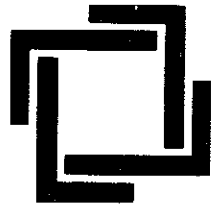


THE FINAL REPORT OF A STUDY OF THE TECHNICAL AND ECONOMIC CONSEQUENCES OF SCRAMBLED TV SERVICES OFFERED BY DIRECT BROADCAST SATELLITE

CARRIED OUT FOR THE
COMMUNICATIONS RESEARCH CENTRE
OF THE
DEPARTMENT OF COMMUNICATIONS
UNDER DSS CONTRACT NUMBER
3ER.36001-1-2052

by

Philip A. Lapp Limited
CONSULTANTS TO INDUSTRY AND GOVERNMENTS

FEBRUARY 1982 Work Carried Out By K.E. Hancock
D.C. Coll
D. George
C.L. Balko

Approved By .....
K.E. Hancock
Vice President
Telecommunications

HEAD OFFICE: SUITE 302, 14A HAZELTON AVENUE, TORONTO, ONTARIO, CANADA M5R 2E2
Phone (416) 920-1994

OTTAWA OFFICE: SUITE 904, 280 ALBERT STREET, OTTAWA, ONTARIO, CANADA K1P 5G8
Phone (613) 238-2452, Telex 053-3314

CONTENTS

A STUDY OF THE TECHNICAL AND ECONOMIC CONSEQUENCES OF SCRAMBLED TV SERVICES OFFERED BY DIRECT BROADCAST SATELLITE

1. INTRODUCTION

In the past a number of television services such as Pay TV (distributed by Cable Television Networks), Subscription TV Networks, and more recently Pay TV, (delivered by satellite to cable headends), have had the requirement for scrambling or encryption of the transmitted signal to prevent use by unauthorized persons. These requirements have lead to the development of a number of methods of scrambling and encryption, with various levels of security as needed by the particular service.

The likely advent of a direct broadcast satellite system in Canada, and its probable use by Pay Television and other services requiring secure transmission, has lead to the need for an investigation into the unique problems arising from the wide-spread use of a direct broadcast satellite for these services. This study investigates some of these problems and their possible solution. As well as the obvious requirement for technically feasible encoding and decoding equipment, the overall needs of the system, the economic aspects of the various types of service likely to use scrambled systems, and some of the unique Canadian policy considerations are investigated by this study.

2. CONTRACTUAL REQUIREMENTS AND STATEMENT OF WORK

Work contained in this report was carried out under DSS Contract No. 3ER.36001-1-2052 for the Communications Research Centre for the Department of Communications.

The contract identified the study requirement as:

"To provide a Report as a result of a study and review of the technical and economic trade-offs and consequences of scrambled TV services offered by direct broadcast satellite (DBS), as detailed in the Statement of Work. The study is to include the following aspects of scrambled TV services offered by DBS:

- methods of scrambling which could be applied, including complexity, security and durability.

- economic issues such as markets and penetration of services in light of methods identified by the study, as well as cost/performance trade-offs. Also, identification of forces driving technology development.

- system configurations required for distribution of a variety of services, including discussion on scrambling/descrambling insertion points, demands on the satellite resulting from mixtures of services, interference between channels caused by scrambling, key distribution and addressability.

- policy sensitive issues such as TV services to remote areas and fostering of standardization of Pay TV hardware including international compatibility of signals. Recommendations for future activities in order to resolve technical unknowns.

This requirement was expanded in the contract by the following Statement of Work:

"The study will provide a report of information on four aspects of scrambled TV services via DBS. The report is to reflect the results of a study and review of these aspects, as follows:

- Technical Considerations (Section 1)

  Assess candidate scrambling and addressing concepts suitable for controlling reception of video services (pay TV, closed circuit services, etc.) likely to be delivered by community and direct-to-home satellite systems. Include those concepts now in use or known to be under consideration for subscription TV. Also, include a discussion of the complexity, and durability of candidate techniques.

- Economic Considerations (Section 2)

  The requirements for controlled reception of scrambled services may include among others:

  (a) Commercial Broadcast Signals;
  (b) Pay TV;
  (c) Educational Networks;
  (d) Teleconferencing;
  (e) Video/Teletext Services;
  (f) Medical Services.

Discuss related economic issues such as potential markets and penetration of services in light of concepts identified in the Technical section of the report. Identify forces driving present technology development in this area. Also identify cost/performance trade-offs which are available.

- System Configuration (Section 3)

  Consider system configurations for distribution of services identified in the Economic section of the report taking into account the ease of expansion of the number of channels and the capability of selectively denying access to any combination of channels. Include demands on the satellite due to interference between channels caused by scrambling, and bandwidth expansion caused by points, addressability, vulnerability to interception, short and long term integrity/ vulnerability, and key distribution/protection.

- Policy Sensitive Issues (Section 4)

  Discuss provision of pay TV to remote areas with regard to durability and cost of systems.

  Identify policy issues regarding the use of multiple scrambling techniques. Investigate the potential for the development of a "universal" solution which would foster standardization of pay TV hardware both for domestic and international signal compatibility.

  Recommend, as required, future activities which will resolve technical unknowns. Identify technology developments which may result in economical implementations of controlled reception techniques."

By agreement with the Scientific Authority, the item headed "Teleconferencing", under Economic Considerations, was deleted during the course of the contract. In addition, minor reformatting of the various sections of the report was mutually agreed to in the intersts of continuity.

The contract commenced on November 6, 1981, with a contractual completion date of March 31, 1982. After the commencement of the contract, it become apparant that it would be possible to complete the work by mid February, 1982. The Scientific Authority welcomed such a reduction in time scale and the contract was carried out meeting this revised completion date.

3. CONTEXTS WITHIN WHICH THE STUDY TOOK PLACE

The study took place in the context of existing television scrambling technology (developed primarily for the cable and pay TV industry); rapid advances in digital signal processing electronics and the economics of integrated circuits (VLSI); the development of non-programming services (including Telidon); the advent of office automation (which really means mediated office communications and information systems) and the trend towards digital communications, including digital television.

In parallel with these technological changes, the move toward the use of a direct broadcast satellite in Canada takes place within a framework of broadcasting policy that is in a major state of flux. The concept of Pay TV itself is a radical change which has been resisted for many years in the face of growing pressure from certain segments of the broadcast industry. The use of a broadcast satellite itself is still the subject of considerable controversy. The programming that might be permitted on a DBS satellite is again the subject of considerable discussion and disagreement. Some of these matters have a direct impact upon economic and other considerations of scrambled DBS service, others have a secondary impact, and still others have a major impact on the concept of the use of satellite transmissions for any form of video service.

In the classical secure communications situation, there exists a message originator and a message receiver, and one or more eavesdroppers. The assumption is that the originator and authorized receiver form a co-operative agreement to exchange information using an encryption scheme, which, hopefully, the eavesdropper does not fully know. In the DBS scrambled service situation the receiver cannot be considered to be cooperative. It is in the interests of the receiver to be able to make use of the video signal without in fact becoming a subscriber. Again the classical broadcast mode precludes two-way exchange of information, therefore, the subscriber cannot authenticate a message. A possible exception to this is if the domestic telephone service is used in one form or another to communicate authentication and other information from the subscriber to the originator.

The degree of security is usually measured by the time and resources it takes an eavesdropper who has complete knowledge of the encryption method being used (and often a duplicate of the actual apparatus) to decipher the

intercepted signal. The implication of security when the method of scrambling is known is that the exact state of the encryption/decryption process at any given time is determined by a "key" known only to the originator and cooperating receivers. The security of the information is therefore no better than the security of the key. It may be, however, that even though the method is known and the key is fixed that duplication of the decryption process might be beyond the capabilities of all but the most dedicated of intruders, and this aspect is certainly a factor in the security level of scrambled TV.

Let us consider briefly the level of communication security in current satellite transmission and television broadcasting, from the point of view of the effort and resource required to intercept and extract information from them. In this regard, it should be noted that no system is totally secure, some eavesdroppers are willing to go to extreme lengths to intercept and decipher massive amounts of traffic. Security depends on how often a key is used, its complexity, the value to the eavesdropper in breaking it, and the value to the communicants in maintaining it.

By and large, satellite transmissions were relatively private until fairly recently. This was due in large part to the monopoly position of government agencies and the common carriers in satellite communications, and to the elaborate and expensive earth station equipment required to receive the signals. This situation has changed radically in the past year or so. It is possible, for the cost of a small automobile, to receive and demodulate TV signals emanating from US satellites and display the receiver output on a standard TV set; even though the legality of the reception of satellite signals by individuals in Canada is still in question. These signals, emanating from a US satellite, are intended for the use of subscribers such as cable TV operators who have paid for the priviledge of using the content, and as such might be considered to be the same as point-to-point communications whose interception and use is considered to be "theft of communication", and yet (aside from the fact that it is contrary to a bi-lateral agreement for Canadians to receive signals directly from a US satellite) the signals can be picked up throughout the "foot-print" and might therefore be considered as broadcast signals, which once launched, are free to be received and used.

Direct broadcasting from a satellite is usually taken to mean direct-to-home or single location, although in many instances, particularly in urban areas, there is likely to be further local terrestrial distribution. The obvious implications are that there are large numbers of relatively unsophisticated users who may be scattered over a large area. The receiving antennas must be small, light but rugged and inexpensive to acquire, mount and maintain. The RF receivers must be likewise inexpensive, easy-to-use, reliable and rugged. Descrambling apparatus must have the same characteristics of low cost, high reliability, and ease of operation.

As mentioned previously, most secure communcation, i.e. encryption, deals with messages composed of discrete elements - for example, data communications. Some systems for scrambling analog voice signals do exist, but the level of security is low. Secure voice communication is most readily achieved by sampling voice waveform, digitizing the samples, enciphering the resulting bit stream, and transmitting it as a digital signal. Much work has been expended on the speech sampling process so that its digital representation can be transmitted in the same bandwidth as the analog signal. The redundancy in the voice waveform makes this bandwidth compression possible. Voice bandwidth bit streams, i.e. from 300 to 9600 bits/second can be easily enciphered and deciphered using single chip devices, with its security certified by the US National Bureau of Standards. This standard chip is being used extensively to protect information in data communications and data bases.

Analog television signal scramblers have been extensively developed for the cable and broadcast (subscription) pay TV market. Those of these systems that are relevant to DBS, described in some detail later, tend to be either fixed in their operation or broadcast the key either along with the signal or in an adjacent band. Thus, these methods rely for their success on a fairly benign set of eavesdroppers. Once the mechanism is determined, a simple copy of the receiver will suffice to duplicate its operation. The complexity of most of them is well within the grasp of most electronics technologists to defeat. Certainly none of them would stand up to a concerted, well-funded attack.

However with modern LSI techniques with much of the encryption techniques embedded within the crystals and the decoding devices made chemically secure, DBS

decoders manufactured for a large market are likely to be beyond the reproduction capabilities of "garage entrepreneurs". Large scale copying and theft would be difficult to conceal, and the normal protection of the Criminal Act against theft of services could possibly prevent a well funded concerted attack on the security of commerical Pay TV and similar services. It should also be noted that most service industries expect, and can be designed to live with, a certain, albeit low, level of theft of service.

The final consideration in this section must be that of the development of a DBS system capable of multiple-point uplink or transportable uplinks whilst maintaining synchronization and security. An additional factor in the security could well require individual electronic addressing of all subscribers, although there are non-electronic alternatives.

It can be seen that the study takes place in the context of a large number of complex variables only some of which are amenable to technical solution. The others have sociological, economic and political implications which must be considered in drawing conclusions and making recommendations.

4. TECHNICAL CONSIDERATIONS AND CONCLUSIONS

In this section of the report, the various technical approaches for scrambling and descrambling are considered. Technical considerations in this context are defined as the technical requirements for scrambling and descrambling systems and relate mainly to hardware requirements. More detailed consideration of scrambling keys and cryptographical software are considered in Section 6 - "System Considerations and Conclusions".

In considering technical requirements for decoders for use with a direct broadcast satellite, a number of key requirements are first defined.

Two groups of subscribers are considered. The first group would be those subscribing to public services such as Pay TV. The assumption is made that these services will be distributed very widely, and therefore the major decoder requirements are based upon a consumer environment with the scrambling system required to operate in a non co-operative addressee situation, and with the number of decoders required being in the order of one million.

The second group of subscribers are those to whom private services are distributed, this being defined as those services planned for a specialized or limited audience rather than a general audience. These include but are not limited to such services as educational, medical and teleconferencing.

Wherever possible, and in conjunction with the scientific authority, a norm for each requirement in each of the two service situations is defined to permit classification of scrambling methods into broad categories such as low, medium and high.

Having defined the requirements, a wide range of scrambling methods were investigated, including those in current use, those under development and those conceived but not currently under active development.

A matrix was constructed to show how each of the scrambling methods met the defined decoder requirements.

This section expands on each of the decoder requirements and then considers each scrambling method in the light of those requirements and makes a preliminary assessment as to the most likely candidates for DBS scrambling systems. Conclusions are then arrived at.

4.1 Definition of Major Scrambling Decoder Requirements

Given below are the various requirements for scrambling decoders for use with a DBS system.

It is perhaps appropriate at this time to discuss in broad terms why there is a need for scrambling or security of certain types of DBS service, and how this security requirement differs from many others.

A Direct Broadcast Satellite represents an efficient and cost effective method of distributing one way services, such as television, radio and information services, to Canadians regardless of their geographic location. In particular the DBS is seen as an economic method of providing such services to Northern and remote areas where the sparse population density would make the cost of distribution by any other method prohibitive.

As well as services which are supported either by advertising or, in the case of CBC services, by government funding, it is perceived that DBS will be used for the distribution of services paid for specifically by the person receiving them. Typical of these are Pay TV and specialized services such as educational courses, medical information and so on. In the case of these services paid for by the individual receiving them, there is obviously a requirement that it shall be difficult or impossible for non-subscribers to receive the service. It is perhaps a truism in today's technical world that anything that can be coded can also be decoded. The matter of security in this sense therefore hinges around the difficulty or inconvenience of such decoding. This matter will be discussed in greater detail under the heading "Degree of Security".

One of the key characteristics of a DBS is that the receive signal will be such that it is possible for it to be received by a small (maximum 2 meters) parabolic antenna located at the subscriber's home or business facility. It should borne in mind however that it will frequently be appropriate, particularly in an urban situation, for the signal to be received by a fairly sophisticated ground station and then redistributed by Cable Television or other appropriate means. Again this will be discussed in greater detail under "Effects of Redistribution".

A major assumption made throughout this report is that economic, sociological and technical requirements for scrambling systems will dictate that the decoder should be a unit separate from the TV set, and must therefore have an RF output. Possible modular TV sets of the future, and their impact on decoders in public service use are not considered due to the uncertainty of their universality.

4.2 Decoder Cost

4.2.1 Public Service

For a DBS and any service that it carries to be viable, the overall cost must be shared by a very wide audience. Previous studies have indicated that to be acceptable the total cost of a direct-to-home Receive Only Satellite Earth Station (ROSES) should be between $500 and $1000 in 1981 terms. Discussions with interested organizations and with the scientific authority for this contract came up with the figure of $100 as a norm for the descrambler portion of the ROSES.

It should be recognized that there are a number of policy implications to this cost figure such as whether or not the decoder would be owned by the subscriber or by the service distributor; whether or not a "universal" scrambling system is in use permitting the decoder to be part of the television set; and whether or not it is necessary for the subscriber to have access to the decoder for encryption key changing or other purposes. However within the framework of the general approach being taken here it is assessed that these matters would not have a significant effect on the required cost norm. The cost of public service decoders is considered to be a very key factor in the whole consideration of DBS scrambling.

4.2.2 Private Service

In that security requirements for private service can be expected to:

- require a high degree of security
- be produced in comparatively small quantities, say a maximum of 25,000,

a cost norm for the decoder was set at $500 in 1981 terms.

