiley and Sons, Ney York, PP 271-329.

[7] A. Bruce Carlson, "Communication Systems, An Introduction to Signals and Noise in Electrical Communication," McGraw-Hill Book Company, New York, PP 222-238.