4.3 Reliability

Reliability in this context is taken to be the electronic reliability of the components of the decoder when operating with normal domestic and office power sources. As in both public and private service the decoders are required to operate in conjunction with domestic television sets, the required reliability norm has been taken as equivalent to a "top of the line" domestic television receiver.

4.4 Robustness

For the purposes of this report robustness is taken as the ability to operate satisfactorily under defined environmental conditions.

4.4.1 Public Service

In this case the environmental conditions defined as the norm of those of an active home environment. The assumption is made that the decoder is a separate box from the television set and must therefore be robust enough to withstand normal abuse from children, dogs, cups of coffee, etc. On the other hand temperature will be usually be kept within +10°C to +30°C.

4.4.2 Private Service

In this case the norm is taken as the office environment. Generally speaking the abuse given to office equipment is somewhat less than that given in the home.

4.5 Size

While in most cases it is envisaged that the size of the decoder will be a lot less than the maximum acceptable size, the norm, or in this case the maximum, is taken as 8 cm high and the approximate cross section of a domestic TV set. The TV set could therefore sit on top of the decoder. The norm for both the public and private service requirements is therefore taken as 25 cm X 15 cm X 8 cm.

4.6 Degree of Security

This is another key factor and is defined as the difficulty of decoding the scrambled signal by an unauthorized user. The concept of a norm is not appropriate to this parameter and instead four levels of security have been selected and will be defined below. These definitions will be appropriate to both public and private service.

The four levels of security are termed:

- trivial
- easy
- hard
- secure

4.6.1 Trivial

Trivial is defined as that level of security that only requires either the most simple modifications to a TV set, such as offsetting with the fine tuner, or the use of a readily available and comparatively inexpensive piece of equipment. Examples of trivial security are the use of frequencies requiring a standard inexpensive commercial converter, or the use of simple sync suppression which is automatically overcome by modern high quality TV sets.

4.6.2 Easy

This is defined as that level of security which could be easily overcome by simply made and possibly readily available and inexpensive electronic circuitry.

Envisaged here is the type of thing that hobby magazines would publish with circuitry and "how to do it" instructions. Such articles are already available to overcome the more simple types of TV scrambling (35). However the point to be made here is that although a great deal of knowledge is not required, some interest and "do it yourself" skill is required. This would, in all probability, limit the number of viewers prepared to go to these lengths to a percent or so. The actual number would depend upon the value of the service to be received and a number of other factors.

4.6.3 Hard

This is defined as a level of security which would foil a computer hobbyist, but could be designed and manufactured by professional organizations.

4.6.4 Secure

This is defined as a very high level, usually digitally encrypted, security. To overcome this type of security fully trained professional cryptographers would be required with major computer facilities. This is the sort of security level used by the military and by banking organizations for the transmission of their most secret or valuable information.

4.7 Residual Intelligibility

This is defined as the intelligence that can be received from a scrambled TV channel. It is broken down into audio and video. In a number of cases, while the video signal might be scrambled, the audio may not be scrambled, and vice versa. In some cases, with certain programming conditions, it may be possible, for short periods of the scrambled video transmission, to identify the scene.

For both private and public services the norm for residual intelligibility is taken as that level where although some intelligence is receivable, this level is low enough to prevent the understanding of the program as a whole, and is such that it will cause irritation with the picture and inhibit any attempt on the part of the viewer to watch on a continuing basis.

4.8 Degree of Restoration

This is defined as the quality of the overall television signal, including both video and audio, obtainable after descrambling or decoding.

This is considered to be another key requirement. It should be borne in mind that all scrambling or encoding will degrade a quality of a television signal from that achieved prior to scrambling or coding. At the same time, by definition, the signal is one which has a direct value to the viewer in-so-much that he is paying cash for it, and is therefore normally expected to be of the highest technical quality.

These two requirements mean that:

a) the input signal must be of the highest quality
b) the scrambling/descrambling process should not degrade the input signal to a point where the degredation is annoying to the subscriber.

Thus the norm for this parameter is taken as the signal quality delivered to the subscriber shall be of an impairment grade of four or better, where impairment

grade four is defined as "perceivable but not annoying". (See Note 1).

This norm is applicable to both public and private service.

4.9 Degree of Interference with Other Signals

By this is meant any spurious signals emananated either by the satellite transponder, the ROSES or the decoder itself, as a result solely of the scrambling or descrambling mechanism, that in any way interfere with any other signal being transmitted through the satellite, or received by the subscriber's television set.

For this parameter the BP23 impairment definition (See Note 1) is once more used, and the norm defined as being that emissions should not degrade other signals below impairment grade four.

This norm applies to both private and public service.

4.10 Bandwidth Requirements

It is possible that some forms of encryption or scrambling will require that pilot tones or other signals be transmitted outside of the normal NTSC colour television frequency bandwidth. To compare scrambling systems in relation to this parameter, the norm of a standard NTSC type M transmission of a video bandwidth of 4.2 MHz with RF bandwidth of 6 MHz is taken.

This will apply to both private and public service.

(Note 1) As defined in Broadcast Proceedure 23:

Impairment grade	Impairment
5	imperceivable
4	perceivable but not annoying
3	somewhat annoying
2	severely annoying
1	signal unusable

4.11 Encoder Costs

In considering the overall costs of any scrambling or descrambling system the one time cost of the encoder must be taken into account. While it will be appreciated that this is not strictly a decoder requirement it is one consideration in the selection of the overall system.

The selection of a norm in this case is to a large extent arbitrary and has been selected as $25,000 for both private and public systems.

4.12 Conformity to Current Standards, Regulations and Policies

In broad terms all services, including scrambling services, provided by a DBS will fall under either one or both of the Broadcast or Radio Acts.

Again in broad terms the Radio Act is the jurisdiction of the Department of Communications whilst the Broadcast Act is the responsibility of the Canadian Radio-television and Telecommunications Commission (CRTC).

Both of these organizations publish regulations and policies, in some cases backed up by standards. (38)

The decoding requirement being considered under this paragraph is the degree of conformity with current, or in some cases likely future, regulations, policies or standards propagated by these two organizations.

4.13 Ease of Multi-Channel Scrambling or "Tiering"

In a number of services requiring scrambling, notably Pay TV, there is frequently a requirement to concurrently deliver more than one channel of scrambled television.

In many cases it is a requirement of the distributing agency to permit subscribers to receive one or more levels of service, each level consisting of one or more Pay TV and possibly other nonscrambled services. This concept is called tiering. For further clarity a written and diagrammatic explanation of one example of a tiering system is given in Appendix D to this report.

When a tiering system is used it is a requirement of the scrambling system as a whole, and the decoder specifically, to permit the subscriber to receive only those tiers for which he has subscribed.

The requirement considered in this paragraph is the ease in which this selection can be carried out. For both public and private systems the norm for this parameter is taken as the selection of tiering requiring no additional curcuitry or mechanism for tiering selection.

As this parameter is likely to be of considerable importance in future multi-tier systems, for the purposes of this study it is considered a key requirement.

4.14 Effects of Redistribution

Although a Direct Broadcast Satelitte system is frequently considered to be a "direct-to-home" system where the ROSES is situated at the subscribers residence or office, in practice a considerable portion of subscribers are likely to receive the signal via a cable television system, a rebroadcast transmitter, a multiple distribution system or other terrestrial distribution network.

This being so, it is important that the ease in which any specific scrambling system can be distributed by one or more of these terrestrial distribution networks be considered.

For this parameter the norm is taken as a scrambling system that can be used on a normally loaded cable television network without causing unacceptable interference to other channels, or for some other reason requires descrambling and rescrambling.

It should be noted that this does not apply to cable television systems using passive "traps". In this case descrambling and transmission without rescrambling is considered acceptable.

Because of the likely use of redistribution systems with a DBS, this is once more considered to be a key requirement.

4.15 Availability

Under this heading we indicate the current availability of the scrambling system together with, wherever possible, the company or companies manufacturing such systems.

As this is a information parameter no norm is specified.

4.16 Technical Review of Candidate Scrambling Systems

Below, various methods of scrambling possibly suitable for DBS use are reviewed in sufficient detail to indicate key technical characteristics. No attempt is made to give complete technical design information, as where this is non-proprietary, it is available in documents referenced in the bibliography in Appendix A. (34, 35, 36, 37)

This section should be read in conjunction with the "fold-out" matrix of candidate systems against key descrambler requirements given as Figure 7.

To aid in the comprehension of the system descriptions given below, the composition of an NTSC Type M television channel is given as Figure 1.

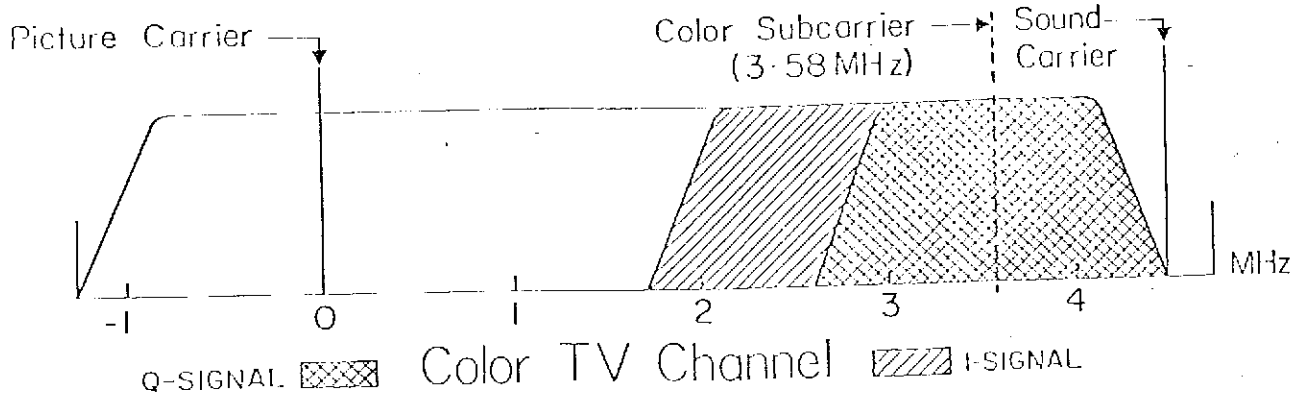
4.16.1 Nonstandard Transmission Frequency

While at first glance this may seem to be a trivial method of security, in some circumstances it might be quite adequate. Examples of this could be specialized non-video private services destined for a small audience and of little or no interest to the general public.

A nonstandard frequency, perhaps using an additional carrier on a portion of an overall transponder not occupied by a video channel would be particularly appropriate for specialized data or voice services. The cost of providing such a nonstandard receiver frequency of narrow bandwidth would be quite low. For these narrow band private services all key requirements would be met with the security being provided by the signal itself in the case of data, and the undesirable programming content in the public sense for audio services, and of course by the nonstandard frequency. Due to the required standardization of frequency plans, this method is not applicable to private video services, nor of course to public services. However for specific narrow band low speed data and audio private services it should definitely be considered a low cost candidate.

FIGURE 1

COMPOSITION OF A NTSC TYPE N TELEVISION CHANNEL



(derived from information given in CTRI Pay-TV Technology 1981)

4.16.2 Interfering Carrier

The simplest of all scrambling systems consists of the addition of a jamming carrier to the transmission channel. This effectively prevents clear reception of the signal unless a specially designed filter (a positive trap) is inserted ahead of the receiver to remove the jamming interference.

The basic form of video jamming signal is a single unmodulated carrier placed about 2.25 MHz above the video carrier (see Figure 1). Such interference is however relatively easy to remove and does not produce a completely effective form of scrambling. More effective versions, such as the Model 2-DF trap manufactured by EAGLE Comtronics Inc., employ dual modulated interfering carriers placed sufficiently close in frequency that their resultant interference can be removed by a simple multipole positive trap.

The addition of modulation to the jamming carriers results in more effective video scrambling and can at the same time introduce some interference into the FM audio channel. The mechanism of this audio channel interference is indirect and actually a result of distortion products produced within the receiving TV set itself.

Figure 2 shows a typical composite TV spectrum after the addition of a jamming signal. The effect of the restoration filter (positive trap) is to remove the interference together, unfortunately, with a portion of the energy of the original signal. This is illustrated in Figure 3.

Two degradation effects are now unavoidable. One is a slight reduction in the signal-to-noise ratio of the restored video signal. Typically this is of the order of 0.7 dB and should be compensated for by a corresponding upgrading of the original channel carrier-to-noise ratio by means of pre-emphasis. The second effect is a slight loss of picture resolution due to the inevitable removal of some of the video intensity information.

Although low in cost, the low degree of security, low degree of restoration and high degree of residual intelligibility as well as other problems preclude the consideration of this simple system for use with DBS.

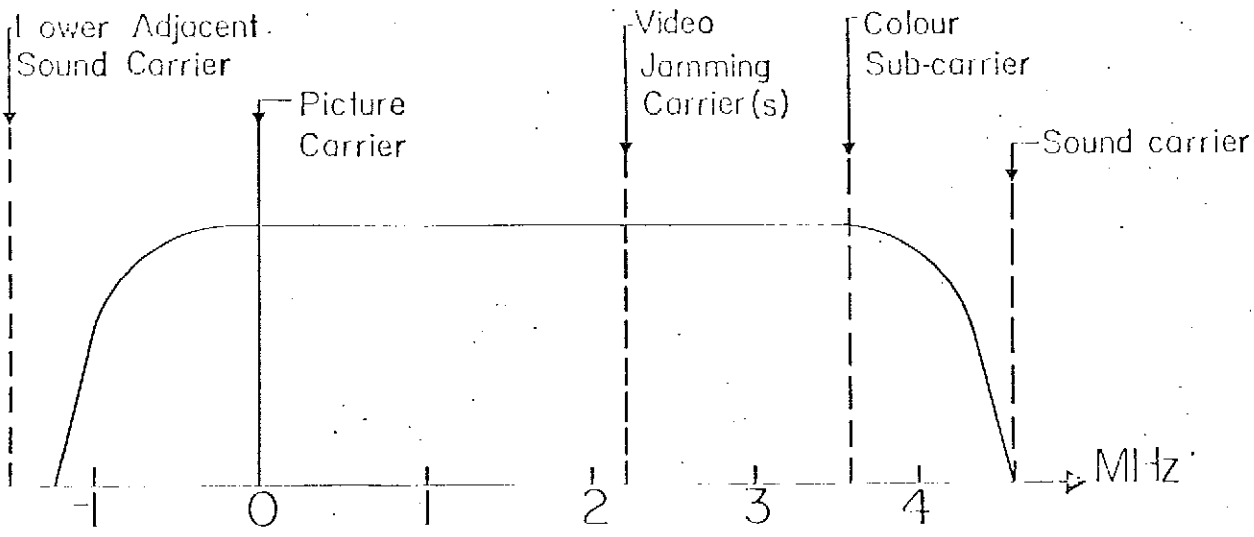


FIGURE 2: JAMMING CARRIER(S) IN VIDEO CHANNEL

(derived from information given in CTRI Pay-TV Technology 1981)

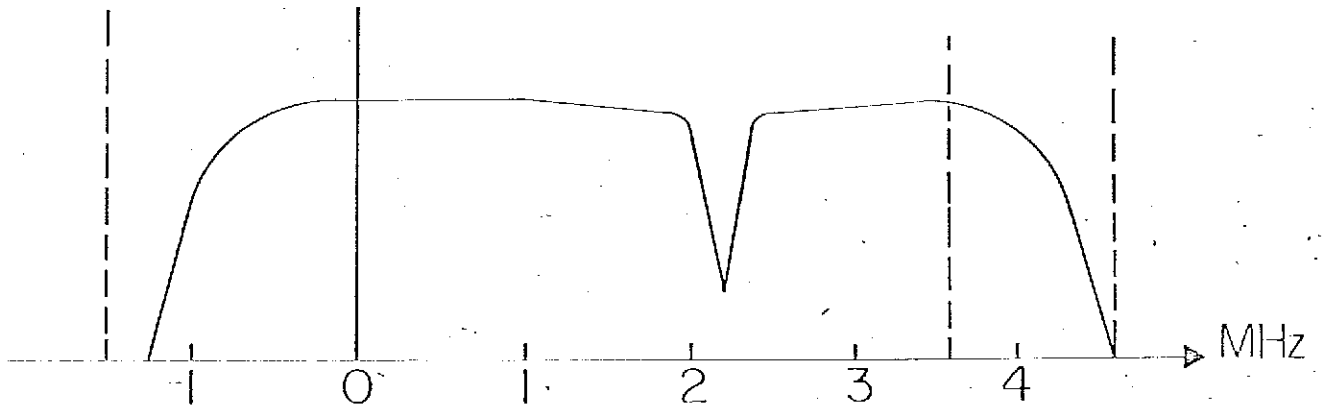


FIGURE 3: EFFECT OF POSITIVE TRAP LOCATED SO AS TO REMOVE JAMMING CARRIER(S)

(derived from information given in CTRI Pay-TV Technology 1981)

4.16.3 Continuous Video Inversion

A relatively straightforward video scrambling technique, the complete inversion of the composite video signal ranks high in effectiveness. The domestic receiver then synchronizes on anything but the line pulses, since they are received with their polarity reversed.

In the descrambler, the carrier is extracted from a phase-lock circuit, delayed and added back in, at twice its original level, to restore the correct relative polarities. The scrambling equipment necessary to implement this is any standard AM video modulator with a phase reversed carrier. No special equipment is needed since the required modification is inexpensive.

A fraudulent method of restoring the signal is conceivable in which the television set is modified by reversing the polarity of the AM video detector diodes. This would require some specialized technical knowledge but would be within the capability of any TV repair shop. The complete modification, together with the addition of a switch to restore the set to normal, would probably cost less than $30, labour included.

The advantages of continous video inversion as a scrambling technique are its effectiveness in producing an extremely unintelligible picture and the quality of the restored video. It also has the advantage of not significantly disturbing the spectral energy distribution of the transmission and thus of causing no additional interference in adjacent channels.

The video waveform for a continuously inverted signal is illustrated in Figure 4.

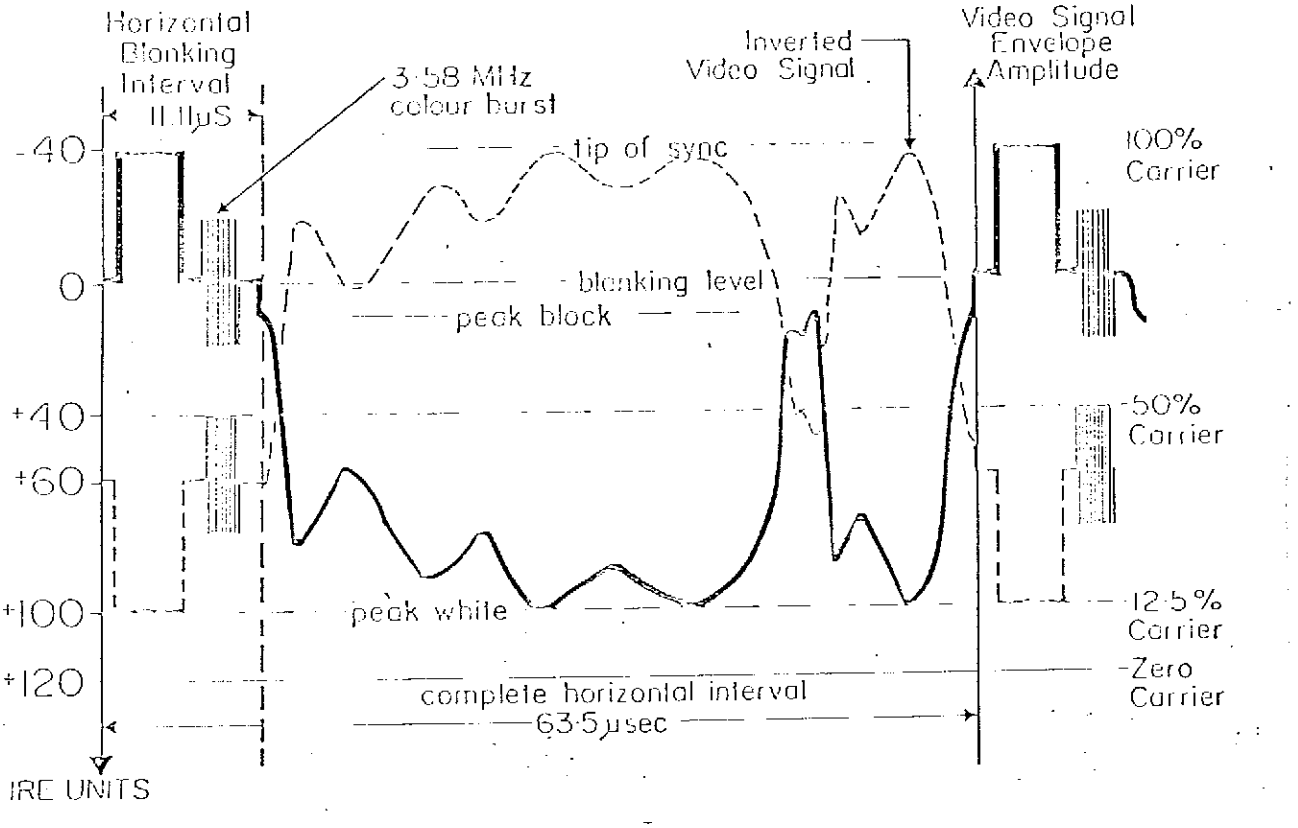
Despite its low cost and other advantages it is not rated high as a candidate system for Public service due to its low security level.

4.16.4 Sine Wave Sync Suppression

Sine wave sync suppression consists of adding to the video signal a synchronized carrier having a frequency of 15.734 KHz. Each negative peak of the carrier's sine waveform is timed to coincide with the presence of the video line synchronization pulse. The addition can be performed at IF or at RF and has the effect of further amplitude modulating the video signal. The result is that the horizontal sync pulse is suppressed and the television receiver attempts to synchronize itself to random peaks of the remaining signal train. Refer to Figure 5.

FIGURE 4

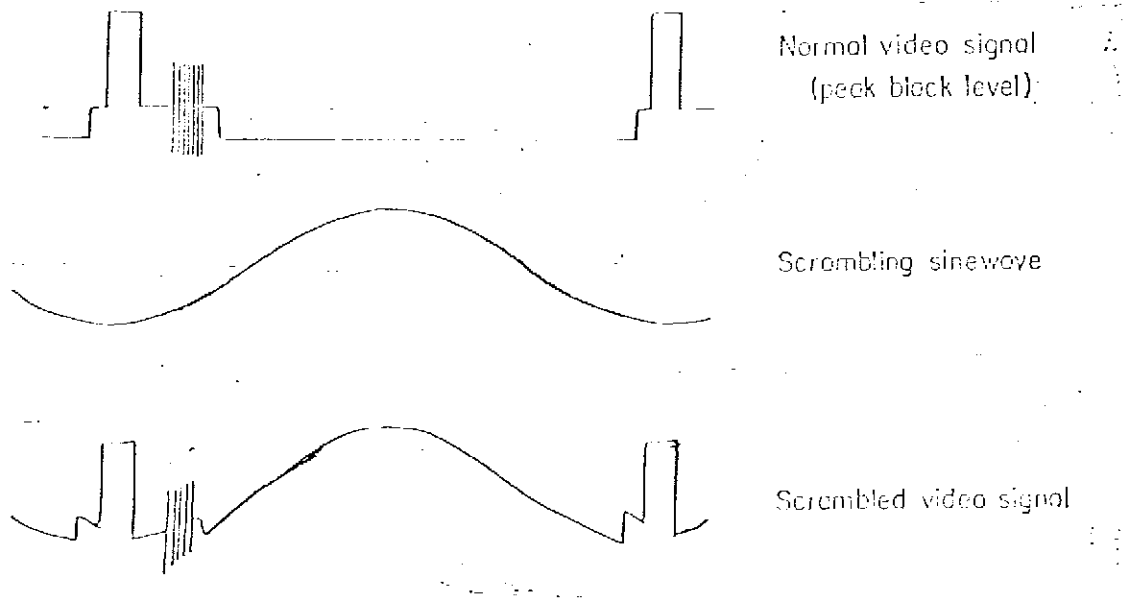
EFFECT OF VIDEO SIGNAL INVERSION ON VIDEO SIGNAL ENVELOPE AMPLITUDE



(derived from information given in CTRI Pay-TV Technology 1981)

FIGURE 5

SINE WAVE SYNC SUPPRESSION SCRAMBLING WAVEFORMS



(derived from information given in CTRI Pay-TV Technology 1981)

Sine-wave sync suppression is a low frequency form of jamming. It differs from that previously mentioned in its need for a precisely phase-controlled means of restoration. A simple filter cannot be used since that would destroy too much of the energy of the sync pulse proper.

A practical means of restoration is to permit the FM audio carrier to suffer similar amplitude modulation at 15.734 KHz and to recover the required sine wave via appropriate amplifier detector and filter circuits.

Oak Industries manufactures a system of this type designed for STV use which could possibly be used on DBS. Its current cost is approximately $160 Canadian.

While giving fairly reasonable security, residual intelligibility is not too high and the degree of restoration is usually slightly below that defined as the norm. For these reasons sine wave sync suppression is not considered to be high on the list of possible candidates for DBS scrambling.

4.16.5 Gated Synchronization Suppression

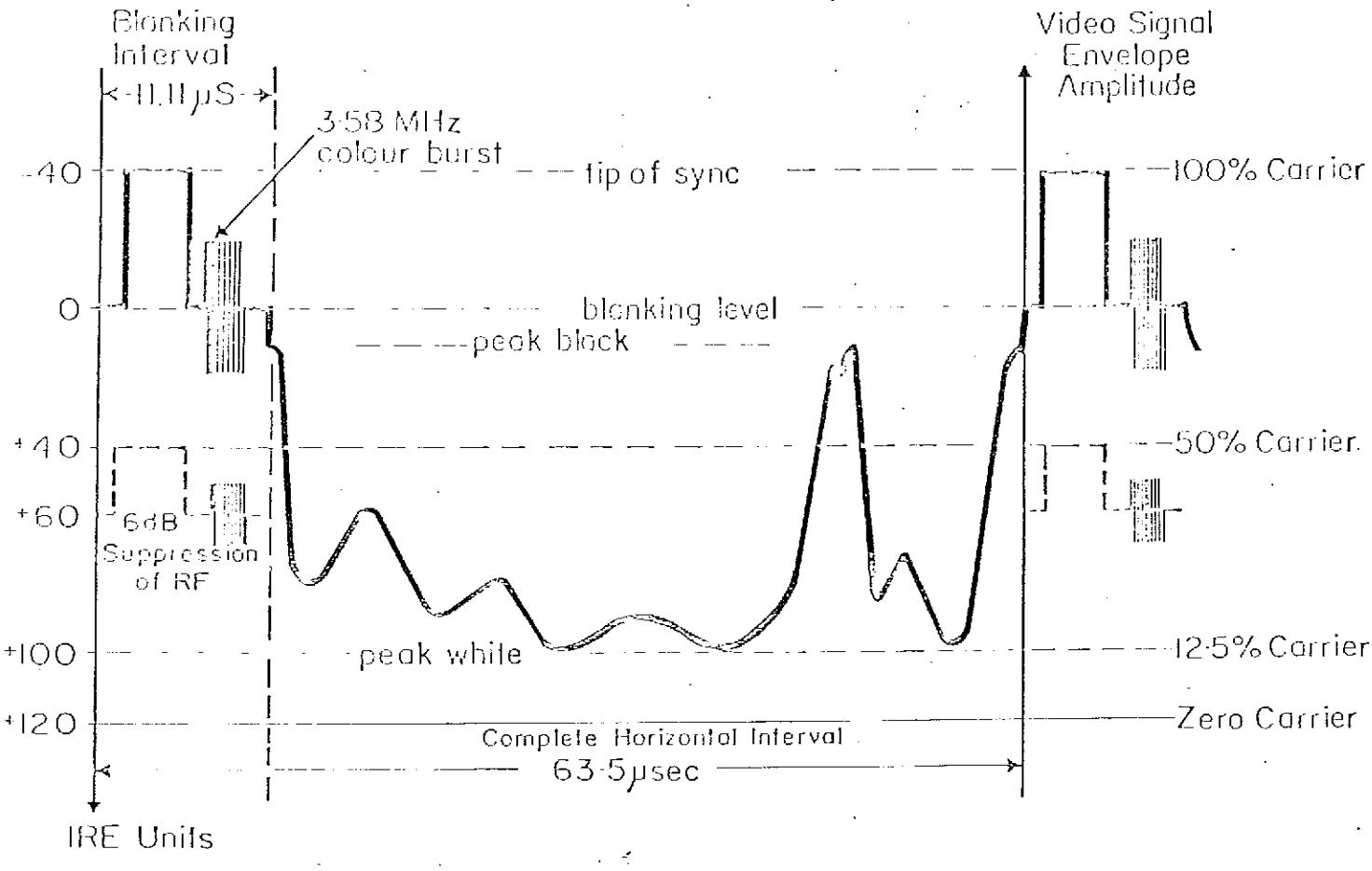
Fast acting digital switches can be made to attenuate or remove completely the video line synchronization pulse while leaving the active video signal undisturbed. This gives rise to a category of scrambling techniques called gated sync suppression.

In one embodiment, an attenuator is switched in series with the modulated video carrier signal during the horizontal blanking interval. To restore the signal, a corresponding attenuator is introduced at RF or at IF by the descrambler during the active portion of the line signal. Alternatively the diminished sync pulse can be restored by switching in an amplifier with a suitably low noise figure.

To appreciate how sync pulse suppression may be achieved by operating on the video RF signal, see Figure 6. The dotted waveform shows the result of a 6 dB attenuation on the video signal's envelope amplitude. The resulting tip of sync is depressed 30 to 35 IRE units below peak black.

FIGURE 6

EFFECT OF SYNC SUPPRESSION ON
VIDEO SIGNAL ENVELOPE AMPLITUDE



(derived from information given in CTRI Pay-TV Technology 1981)

Complete sync pulse removal is also possible. Systems using this technique need to provide both timing signals and a reference level for proper restoration of the sync pulse. Sync pulse removal is presently confined to STV systems and is achieved at video baseband. It is combined with colour-burst shifting to yield a suitable level of security.

Gated sync suppression used on its own may occasionally yield an unintentionally intelligible picture should the subject matter contain a strong vertical stripe. In this case the video may spasmodically lock up and yield a fleetingly intelligible picture.

All such systems require a source of timing signals to restore synchronization.

The timing signal can be provided by amplitude modulating the audio carrier with pulses. A one microsecond start pulse is transmitted for each missing sync pulse and the full pulse synthesized digitally within the descrambler. This is the system used by Jerrold Division of General Instruments in their 400 DRX system.

The Jerrold descrambler suppresses the horizontal blanking interval to the -6 dB (quarter power) level. Blonder Tongue suppresses to a level of -8 dB. Dynacom removes the sync pulse completely.

In assessing the relative security of the above systems, the type of television receivers in the viewing area should be taken into account. This is because some sophisticated television receivers can derive sync by means of count-down circuits referenced to the frequency and position of the 3.58 MHz colour bursts. This stems from the fact that the horizontal scanning frequency is exactly 2 divided by 455 times the burst frequency. The absence of colour bursts during the first 9 lines of the vertical blanking interval can be used to establish a vertical sync reference.

This and the comparatively simple circuits required to overcome this form of scrambling precludes its consideration as a prime candidate for DBS scrambling.

4.16.6 Continuous Carrier Suppression

This technique is still under development by Scientific Atlanta. The intent is to suppress the video carrier at the output of the modulator by about 6 dB. The reduced level of carrier remaining is insufficient to operate conventional AM detectors correctly.

The descrambler consists of a sensitive phase locked loop that restores the carrier to its normal level. An advantage claimed by the designers is a significant reduction in power level for the scrambled signal.

The level of security provided is likely to be between easy and hard, with the acceptability of this dependent upon the final production product.

The proposed continuous carrier suppression system could offer an advantage when redistributed over cable systems in that the potential carrier level reduction could be as much as 5 dB. This could yield a corresponding 15 dB reduction in the level of composite beat interference generated by the pay channel carrier. If several channels of pay television were scrambled in this way, it is conceivable that 50 channels could be delivered over relatively unsophisticated distribution amplifiers.

However, insufficient information is available at this time on the effect of the low-level carrier on the satellite transponder performance or on the detailed performance of the equipment for this experimental system to be considered further at this time.

4.16.7 Line Inversion

This scrambling method is similar to video inversion in that the video signal is inverted relative to the normal polarity. However, in line inversion the video signal is inverted only on some lines as determined by a pseudo-random sequence or key. This avoids descrambling by merely inverting the detector polarity in the TV receiver. It is possible to invert only the visual portion of each video line, leaving the synchronization signals, the colour bursts and the vertical retrace interval uninverted. The security of the system may be increased by adding a pseudo-random sync suppression mechanism to the pseudo-random video line inversion. Line inversion systems, both those driven by simple fixed or pseudo-random sequences, with or without added sync suppression, are well within the state of the art of television electronics, and are amenable to integration. The reliability, robustness, and size is certainly comparable to consumer electronics products. Line inversion provides a hard level of security and is reasonably effective in scrambling the video portion of the television program; it does not address the audio problem. The signal may be restored without visible degradation. The transmitted signal once again looks very much like a standard television signal and is

compatible with normal television bandwidths and standards and regulations. A signal scrambled in this way would not interfere with other signals.

Pseudo-random line inversion scrambling techniques are suitable for multichannel Pay TV because a different scrambling pattern can be used for each channel. However, since the scrambling is on a per-channel basis, i.e. it is the base band video signal that is scrambled, it is not directly applicable to tiered systems. Presumably, in a tiered system one would want a scrambling technique in which one class of customers might be able to descramble a number of channels or all of the programs in a given channel whereas another class of subscribers might only be able to extract one channel from a number of channels or one program from a series of programs. Pseudo-random line inversion systems are available from several companies - see Figure 7. It should be noted that some of these systems, commonly used on STV, are very susceptible to intelligent descrambling because the descrambling key is transmitted either as a data signal in the vertical retrace interval or as AM modulation on the FM sound signal. This system should however be considered to be one of the key candidates for the most viable technical system.

4.16.8 Line Swapping

Line swapping refers to a technique of digital frame store and scramble in which the baseband video signal is sampled, digitized and stored and the samples representing the various lines are read out of the frame store in a pseudo-random order. The storage is digital but when the digital values of the samples are read from the store they are converted to an analog value with a digital-to-analog converter. A composite television signal is thus transmitted. Decoders for line swapping scrambling are available in small quantities for approximately $4,000. Previous comments about the mass market implementation of these systems are applicable here: one would expect the sort of reliability, robustness, and size associated with normal consumer electronics implemented with integrated circuits. This system affords excellent hard security and is reasonably effective in the scrambling of the video signal. The degree of restoration can be excellent with this technique, depending mainly on the sampling rate and the fineness of the quantization of the original digitization. The transmitted signal is a composite television signal and hence occupies normal television

bandwidth, does not interfere with other signals, and conforms to current standards of policy. This system which is being developed by Microtime is currently in the preproduction stage. The encoders and decoders utilized for this technique contain digital memories of sufficient capacity for shuffled, encrypted systems. The fact that the order of the samples in any one scan line is not altered means that precise synchronization between the sampling instants at the transmitter and at the receiver is not required. That one fact may be the key difference between the technical feasibility of an all digital encrypted signal system and the digitally processed analog systems such as line dicing and line swapping.

Again current price and development stage precludes the consideration of this system for immediate use, but this could well become a key system for future use.

4.16.9 Line Dicing

This is a technique in which the video signal is sampled at a high rate, samples are digitized and stored in a one-line memory. While the signal from one scan line is being sampled, digitized and stored, the samples from the previous line are being read out of the memory, in succession, but starting at a random point. The samples are fed to a digital-to-analog converter to reform a video signal which is combined with a composite sync and transmitted. The point at which signals are read out from the line buffer is varied pseudo-randomly according to a prearranged sequence, i.e. key. In this case the samples are not encrypted, the scrambling occurs because, effectively, each scan line appears to start at a random point on the image. Systems based on this technique have been built; the decoders are extremely expensive ($32,000 in small quantities). The system provides hard security, provided that the key is not transmitted in a simplistic way along with the scrambled signal. The audio signal is digitized and the pulses transmitted in psuedo random order via a common video/audio random number generator. The signal may be restored with excellent results, the only source of error being the slight offsets in time at which the

restored horizontal lines start, caused by errors in sychronization of the receiver sampling and the transmitter sampling. The transmitted signal is in essence a standard television signal and therefore occupies normal television bandwidth, does not interfere with other signals and conforms to regulations and policy.

A Westinghouse system of this type is just about to go into production as a satellite distribution system scrambler to cable TV head ends. It is most effective but the descrambler is currently priced in the order of $20,000 U.S. This of course completely eliminates it from consideration as a DBS scrambler in its present form. From a technical view point there is no major reason why an inexpensive system should not be developed using LSI techniques combined with high production. For this reason it should be borne in mind for the future.

4.16.10 Audio Encryption

This scrambling method refers to situations in which the audio signal is scrambled or encrypted. There is a school of thought that states that in Pay TV movies and perhaps other applications, the audio component is an essential ingredient of the service, and that scrambling of that portion of the transmission is sufficient to limit residual intelligibility to the defined norm. There are any number of ways in which the audio signal may be scrambled or encrypted, many of which are very appropriate because of the relatively narrow bandwidth of audio signals. As the bandwidth of the signal is reduced, or as the signal is compressed through vocoding techniques, the encryption technique becomes more and more feasible, at the expense of fidelity. The audio signal may be digitized and transmitted as a digital signal during the sync period ('sound in sync') or it may be digitized and encrypted and then transmitted instead of the regular audio carrier, or it may be transmitted on a subcarrier placed in portion of the spectrum where the video energy is usually low. Audio encryption techniques are becoming available, and one could consider a decoder costing $100 in very large quantities. Again the device would be as reliable, robust and as small as other integrated circuit devices.

The quality of the sound restoration depends once again on the sampling rate and quantization fineness with which the original analog signal is represented. There is no reason to assume that the encryption and decryption process, nor the digital transmission, would add any further error.

The bandwidth required by the digital signal is a direct function of the fidelity required. As with all fully digital, encrypted signals the communications reliability of the system depends upon the accuracy with which synchronization between the transmitted and received keys can be established. Therefore, a relatively good received signal is required before encryption techniques can be used.

The consideration of this system as a prime candidate for immediate use poses problems of both availability and acceptability. Much will depend on how the market develops. There is a considerable body of informed opinion that for Pay TV movie channels (but not sports or spectacular channels) this is the ideal system, being inexpensive, providing hard security but having a "barker" channel effect with the clear video encouraging viewers to sign up as subscribers.

4.16.11 The Concept of a "Vector Controlled Scrambler"

The idea, which has not yet appeared on the market, is the same as a cryptographic key which can be changed from time-to-time. The basic idea is that the control vector or key is encrypted, transmitted to the subscriber, and decrypted to yield the necessary control information. If used with the Line Inversion system, the reservation regarding susceptibility to descrambling no longer holds. Shift register taps could be the key.

There are also methods of audio scrambling which, combined with the encrypted control vector, might be more economic than full encryption.

4.16.12 Complete Digital Frame Encryption

This scrambling method refers to a technique whereby the visual portion of the television signal would be digitized and encrypted but in which the NTSC synchronization signals would be preserved and in which the signal would be transmitted in an analog form as

NTSC compatible signal. The sampling rate would be locked to the synchronization signals and the colour burst, samples would be digitized and modified by the addition of a key and then the samples would be restored to analog form in a digital-to-analog convertor. The transmitted wave form would for all intents and purposes look like the transmission of full bandwidth white noise (snow). Such systems do not exist at the present time, but one could conceive of a well equipped experienced digital video house prototyping an encoder and decoder for about $25,000 each. If the system were developed commercially, one would expect the decoder to be as reliable, robust and small as comparable consumer televison equipment, based on integrated circuit technology. This system would provide high quality hard security, but the presence of the synchronization information would provide dedicated, well resourced cryptoanalysts with the information they require to decrypt encoded messages, thus precluding a "secure" categorization. The scrambling effectiveness of the video would be excellent; the audio signal would have to be handled separately. However, the degree of restoration would be very much dependent upon the ability to derive accurate enough synchronization information from the received signal to carry out the precise decryption. In cases of low signal-to-noise ratio or of multi-path propagation, this technique would be susceptible to periods of poor restoration. The transmitted signal would be a standard regular bandwidth television signal and hence would not interfere with other signals and would conform to current standards and regulations. As with any encryption scheme, this technique lends itself to tiering and multichannel applications. Such systems are not now available.

This approach is not considered to be a current prime candidate for immediate future DBS systems, and should not be considered very seriously for future public service DBS, because of the synchronization problems involved.

4.16.13 Complete Digital Bit Stream

This method is that with the highest potential level of security, but is based on the use of digital television transmissions. In it the analog television signal and the analog audio signal are digitized in their entirety and encrypted with a secure digital key. Perfectly feasible in concept, such systems are not yet

commercially available. A prototype decoder could be implemented for approximately $25,000. Commercial versions of the full digital decryption device would be as reliable, robust and small. This encryption technique does however require considerable study and development before it could provide secure levels of security due to the high periodicy and correlation of a TV signal (see section 6). The scrambling effectiveness however would be total for both video and audio: there would be no vestige of intelligible information in the received signal until it was detected, decrypted, and the video and audio signals reconstituted from the decoded bit stream. The encoder could be prototyped for approximately $25,000.

Restoration should be virtually perfect, consistent with the sampling and digitizing scheme used. Standards for the digitization of television signals are currently the subject of international discussions. The transmitted signal would of necessity, be a wide-band, high bit rate digital stream, and therefore could well interfere with other signals unless it were transmitted to an appropriate frequency plan. The unprocessed bandwidth requirement would be many times that of regular TV, digital television requiring over 80 megabits per second. It should be noted perhaps that with appropriate processing digital television could be transmitted through the same satellite transponder bandwidth as is now used for analog television (about 36MHz on ANIK C). There are no current regulations or standards regarding wide-band digital signals on DBS. Encrypted digital television signals are very amenable to tiering and multichannel applications because of the ease with which they may be multiplexed with signals from other sources and the flexibility with which different keys may be used for different signals. Systems of this type are not available. Signals in their digital format would not be amenable to redistribution over standard television distribution systems, nor would the bit rates be compatible with even wide band digital local area networks. It is possible that digitized television might however be a natural distribution mode for fibre optics.

These considerations preclude the selection of this system as a current candidate, but it is recommended for future study.

4.16.14 The Intrinsic Vulnerability of Encrypted Television Signals to Decryption

In sub-section 4.16.13 above, reference was made to some of the problems of ensuring "secure" encryption of television signals. In this sub-section this problem is developed further.

Television signals are highly correlated. They contain synchronization information which is repeated exactly from line to line and frame to frame; they contain information to demodulate the colour information; and the images they represent are invariably correlated horizontally, vertically and in time, i.e. along the line, from line to line and from frame to frame. These periodicities and correlations in the "plaintext" image can provide the cryptoanalyst with virtually all the information needed to break conventional cryptograms.

Television pictures are created by a raster scan of the image. That is, the intensity (luminance) and colour (chrominance) at each point on the image is sensed, in a very specific pattern, and the values transmitted to a receiver where the image is re-created in the same pattern. The pattern consists of lines across the image from left to right moving from top to bottom. The image is scanned from top to bottom twice before the pattern is repeated. Each scan creates a field, the scan lines of the second field fall between the lines of the first field, i.e. they are said to be interlaced. The scanning pattern is repeated periodically. In North American television a frame consists of 525 horizontal scan lines with 30 frames occurring each second.

If the image is considered as a rectangular array of picture elements (pixels), then there might typically be 768 pixels on each of the 480 visible lines, or a total of about 367,000 pixels per frame, that is about 11 million per second.

When television signals are digitized the samples are taken only on the 84% of each scan line that contains picture information - the rest of the line contains information to synchronize the image reconstruction process at the receiver with the scanning at the camera. Likewise, only about 240 of the 262.5 lines in each of the fields contain picture information, the others from the vertical retrace interval.

Because of the size of objects in the image and the relatively slow rate at which the images change, each pixel tends to be similar in intensity and colour, i.e. correlated, to those to which it is adjacent. Because of the scanning pattern, each pixel is "adjacent" to those on preceeding and following scan lines in its own field, and in preceeding and following fields; and to the co-located pixel in preceeding and following frames. The area over which the pixels are correlated is a function of the fine detail in the picture, and the time over interframe correlation is high is a measure of how active the image is, i.e., still pictures are perfectly correlated in time.

In a straightforward encryption scenario, the samples (pixel values) would be digitized, buffered along with framing information and perhaps digitized speech, combined with a digital key and synchronously transmitted. Even though the output stream would be encrypted, the "clearview" information would contain periodically repetitive framing codes, or characters. The detection of these periodicities would point directly to the location of correlated pixels, even if the key were not obtained. Because of the large number of pixels and the fast frame repetition rate, "cipherview" for a large number of identical (or nearly identical) "clearview" pixels may be accumulated rapidly, which should lead any well resourced and dedicated cryptoanalyst to a solution of the key in a reasonably short period of time.

The cryptoanalyst's chore can be increased to some degree by shuffling the pixel values before encryption. This could be done by storing the pixels from one or more frames (depending on the image activity) in the order in which they are generated and transmitting them in a key-controlled, pseudo-random order. Alternatively, the scanning pattern itself might be key-controlled and irregular. The effect on the cryptoanalyst is to require him to analyze more data, which at the rates used in digital television is a major consideration, before the key may be found. Fundamentally, however, the only effect is to complicate the analysis by confusing the periodicities inherent in the normal raster scan. If the length of the shuffling pattern is constrained by realistic memory sizes or equipment cost, it is only a minor impediment to the resourceful cryptoanalyst.

The security of any encryption system is dependent on the security of its keys and, in many cases, on the separation of "plaintext" and "ciphertext". The periodicities of the television raster and spatial and temporal correlations in the image provide the cryptanalyst with a valuable starting place unless, the new cryptographic techniques, in which simultaneous possession of 'plaintext' and 'ciphertext' are of no value in breaking the code, are used.

Although a literature search of unclassified material was carried out, no reference has been found to the particular problem of providing secure encryption of a television channel. Although such a level of encryption is of little interest to commercial users of a DBS, it is envisaged as being of very considerable interest to military users. As such, a preliminary investigation of the problem of high level security of fully encrypted television signals is recommended for further study.

4.16.15 Conclusions

From the work described above it is now possible to draw some preliminary conclusions regarding the most likely candidate systems for DBS scrambling.

It should emphasized at this stage that this selection is a preliminary one as, as this work progressed it became obvious that a number of non-technical factors would be significant in the final selection. One example of this is the acceptability or not of audio scrambling only for movie channel Pay TV public service.

Another factor precluding definitive selection at this time is that of the very volatile nature of current technology, and the understandable reluctance of companies with scrambling systems under development to give full information.

Perhaps one of the major conclusions drawn so far is that it is quite possible that the optimum current solution for DBS scrambling of Pay TV movies will be hard encryption of the audio carrier only.

Line manipulation, which includes line inversion, line swapping and line dicing is the most likely candidate for hard security scrambling systems for all types of Pay TV and for video private services. During the four

months that work has been carried out on this contract, two major manufacturers, Zenith and Oak, have marketed low cost line manipulation scrambling systems suitable for DBS use. The general feeling in the industry is that there are other manufacturers also working on advanced scrambling systems for this market using one or more of the concepts identified in this Section.

For the future, both for high security, public and private services and for secure private services, complete digital frame encryption and complete digital bit stream encryption are likely candidates. With regard to both of these future systems, additional study is required to ascertain the problems, and possible solutions, of secure type encryption.
Finally for low bandwidth private services such as low speed data and audio services, "piggy-backing" in a transponder also used for video services, the simple use of an nonstandard frequency, could well meet these unique security requirements. If additional security was required the "audio only" encryption concept would be very cost effective.

5. NOTES ON SYNCHRONIZATION IN THE DELIVERY OF SCRAMBLED SERVICES VIA DBS

Synchronization is a vital necessity in a communications system in which the information is encoded in any way at all. This is true of the image in normal television, where the electron beam in the receiver must be moved across the face of the display in perfect synchronization with the raster-scanned image in the originating camera. More than the requirement to merely synchronize the camera and display raster scans (which occur at relatively low frequencies), colour television depends on precise synchronization of a local oscillator at the receiver to decode the phase-modulated colour signals. When the received signals are distorted or corrupted by noise, the receiver loses synchronization and the picture 'rolls' and/or the display colours are not true.

In the case of scrambled television signals, which are deliberately manipulated, usually by a sequence of operations, it is evident that another layer of reliable synchronization is required. In addition, if the manipulation is carried out upon digitized signals the precision with which synchronization must be established is increased, and the reliability of successful performance decreased.

If it is assumed that a scrambled television signal contains scrambled video, encrypted digital audio, encrypted addressing/authorization data, decryption keys, and descrambling information, communications synchronization is required at several levels. For example, the following levels of synchronization are required:

For the video: descrambling sequence synchronization digital sampling clock;

For the data: data carrier synchronization (if appropriate), bit timing, decryption sequence synchronization, key synchronization, and word (frame) synchronization;

For the audio: carrier synchronization, bit timing, decryption sequence synchronizations, key synchronization (D/A synchronization).

Reliable performance will be enhanced by the number of these operations which are handled by passive, serial devices; or for which timing information is explicitly transmitted. The more complex the encoding scheme, and the higher the reliance on timing recovered from the received signal (or from the TV synchronization), the less robust the overall system will be. The functions of these synchronization operations are as follows:

Key synchronization - assures that the correct key is being used.

decryption key synchronization - assures that the decryption sequence is in synchronization with the encryption sequence - unnecessary if passive serial devices are used, e.g. feedback - shift registers.

word framing - necessary to establish word boundaries in the synchronous data stream, to extract meaningful information.

bit timing - to sample the demodulator output at the correct time to maximize probability of correct reception.

carrier - for coherent demodulation of data signals, if required.

digital sampling clock - to sample scrambled video signal to reorder (and/or decrypt) digital processing - e.g. as in line dicing or scrambling.

6. SYSTEM CONSIDERATIONS AND CONCLUSIONS

This section is concerned with those aspects of the delivery of scrambled television signals that arise when the components that make up a system are brought together.

The components of interest are:

- television signal origination
- satellite up-link
- operational control centre communication links
- scrambling, descrambling
- subscriber-site control units

There are, of course, a very large number of system scenarios that could considered given the range of possibilities for:

- the level of security
- the scrambling methods used
- the number of television channels
- the satellite configuration
- the communication links between origination points, control centre, and subscribers
- the procedures for operational control and system management
- the reliability required
- the number of unauthorised users that could be tolerated
- the time constant of the authorization process
- etc., etc.

It is necessary to make some assumptions about the system to focus the presentation that follows, but first some general concepts will be discussed.

As the unauthorized reception of television signals broadcast from satellites using straightforward

modulation techniques is a relatively simple exercise for virtually any handyman or local entrepreneur, it will be assumed that all television signals will be scrambled in some way before transmission. The degree of security provided, will be a function of many parameters, most them economic, but the question of encryption and the ultimate level of cryptographic security afforded by any of the scrambling techniques will arise. That being the case, it is necessary to consider the question in the DBS context.

Conventional cryptography assumes that both the transmitter and receiver desire secrecy. In DBS applications it may be assumed that this motive is held initially only by the transmitter. It will also be assumed that one-way electronic communication only is available, with no feedback.

It shall be assumed, however, that if needed, encapsulated electronics are available whose function and internal workings would be destroyed by efforts to determine the circuit configurations therein. It is assumed that these devices could also be shielded to prevent electromagnetic probing.

Another basic concept is that direct digital encryption of the television signal will not be economically feasible for some time. Nevertheless, cryptographic methods could be used to distribute key parameters on an hourly, daily, or program basis to enable unscrambling for the given time period. On the other hand, highly secure analog scramblers may not be possible, but may not be needed in this application.

The security normally acceptable in the DBS case is not as high as in commercial or governmental cryptography. The aim is to make it very inconvenient in a time and/or ecomnomic sense to unscramble the signal in an unauthorized, unaccountable fashion. Each receiving station is taken to have a control unit through which the subscriber selects the programs to be viewed. The same device could record this data to be retrieved later for billing purposes. An ability to over-ride the recording functions or to duplicate the control would threaten the security of the system. On the other hand, if this were possible only at great cost, effort or time expenditure so that only a very few violations would occur, the level of security would presumably be acceptable. Cable television systems operate now with a certain number of potential subcriber locations illegally connected or using unpaid-for additional TV connections, and have determined the tolerable level of this theft of service balanced against the cost and negative impact of eradicating it.

Scrambling in the "unrecognizable signal" sense may not be necessary either. Degrading the picture and/or the audio signal quality could be a sufficient objective. Scrambling parameters could change on a line, field, or frame basis, according to the current key or following an encrypted message sent with the television signal.

The science of cryptography has recently made great strides. Two basic concepts are 'unconditional' and 'computational' security. Since the first is not particularly relevant to the DBS situation, nor practical, attention shall be given to computational security. This approach is based on the futility of random or systematic searches for the true message caused by computational requirements and because all plaintext messages of the length of the intercepted message would also be decoded to no advantage of the interceptor. This assumes clearly that the interceptor knows the basic encryption system being used, but not the key. Such an assumption is relevant to the DBS problem as it would not be feasible to guard the scrambling system as though it were a government secret. Too many people would know the details of all or part of the system.

The protection afforded by having the true message hidden in all plaintext messages of the same length is not operational in the television case. Unfortunately, the validity of the proper descrambler will be immediately evident in the quality of the descrambled video and sound. It would appear, then, that the economic and time factors associated with routinely trying all possible cases is the limit of the protection yielded by modern cryptographic science. Presumably this can be made to suffice by proper choice of the "rekeying" frequency.

Protection of the key is the heart of all cryptography. The basic configuration is shown in Figure 8.

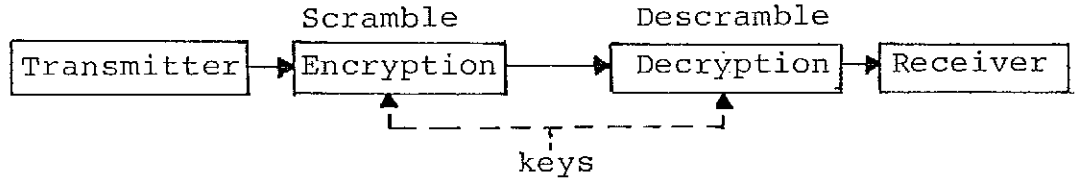


Figure 8. Basic Cryptographic System

Such a system is useless as a method of guaranteeing that only key holders can descramble the signal if many holders of the key (assuming a one-transmitter, multiple receiver situation) are not dedicated to its security.

An alternative is shown in Figure 9, where the key is

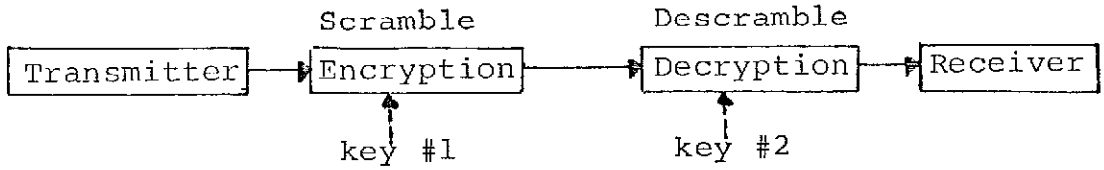


Figure 9. Split Key System

split into two parts. It is even possible in this scheme to have key #1 a matter of public knowledge so that anyone desiring secure communications with the receiver can encode his message via key #1. Key #2, known only to the receiver, is used to decode the message and an eavesdropper is still not able to do that even though he knows key #1. This is, however, the reverse of the situation with a DBS. If key #2 is compromised there is no further security and minimal receiver security is to be expected. Unfortunately, the situation where key #2 is known, and key #1 is secret, is of no practical significance as a split key system because key #2 serves no purpose.

Another cryptographic technique with possible application with DBS is the one-way function 'f' which is computationally easy to compute but whose inverse 'f' is not computationally feasible, ie. it is impossible to compute with any known machine using any known algorithm in any finite length of time. Its conventional use is to improve the security of timeshared computer password files. Applications of one-way functions to DBS scrambled television broadcast are described in the Appendix E.

6.1 Development of the System, and Assumptions Made

In subsequent discussions of the system it shall be assumed that the television transmission (which includes

video and audio components) is scrambled, for example, in the following manner:

The audio component is scrambled either by analog or digital means. Analog scrambling may be achieved by spectral inversion, corruption by multiplicative or additive interfering signals, or by complex but invertible filtering. The audio signal may be digitally scrambled by sampling it at a high enough rate, quantizing with sufficient resolution, and encrypting the resulting bit stream by an appropriate method. For high fidelity sound, over 500,000 bits per second (e.g., sampling at 44 kHz, and quantizing to 12 bits) may have to be transmitted; no mean feat to include along with the video information in the standard television bandwidth.

The video signal (luminance and chrominance, or just luminance alone) may be scrambled to a level satisfactory for almost all commercial DBS applications by a combination of pseudo-randomly controlled line manipulation techniques. These techniques may include sync suppression, video inversion and line dicing, although a combination of the first two is probably sufficient for all practical purposes.

Thus both audio and video may be scrambled; and the scrambling controlled by pseudo-random sequences. These sequences must, of course, be known to the receiver, which must be able to produce replicas of them synchronized to those on the received signal. The descrambling sequence can either be generated at the receiver or transmitted with the scrambled television signal. In the first case, synchronization information must be transmitted or derived from the received signal. The second case is simpler, and can be effected securely if an encrypted version of the descrambling sequence is transmitted, for example, as amplitude modulation on the FM audio signal.

It seems reasonable to assume that the descrambling will be controlled by something like a maximal length shift register sequence, which in turn is determined by the setting of a limited

number of taps on a feedback shift register. The tap settings are the key to the descrambling sequence, and must be changed often enough to make finding their values by exhaustive search of no consequence; the implicit assumption being that a simulation of the descrambler, with accessible taps, is available to the eavesdropper. The key can be changed by transmitting an encrypted version of the new one in the old code.

A basic DBS system for the broadcast of scrambled television signals shall be assumed to consist of:

- an operating centre;
- one or more up-link transmitters;
- one or more remote up-link transmitters;
- a DBS;
- communication links
- one or more subcribers.

It is assumed that the operating centre has access to an up-link transmitter whose signal can be received by all subscribers and all other up-link transmitters.

It is assumed that the only communications between the control centre and the subscribers is via the satellite transmission, and there are no terrestrial links either from the control centre to the subscriber or vice-versa. It should be noted however that this assumption may be overly severe. A metering scheme for Service Subscription System is described in the Appendix F. Since this scheme has widespread implications for all types of utility remote metering, it is not discussed in the DBS context at this time.

It is also assumed, for the sake of argument, that the addresses of all subscribers in good standing are continually transmitted on the control channel to maintain their descramblers in an operational state. The descrambler would be designed to stop providing clear television signals to the subscriber when not addressed. The authorization for the program and tier for each subscriber would also be transmitted regularly. It should be noted that there are methods of authorization which do not rely on the broadcast of control information through the satellite. The obvious example is where the subscribers access is controlled by direct terrestrial links via the switched telephone network or the public data networks. As the number of locations

with two-way data communications grows, it will be reasonable to re-examine the assumption that direct control is not feasible, but at the present time it appears to be out of the question. There are other channels such as the postal system, over which control can be exercised, that are not electronic. Before the postal system is dismissed, the amount of billing information and funds transfer that it now carries should be considered.

It is assumed that there is a control unit at each authorized subscriber location. This unit would be an individual, personalized and sealed unit. Its primary functions would be:

- to check its address against the authorized list as that is broadcast
- to turn itself off if not authorized
- to decode the keys as they are broadcast
- to descramble the television signals on authorized channels

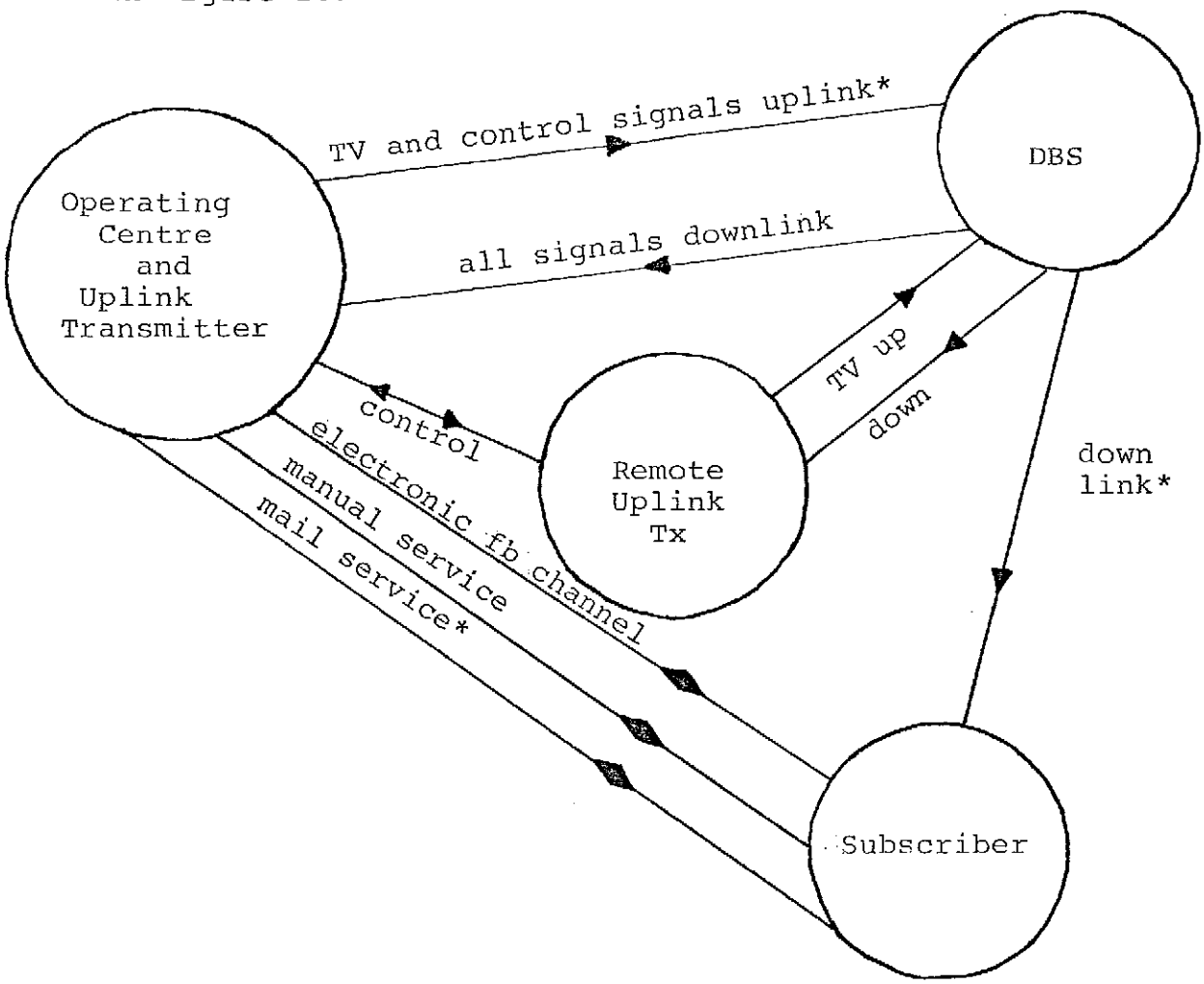
It would have additional functions if a metered system, such as that described in Appendix F were in use. Two elements of security are essential in regard to the subscriber asccess control unit. It cannot be bypassed and it cannot be fooled by the local injection of proper address and authorization data. The first requirement implies that the television signal is indeed scrambled; the second that the key is changed regularly, and the data is encrypted.

The communication channels are assumed to be composed of both essential and non-essential links. The essential link is between the operating centre and the subscribers via the DBS (an uplink and a downlink). The non-essential but useful other links are:

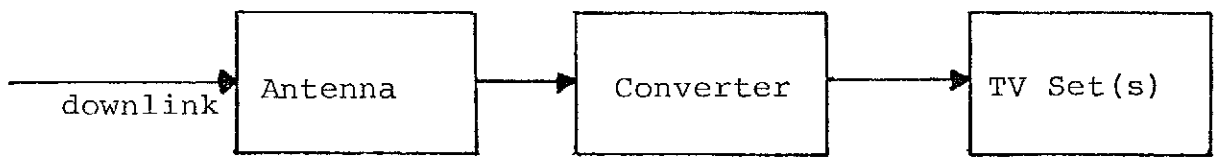
- From the control centre to the subscriber, eg.
  - electronic feedback channel
  - mail service
  - manual service
- From the control centre to the remote uplinks and return
- From the remote uplinks to the DBS and return
- From the DBS to the control centre on all beams and channels

6.2 The Basic System

It is now possible to postulate a basic system as shown in Figure 10.



Subscriber system



*Essential channels: TV and control signals uplink;
subscriber downlink;
mail service

Figure 10. Basic System Configuration

The following assumptions are made about the system in Figure 10:

- downlinks to the uplink transmitters may be missing with some satellite antenna configurations
- electronic feedback channels from the subscriber to the operating centre could be used to request selections (which would require unique addressing of the subscriber control units via DBS) or to monitor subscriber selections (which would not require unique addressing). This link is not essential.
- 'Manual Service' relates to meter reading, installation and repair by a serviceman and is very undesirable (or impossible) for remote subscribers.
- Mail Service (or equivalent) is required for billing and payment, and for the "Service Subscription Service" described in Appendix F.
- The control link to "a remote uplink transmitter" must provide precise timing and synchronization for some types of analog scrambling. It would be better if such a control link can be very "loose". This could be of the "mail service" type, giving the same information as is given to the subscribers converter, if self-synchronous encryption were used.
- TV downlinks to the uplink transmitters are useful but not necessary.
- No scrambling takes place in the satellite.
- There is no central control of the synchronization of scrambling, and no centralized scrambling.
- A basic system philosophy decision required is whether or not subscribers will select their own services/programs and be monitored, or make a request through the operating centre. If the latter, electronic communications are needed from the subscriber to the operating centre, and unique (addressed) control signals from the centre, through the satellite to the

subscriber. The former requires either monitoring through the telphone system or use of a local metering system, as described in the Appendix F. If meters can be used, the "select and monitor" approach is much simpler.

The important concepts inherent in this system are:

a) the scrambling/encryption is originated at up-link transmitters using the local TV signal for 'bit' synchronization.
b) hour, day, and week timing is added to the primary (control centre) television signal to time the switching to the particular key being used in each time period.
c) self-synchronizing encryption/decryption should be used.
d) the video is not encrypted, the audio may be; the key for descrambling the video and decrypting the audio must be encrypted.
e) the keys are changed from time to time.

6.3 Conclusions

The actual system used in any particular circumstance will depend upon the decisions made by the system licencee, but based upon the many system considerations developed above it is expected that any system will be required to meet the basic system configuration with its various options developed in sub-section 6.2 above.

7. DISCUSSION OF EXTERNAL POLICY, SYSTEM AND ECONOMIC FACTORS

In considering the format and contents of this Report, it became apparent that great care was required to define the specific task in hand and to keep within the limits of that task.

It was necessary for the authors to continually bear in mind that this report relates only to the consequences and issues of scrambled TV services offered by a DBS. In carrying out this work, particularly in carrying out interviews, it was found that there was great temptation to stray from this specific task and to consider wider economic, marketing and penetration issues of the DBS

service as a whole. The reason for this is obvious, scrambling can only take place once the service is in existence, and there are currently many unresolved issues regarding DBS service as a whole. These vary from the type of DBS system to be used, through the likely users for the system as a whole, only some of which will require scrambling, and a whole range of other factors including type of scrambling and the tariff structure for uplinks and satellite transponders. All of these unresolved factors can have an effect on the economic viability of scrambled services.

To carry out the specific requirements of this contract, while maximizing the probability of this report yielding useful results, a number of these policy, system and economic factors that will indirectly impact upon the effectiveness of scrambled services are considered below. In addition a number of basic assumptions regarding many of the related matters referred to above had to be made to yield a manageable framework within which the economic considerations for DBS scrambling discussed in Section 8 could be examined.

7.1 DBS System

The study as a whole has revealed that it is generally considered that Canada currently has a choice of two approaches to a DBS system. In 1983 the International Telecommunications Union (ITU) will hold a Region 2 (North and South America) Regional Administrative Radio Conference (RARC 83), to arrive at an international agreement for the parameters to be used for direct broadcasting satellite in the Americas. These parameters include, among others, the effective isotopic radiated power (ERIP) and the frequencies to be used. Both of these parameters obviously have a key effect on the cost of the ground stations to be used. The current thinking on the outcome of WARC 83 on these two key parameters is for a main service area EIRP of 60 dBW in the frequency range 12.2 to 12.7 GHz.

Therefore one approach for DBS service for Canada is to await the outcome of RARC 83, and to build and use a DBS meeting the parameters decided upon there.

Very briefly the advantages are likely to be the use of smaller antennas for direct-to-home service, and compatibility with U.S. direct broadcast satellites. The disadvantages are likely to be a delay of several years in the provision of a DBS service and, as will be seen below, some impact on the financial viability of Telesat's Anik C services.

The second alternative is to use one or more of Telesat's Anik C satellites to provide an interim direct broadcast satellite service.

Receive-only satellite earth stations (ROSES) for the Anik C system operate in the 11.7 to 12.2 KHz band. There are a number of possible configurations for Anik C which will provide different coverage (13) but it is considered that the most likely configuration for Anik C interim DBS use will be to use quarter Canada beams with 0.25 degree tilt and two TV channels per RF channel. (See figures 11A to 11D) The main service area EIRP in this configuration would be 48 dBW.

Again, very briefly, the advantages of an Anik C interim DBS are that service could be provided probably in late 1982, and that the various users of this interim DBS would rapidly provide satellite loading to an economic level.

The disadvantages are that the ground stations would be on a different (but adjacent) frequency and would require antennas of a larger diameter than those expected to be used as a result of RARC 83 (for main service areas approximately 1.8 meters against 60-100 cm).

With continuing pressures for Pay TV and other DBS services, combined with Canada's investment in Anik C, the assumption is made for the purposes of this task that an Anik C interim DBS service will be approved.

7.2 CRTC's Position Regarding DBS

As the regulatory body for broadcast licensing, the thinking of the CRTC is crucial to the consideration of economic considerations for scrambling of DBS services.

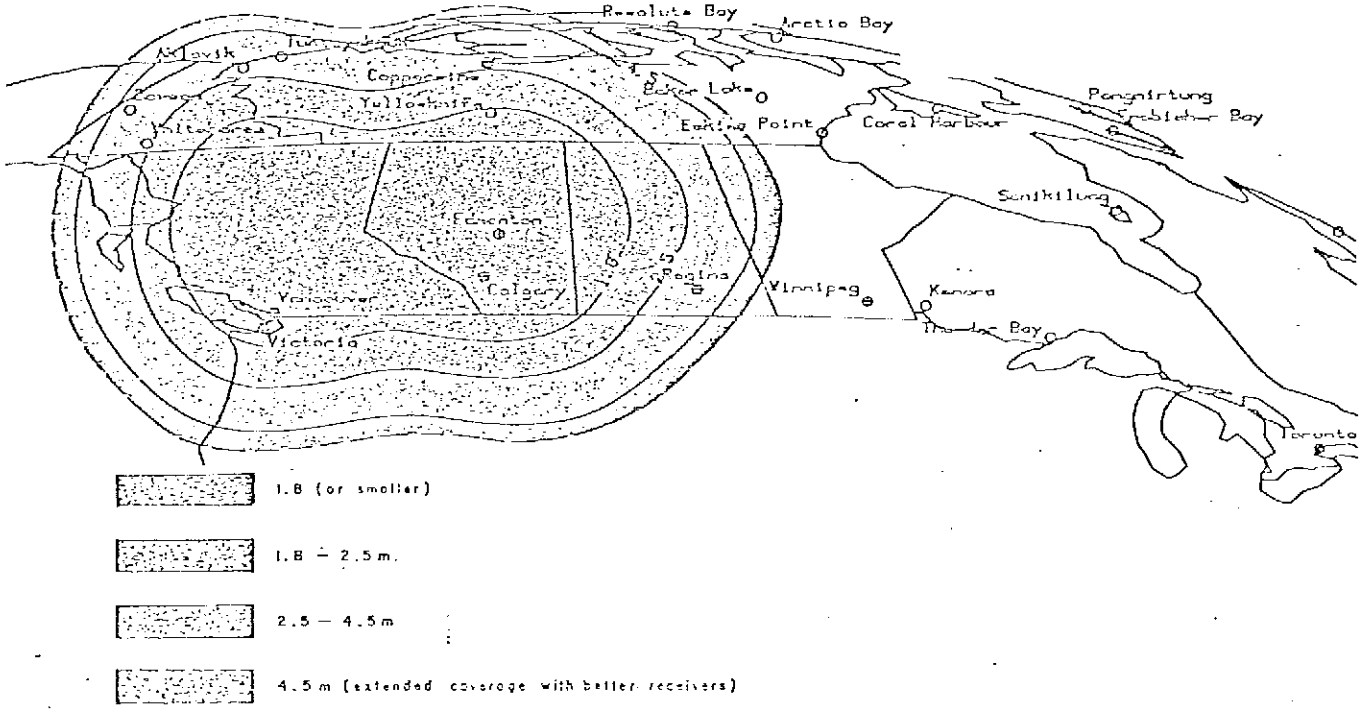
In interviews with CRTC staff members carried out as part of this study, it is clear that current CRTC thinking is that any and all users of any Canadian DBS system will come under CRTC jurisdiction and regulation. (d)

During the period the period that this study was being carried out (November 1981/February 1982) the CRTC has awarded many licences for the terrestrial distribution of the CanCom satellite network package. In awarding

FIGURE 11A

ANIK C COVERAGE - WEST QUARTER CANADA BEAM - 0.25° TILT

2 TV PER RF CHANNEL

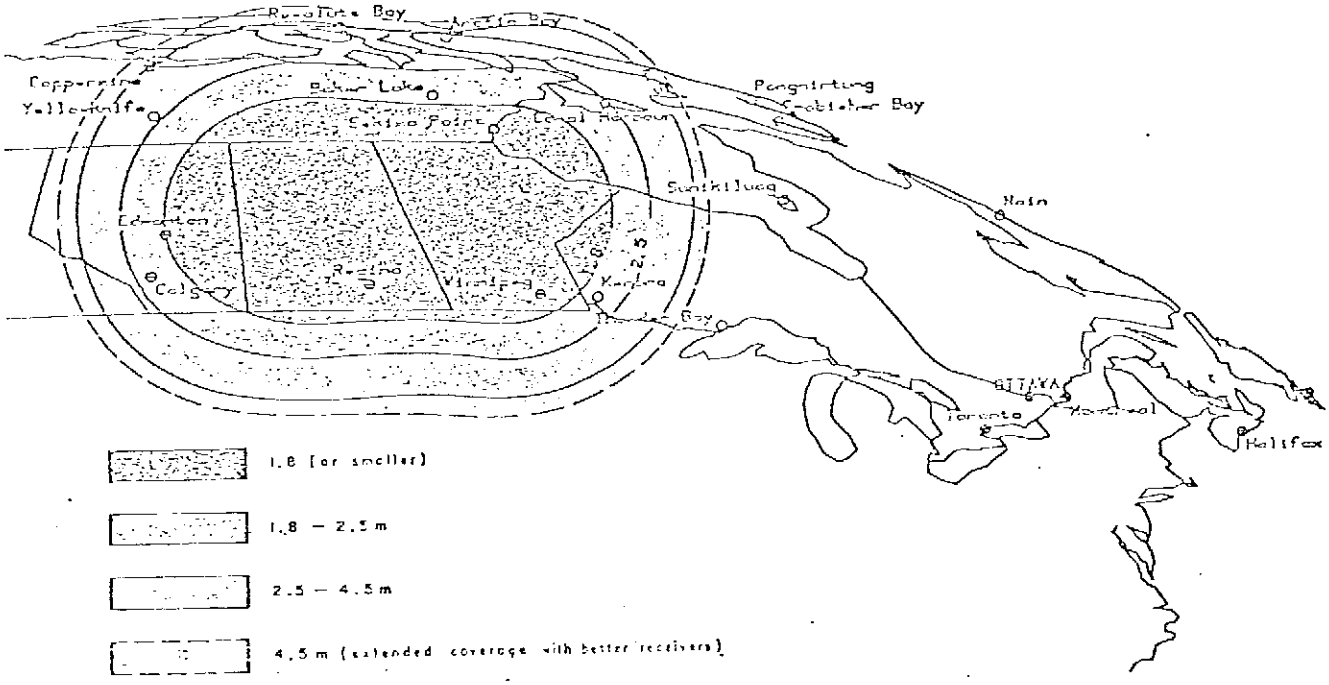


(derived from information given in Telesat Canada's Study of the Use of Anik C for Direct-to-Home and Community Television Distribution Services, September 1981)

FIGURE 11B

ANIK C COVERAGE - WEST CENTER QUARTER CANADA BEAM - 0.25° TILT

2 TV PER RF CHANNEL

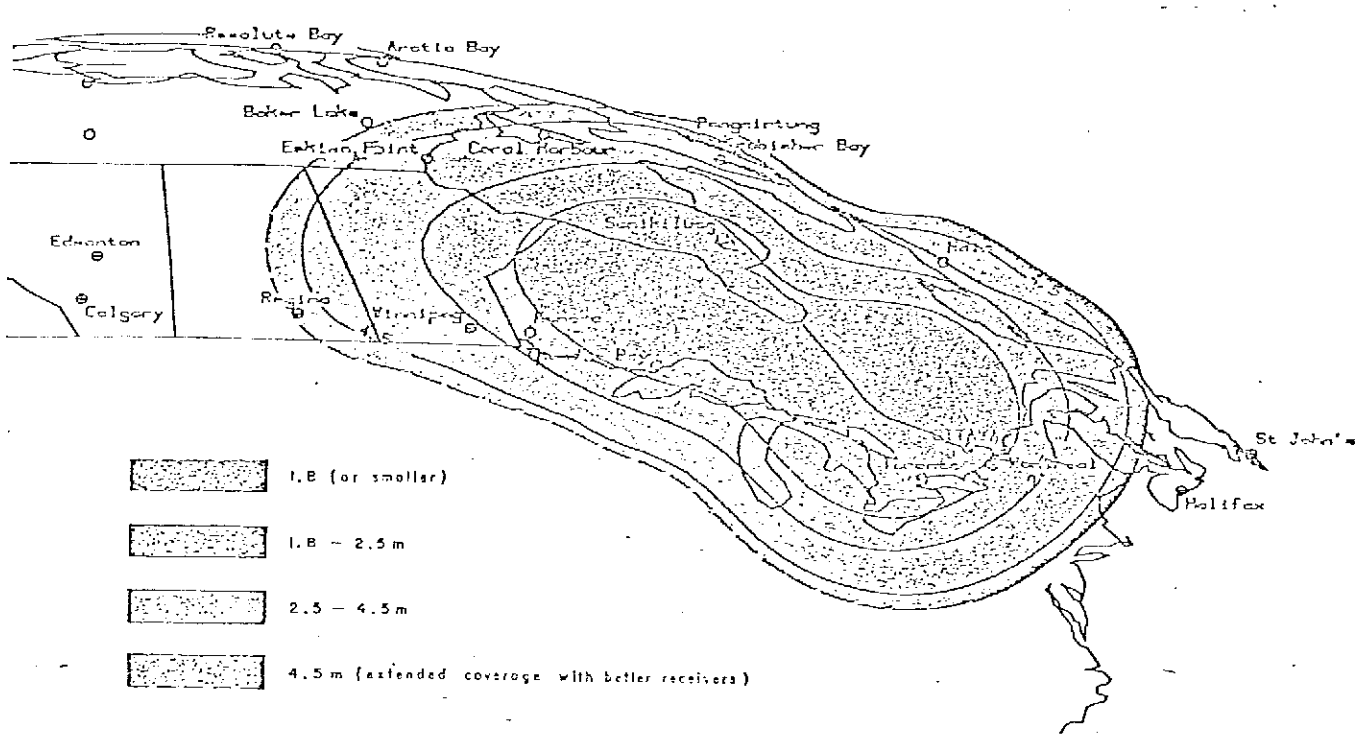


(derived from information given in Telesat Canada's Study of the Use of Anik C for Direct-to-Home and Community Television Distribution Services, September 1981)

FIGURE 11C

ANIK C COVERAGE - EAST CENTER QUARTER CANADA BEAM - 0.25° TILT

2 TV PER RF CHANNEL

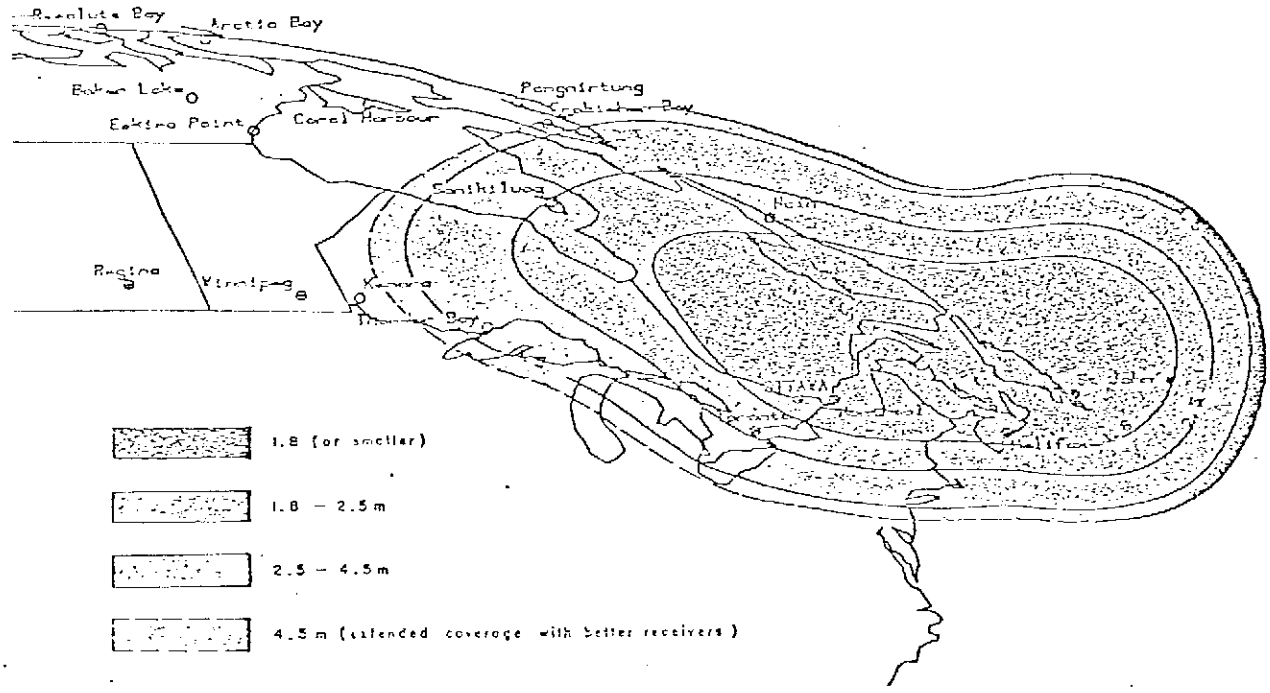


(derived from information given in Telesat Canada's Study of the Use of Anik C for Direct-to-Home and Community Television Distribution Services, September 1981)

FIGURE 11D

ANIK C COVERAGE - EAST QUARTER CANADA BEAM - 0.25° TILT

2 TV PER RF CHANNEL



(derived from information given in Telesat Canada's Study of the Use of Anik C for Direct-to-Home and Community Television Distribution Services, September 1981)

these licences, the CRTC decided that those re-broadcast operations providing an encoded signal to be decoded by leased equipment at the subscriber premises had "all the essential charcteristics of cable television systems in that they will provide a local distribution service exclusively to subscribers for a monthly fee" and would therefore be licenced as "broadcast receiving undertakings" in the same way as cable television systems, rather than as "broadcasting transmitting undertakings" like normal re-broadcast operations. It is thought in some quarters that the Commission's reasoning for this is to avoid the legal challenge on whether or not an encoded broadcast signal is indeed broadcasting. (39)

Assuming that the CRTC permits the use of Anik C as an interim DBS, for the purposes of this report the following assumptions are made regarding policy positions taken by CRTC:

- that scrambling of signals carried by a direct broadcast satellite will be permitted;

- that licences for Pay TV will be issued and that licencees will be permitted to use DBS for the distribution of their services;

- that the CRTC will permit other potential users of DBS such as private broadcasters and the CBC, private user groups such as educational and medical users, to be licenced. The corollary of this assumption is that the Anik C interim DBS service will attract viable loading and will be continued;

- that the CRTC will approve a tariff, similar in format to Telesat's tariff CRTC 8001, at a full period service rate and transmit rates no greater than the lowest significant amounts given by Telesat's "straw man tariff" (1);

- that licences for pay television services would permit distribution to all possible subscribers in the licenced area, including urban, rural and remote subscribers either by direct-to-home DBS transmission or by additional terrestrial distribution systems such as cable TV and re-broadcast systems;

- a final and perhaps critical assumption is that the CRTC will issue licences for all potential Canadian DBS users early enough for the system to be fully established prior to the U.S. direct broadcast satellites becoming operational. In other words the assumption is made that the market penetration for Canadian scrambled DBS services will not be affected by competition from U.S. services.

7.3 DBS System Users

It is likely that the DBS system will be used by organizations distributing programming and other services that would not require scrambling. This and other studies have identified such users as including the CBC, TV Ontario and B.C. Educational Television. It is also possible that the CJOM/TV station in St. John's, Newfoundland, carrying CTV programming would become a permanent regional service using the DBS.

The La Sette organization is currently using a 12 GHz transponder of ANIK B to distribute continental French programming to cable systems throughout Quebec, and have stated (h) that this service would be transferred to a DBS service. It is probable that this service would then be scrambled to prevent reception by unauthorized individuals. As, however, La Sette's market is wholly Quebec cable TV systems, and this service is already an integral part of the subscriber package, from the viewpoint of the viewer, it can be treated as a "free" service.

The possible reception of unscrambled, attractive programming such as CBC 2 and TV Ontario by the "direct-to-home" segment of the market would obviously have a major effect on the viability of scrambled services to this segment of the market in-so-much that it is far more likely that people will invest in an earth station to receive "free signals" and then become pay television subscribers, than they are to invest in an earth station for pay-television purposes only.

As the likelihood of non-scrambled services using the DBS is considered to be extremely high (c)(f), the assumption is made that all markets are able to receive unscrambled signals on their ROSES as well as the scrambled signals.

7.4 DOC Earth Station Ownership Policy

The current policy of the Department of Communications regarding ownership of earth stations restricts ownership of transmit-only satellite earth stations (TOSES) to Telesat Canada who in turn leases the transmit stations to ANIK users for, what is considered by many, a very high leasing fee.

Current DOC policy regarding ownership of ROSES is also restrictive, but currently permits ownership by Telesat, common carriers, broadcasters, cable television companies, resource companies and educational authorities. It does not however, permit ownership and operation by individuals or organizations other than those specified above. There is currently considerable pressure from many groups to change the ROSES ownership policy, and somewhat less, but still significant pressure to permit more liberal ownership of TOSES.

For the purposes of this task the assumption is made that prior to a DBS satellite going into service all significant restrictions on the ownership and operation of ROSES will be lifted, but that the policy on ownership and operation on TOSES will remain, restricting such ownership and operation to Telesat Canada.

7.5 The Use of 6/4 GHz Satellites for Pay TV or Other Scrambled Service Distribution

In 1980 the CRTC licenced Canadian Satellite Communications Inc. (CANCOM) to distribute television services to Northern and remote areas via the 6/4 GHz service of ANIK B, in spite of a number of applications that planned on using the ANIK B 14/12 GHz service or ANIK C (14/12 GHz) to distribute the same service.

This decision caused considerable concern amoung certain segments of the communications industry who felt that by requiring small communities to purchase expensive 4 GHz ROSES to receive this service the future use of a 14/12 GHz DBS would be discouraged.

The CRTC has recently held a major hearing of Pay TV licence applicants, and is currently considering its decision. While it is understood that all applicants plan to use satellites for distribution of their service, only two (14)(15), have specified that they will use ANIK C for distribution, and one of these (15) has stated that they would use ANIK D for the first two or

three years of operation and only then consider ANIK C. It is possible therefore that Pay TV licences would be issued for a 6/4 GHz point-to-point communication satellite distribution system rather than a DBS system. It is felt that such a decision, which could be expected to further erode the market for a DBS system, is unlikely to be made.

The work in this report is therefore based on the assumption that all Pay TV licencees would use the DBS system.

7.6 Copyright

The matter of copyright and copyright charges on material distributed by broadcast satellites, both scrambled and unscrambled, is yet to be resolved. There is a body of opinion that states that copyright charges for signals distributed by DBS could be based on the total possible number of viewers rather than the number of subscribers to the service. Even if this were not so, the position regarding copyright of services received in a direct-to-home mode or from a redistribution system, is currently the subject of considerable controversy. Currently there is not sufficient agreement to even make an estimate of likely copyright charges.

The assumption has been made therefore that the matter of copyright will be resolved in such a manner that the incremental charges due to this factor will not significantly impact upon the market viability of scrambled services.

7.7 Type of Scrambling Used

The scrambling concepts identified in Section 4 as being prime candidates for Canadian DBS scrambling systems are:

a) for feature movie Pay TV (not pornographic movies) and other services in which the audio is critical to useful reception: Audio-only digital encryption;

b) for Pay TV services which would include sports and spectacular programming and pornographic movies or other services in which the video signal alone supplies acceptable information: Line manipulation or this concept in conjunction with other scrambling methods such as sync. suppression.

The assumption is made that by the time DBS service is in operation both of these scrambling and descrambling approaches will be readily available at a decoder cost in the general range of $100 for category a) and $150 for category b) above.

7.8 Programming Permitted

A further factor in the overall viability of a DBS scrambling system, specifically Pay TV systems, is the type of program permitted to be carried via CRTC. At the recent hearings there was very considerable dichotomy between the CRTC's position that Pay TV should have, from the beginning, a very high percentage of Canadian content, and the position of many potential Pay TV operators that for the system to be viable they would have to provide programming attractive to potential subscribers. This was not necessarily high in Canadian content and would, certainly at the beginning, have very high U.S. content.

As this factor is likely to have a key economic impact, but is in no way related to all the scrambling systems used, the assumption is made for the purpose of this task that the programming carried by Pay TV systems will be attractive to potential subscribers and will not have a negative impact upon market viability.

7.9 Future Policies on "Unlicenced" Pay TV

There is currently considerable uncertainty in law regarding the precise jurisdiction of the Department of Communications and the CRTC regarding Pay TV and satellite reception. Recent court decisions in New West Minister, B.C.; Cornerbrook, NFLD; and Sudbury, Ontario, have found some subordinate legislation ultra vires. A recent statement by Communications Minister Fox (39) indicates that these cases will be appealed, as will any further cases that are decided in a manner unfavourable to federal jurisdiction.

In addition to the above, information has been received from several sources that a number of Ontario Cable Television licencees operating in Southern Ontario plan to commence closed circuit "bicycle tape" Pay TV operations in the near future prior to any CRTC Pay TV licencing decisions. It is further understood that legal opinion on this matter indicates that such closed circuit operations would be outside of DOC/CRTC jurisdiction.

It is possible that the general uncertainty of Pay TV jurisdiction, combined with a slow decision on the part of CRTC regarding Pay TV licences could bring about a whole range of unlicenced Pay TV operations. While it is expected that such operations would not use the satellite (Telesat Agreements normally have a clause requiring organizations leasing satellite transponder space to have all required operating licences) a general trend towards unlicenced operation of Pay TV could have a significant impact upon satellite use. At minimum it could cause significant delay in formal approvals while the matter of jurisdiction, and penalties, was decided.

For the purposes of the economic consideration section of this report it is assumed that any non-licenced Pay TV operations would not have a significant economic impact upon a DBS scrambled system.

8. ECONOMIC CONSIDERATIONS AND CONCLUSIONS

In this section the affect of the scrambling concepts identified in Section 4 "Technical Considerations and Conclusions" on the potential markets and penetrations of DBS services are considered. The forces driving present technological development in this area are also identified, as are the cost/performance trade-offs available.

In assessing the categorization of the types of scrambled service to be considered, it was decided that a primary categorization should be into public services and private.

Public services are defined as those that aim toward the widest public market with no restriction on the reception of service other than payment of the subscription fee.

Private services are defined at those that are aimed at a specific limited market and are restricted either by the type of programming or by subscriber criteria defined by the originator.

8.1 Public Services

Public DBS services have been broken down into the following categories:

8.1.1. General Pay TV Services

This category covers a Pay TV service which at various times would include sports, spectacular shows such as Royal Weddings, pornographic movies (if permitted by the CRTC), "prepared for Pay TV programming", feature movies and any other programming acceptable to the CRTC and for which there is a subscriber demand.

8.1.2 Specialized Pay TV

Under this heading comes Pay TV services that are dedicated to only one of the categories tabulated in 5.1.1 above, with the sole exception of feature movies which will be dealt with under a separate category below due to its specialized scrambling option.

8.1.3 Feature Movie Pay TV

This is defined as those Pay TV organizations that carry, virtually exclusively, feature movies and made for Pay TV programming in which the audio content is a significant and critical part of the information being transmitted. This service is categorized separately as it is likely that an inexpensive, but highly secure, audio-only digital encryption scrambling would be applicable.

8.1.4 Information Services

Under this heading are grouped both one-way and two-way "Telidon type" information services. It is envisaged that as this type of service develops, the demand will initially be for specialized information which will be considered later under private services. However the whole concept of Telidon is based on its development into a consumer type service and this is the service considered under this heading. Although a considerable amount of consumer type information is likely to be local, flight and train times etc., it is also expected that there will be a significant amount of national interest information which would require regular updating. The logical distribution method for such information would be via a DBS. Telidon can be used in a broadcast mode using frame grabbing techniques, or in a two-way interactive mode requiring a feedback link. In evaluating this service, both are considered, as statistics show that telephones are as widespread in Canada as television sets (8)(9). The feedback

therefore could be via a telephone line. In both the broadcast and interactive mode Telidon can be distributed either by broadband or narrow band system. For the type of information considered here, it is suggested that the narrow band mode would provide a sufficient information rate. This service could therefore be carried over the DBS on an additional narrow band (audio type) carrier interleaved with video channels on a full transponder. The incremental space segment cost is therefore expected to be very low.

8.1.5 Pay Audio

There could well be a public service market for very high quality music programs. One of the main problems here is of course achieving this very high quality after scrambling and descrambling. With the advent of digital audio, and the comparative ease of digital encryption with essentially no deterioration of quality in the encoding and decoding process, this type of service becomes a reality. Again it is envisaged that such a service would be carried on additional carriers inserted in unused portions of a wide band video carrying transponder, and would therefore have low incremental space segment cost.

8.2 Private Services

In considering the various types of private scrambled service that might be distributed by a direct broadcast satellite, a wide range of services were considered, including those identified under 3.2 Economic Considerations (Section 2) of the contract. Item (d) of 3.2 specifies that teleconferencing may be included among services to be considered. In reviewing this requirement, which by definition necessitates two-way communication, various methods of implementing this service by DBS were considered. Teleconferencing is taken to include both audio conferencing and video conferencing. In the former case a return telephone path would be required. This being so, the concept of having one way via a DBS and the return pass via a telephone is nonsensical. The other alternative would be to have a transmit facility incorporated in the subscriber's earth station. It is considered that this would no longer be a DBS system but a point-to-point system, and there are currently available quite adequate SCPC satellite systems providing this service.

In considering video conferencing the same two-way requirement applies, but in this case a broad-band link is of course needed. Again this would be considered a two-way point-to-point domestic satellite service, rather than a direct broadcast service, and there are currently technical facilities under development to provide this type of service.

It was felt therefore that the inclusion of tele-conferencing as part of a DBS study was inappropriate, and, with the approval of the Scientific Authority, it was dropped from further consideration.

In reviewing the other types of private service likely to be developed, either through a technology push or a market pull, the groups of services given below were categorized.

8.2.1 Professional Service TV

Under this heading comes a wide range of potential services aimed at specific professions or trades. One common factor is that the information to be distributed can most readily be transferred via a video image with a normal audio carrier. It is envisaged as basically a one way information service, although provision could be made for limited audio or data interaction via the domestic telephone network.

Examples of the type of service defined here are medical services to remote areas where video taped information of specific procedures could be transmitted upon request and the use of such a service by the automobile industry to show maintenance techniques on new cars. This would replace to some extent maintenance manuals, or expensive video tapes.

A wide range of potential users are envisaged under this heading.

8.2.2 Educational TV

This type of service has already been pioneered in a number of areas in Canada using cable TV networks as the distribution method. Credit courses are given by both universities and community colleges by the distribution of video images from cameras in the lecture room. Two-way interaction is provided by the domestic telephone service and text books are purchased and used in the normal way.

The extension of this type of service to DBS is a natural one, and would provide additional educational facilities to a wider audience. As this service becomes more wide-spread and popular there will be increased pressures to scramble service to prevent students purchasing text books and watching the course without signing on and paying for it.

8.2.3 Narrow Band Information Services

This service is seen as being very similar to that defined in 8.1.4 above except that the information provided would be aimed to specialized professional and trade users. Again the service could be two-way interactive using the telephone as the upstream link, or one way. It is perhaps worth mentioning that it is considered that the use of such services by private users is likely to be spread over a comparatively random time scale. It is thus less likely to clash with the planned traffic patterns of the public telephone service than would, say the use of this service for the interactive link on pay program TV.

Examples of such a service are as a resource providing information on legal precedence, the use of the service by a multitude of government departments to provide up-dated information on regulations, services, taxes, etc. etc.

8.2.4 Narrow Band Audio or Data

Again similar in concept to the services described under 8.1.5 above but with the addition of possible narrow band data services similar to those currently using dedicated telephone lines to provide stock market, marine, weather and other information on hard copy print-outs.

Examples of private audio services would be talking books for the blind and "store cast audio" for a variety of business users.

8.3 Definition of Potential Markets

The economic considerations of scrambled services are likely to vary from market to market. In reviewing the possible catagorizations of markets, and in discussing this matter with the Scientific Authority, it was decided to break down the potential markets into type

of user rather than to categorize the market by geographical position or other criteria. The reason for this was that it was considered that there will be little difference of economic considerations affecting scrambled TV services for, for example, a rural domestic consumer in B.C. or Newfoundland. On the other hand, there could be considerable difference in impact between the rural domestic consumer and the urban domestic consumer, if only because the urban domestic consumer is likely to receive his service via a cable distribution system.

The markets were therefore divided into various user groups as detailed below.

8.3.1 Rural/Remote Demestic Consumer

This category is defined as all households located outside of major urban areas and receiving of an average less than four distinct TV channels. This definition, together with populations, channels received etc. is taken from previous work (13).

The total number of Canadians in remote/rural areas is estimated to be in the order of 10 million, with some 4 million being in remote areas and 6 million being in rural areas.

This classification would be characterized by a high proportion of direct-to-home users, a high demand factor for entertainment services, and a wide range of disposable income.

8.3.2 Urban Domestic Consumer

This category is defined as all Canadians living in large cities, a total of some 12 million.

They are characterized by the fact that in general they receive television via a cable distribution system, and would be likely to do so for DBS scrambled services. They are further characterized by having a high level of TV entertainment with an average of some 13 distinct channels with over 30% of urban Canadians having over 15 (13) distinct TV channels currently available without charge other than the cost of cable distribution and the initial purchase of a TV set and converter. It should be noted however, that in general, disposable income is high, with entertainment purchases having quite high priority.

8.3.3 Business User

The category includes all users, both remote, rural and urban, who use any scrambled DBS service for a business purpose. Specifically excluded are users of professional services, which are covered separately, and users of educational services which are included in the two consumer groups. Also specifically excluded are Canadian redistribution organizations such as cable television companies, MATV companies and community redistribution organizations together with organizations such as La Sette and CanCom. The subscribers of such organizations are included in the two domestic consumer groups. Examples of business users are: broadcasters; television retailers and the like; and farming, logging, mining, oil and similar businesses.

8.3.4 Professional Users

Under this heading are grouped all users of professional service TV whether they are located in urban, rural or remote areas.

8.3.5 Temporary US Corporate Users

Telesat Canada has received enquiries from the Comsat organization in the United States for use of interim DBS ANIK C transponders. This would be on a temporary basis to provide service to cable television distribution systems in the United States, until such time as the high power American DBS satellite is in service.

In addition, CanCom, along with a U.S. partner, is interested in the use of an interim DBS ANIK C, with a Southerly tilt to serve primarily the U.S. market.(j)

This possible user category is included for the sake of completeness, as it is likely that such services would be scrambled. This user category cannot be considered part of the Canadian DBS scrambling market. However, it is possible that it could have a significant impact upon the economic viability of the Canadian market by siphoning Canadian subscribers, particularly if it provides attractive programming prior to similar programming being available from Canadian sources. This concept will be expanded upon in Sub-Section 8.4.

8.4 Detailed Review of Economic Findings

In this section a detailed review of the findings of the economic considerations affecting scrambled DBS service is given.

It must be emphasized that many factors other than those involved with scrambled service, impact upon the economic considerations. Some of these are given in Section 7 of this Report, as are the assumptions based on those considerations. Any study of this section should therefore be preceded by a review of Section 7.

A summary of the findings given below is contained in the "Foldout Matrix", Figure 12, and this section should be studied in conjunction with that matrix. Definitions of the type of scrambled service and the potential markets shown on that matrix are given in sub-sections 8.1 and 8.2 respectively of this Report.

These findings are based, as required by the contract, on the use of the most likely scrambling systems identified in Section 4 of this report. For the next five years, the period covered by these findings, two main types of scrambling system are expected to be used.

The first of these, the group of scrambling techniques which include line inversion, line swapping and line dicing or a combination of any one of these with other techniques, are combined under the heading of Line Manipulation Systems (L.M.). There are at least two line manipulation scrambling systems readily available, at large quantity costs in the order of $150. Both have high security levels, a degree of restoration meeting the required norm, and ease of tiering combined with individual addressability.

The second type of scrambling system considered is that of high security, digital, audio only encryption (A.O.). This is considered to be applicable to a considerable range of services both public and private. At least one major supplier is in the final stages of development of such a system, which is expected to retail in large quantities at under $100.

These findings are based upon the use of one or another of these scrambling systems as identified in Figure 12.

It is still considered that ultimately scrambling systems will utilize full digital encoding and encryption of the video signal. As there are a number

of major problems, such as bandwidth, still to be resolved with these systems, it is not expected that they will come into general use for some 5 years or so. They are therefore, not considered as part of this review.

In evaluating the economic viability of the various types of scrambled service in the potential markets identified, four key factors were derived as a basis of the overall findings. These key factors were:

a. The estimated total potential market for the particular service in the particular market considered.

b. The perceived interest in that market together with an estimate of the percentage penetration achievable within 5 years.

c. The scrambling system considered applicable to the particular type of service. These are given as either line manipulation (L.M.) or audio only encryption (A.O.). The latter is also considered applicable to narrow band data scrambling.

d. Driving (or limiting) forces. These are the economic considerations that are either the driving force for the use of the service, or are inhibiting its application.

The findings given in this section are based on many inputs including, but not limited to, references 13, 14, 15, 17, 18, 24, 26, 27, 28, 29, a, c, f, h and j; informal discussions with many members of government and industry; and the general knowledge and experience of the consultants carrying out this work. Although every attempt has been made to make these findings as objective as possible, it will be appreciated that in a predictive study such as this, with many variables, the findings are to an extent judgemental.

8.4.1 Rural/Remote Domestic Consumers

There are slightly less than 1 3/4 million households (13) in remote/rural areas of Canada. As these areas are defined as areas that can receive on average less than 4 TV channels, compared with an average of 12.6 channels for urban domestic consumers, this category is a prime market for both pay TV and educational TV. In Figure 12 pay TV has broken down into three groups: General Pay TV, Specialized Pay TV and Feature Movie Pay TV. Estimates of five year penetration have given 50%, 10% and 40% respectively. These figures, however, are

dependent upon the type of programming permitted by the CRTC; whether or not multiple pay TV programming is permitted; and whether or not the programming permitted on general pay TV would contain sufficient video only content programming to justify the 50% higher cost of line manipulation scrambling as compared with the audio only scrambling. This is considered to be the prime trade-off in this area.

In all three pay TV categories the driving force is the market. All hearings on pay TV attracted large numbers of letters from individuals and groups insisting on this type of service to rural and remote consumers.

There appears to be little demand for public narrow band information services (Telidon), and such driving force as there is appears to come mainly from the technical supporters of Telidon, mainly the Federal Government. The limiting force appears to be the market, with little perceived need for this service. However, should it come about, a modified form of audio only scrambling would give full security.

Generally speaking the same comments apply to the Public Service narrow band pay-audio. The technology is there to give very high fidelity sound, with a cost, bearing in mind the small audience, dependent mainly on the space segment cost for narrow-band services.

Again audio only scrambling would be applicable.

The only private service applicable to the rural/domestic consumer is that of Educational TV. The expected 10% penetration for this private specialized service could give reasonable viability, especially as audio only scrambling is likely to be applicable.

There appears to be considerable market demand supplying the driving force for this service, with economics, particularly space segment costs being amortized over a comparatively small number of subscribers, providing the limiting factor.

8.4.2 Urban Domestic Consumers

Statistics Canada (9) gives the number of urban households in Canada in 1980 as slightly over 6,330,000. From the view point of scrambled DBS services this market is however very different from that of the rural/remote domestic consumer. The vast majority of

of these consumers are served by cable televison or MATV systems, all input received being unanimous in the position that these organizations would carry the DBS scrambled services. The subscriber is therefore not required to purchase a ROSES, but would of course be required to lease or purchase a decoder.

With large numbers of "free" TV channels already available it is likely that the driving force here will be that of technology or the supplier, rather than market need. Thus, for the general pay TV service, penetration is expected to be somewhat lower than that for the rural/remote consumer, while movie pay TV service is likely to have equal penetration, and, somewhat surprisingly, so would specialized pay TV service. The comments regarding CRTC decisions relating to these three services given in 8.4.1 above apply equally to this market area, as does the trade-off comment on scrambling methodology.

Again little market is seen for narrow band information services, largely because of little perceived need with many alternatives. The estimated penetration of 3% is expected to be below the viability level, and unless new factors appear, this service is unlikely to be developed.

Similar comments apply to narrow-band pay audio with an estimated 2% penetration factor.

Although an equally low penetration factor of 2% is allocated to educational TV services, mainly due to readily available alternatives in urban areas, this may in fact be a viable penetration level. Incremental costs of providing the course material are comparatively low, and depending upon tariff factors, the audio-only scrambling required, could mean comparatively low space segment costs. These combined with a 10% penetration in remote areas, and the possibility of comparatively high fee structures in both areas could well make this a viable service.

8.4.3 General Comments on the Domestic Consumer Market

It should be noted that Statistics Canada estimate that over the next five years the number of households in Canada will increase at 2.75% per annum, calculated annually. This increase has not been taken into account in the above estimates, which are based on 1979 and 1980 figures respectively.

An economic consideration of considerable importance in considering scrambled services for DBS that has not as yet been covered, is that of the organization required to make such a service viable.

Intrinsic to both of the scrambling systems under consideration is the concept of unique addressing. Only by this method can the service be disconnected from non-payers and from decoders that have been stolen. Again the concept of unique addressing permits the tiering of services with only the services being paid for being descrambled. This type of control is mandatory where, as in the case of direct-to-home service, there is no other contact with the subscriber.

The implication of this however, is to require a major computer based, short reaction time, control system similar to those used by major credit card companies such as American Express. The basic requirements are the same; to know who your clients are; whether or not they are in control of their decoder; and whether or not they have paid for the service. Complete control must be in the hands of the Pay TV licencee. The requirement for such a complex organizational system is likely to be one of the key economic considerations for scrambled DBS service, and any technical factors that can reduce this organizational cost are likely to be in high demand.

8.4.4 Business Users

This classification is perhaps best considered in three major segments. The first of these which covers all public services, concerns mainly but not necessarily exclusively, that segment of the business community concerned with the retailing, maintenance, distribution and manufacture of domestic television equipment. It is expected that all such businesses will purchase all of the public services for display or test purposes. This segment of the business community is estimated at something in the order of 15,000 subscribers for each of the services. The driving force is market demand, with the limiting force being merely regulatory approval of the service.

The remaining two segments of this classification are the use by remote/rural and urban businesses respectively of the various types of private service.

The services consist of narrow band information services such as specialized Telidon, and narrow band audio or data services.

It is seen that both of these services, but in particular narrow band data services with hard copy print out, are likely to attract a significant market in remote and rural areas. It should be emphasized that the data and information carried would be specialized and directed to specific company facilities, such as logging and oil camps. DBS would provide, with audio-only type of scrambling, a secure and inexpensive method of broadcasting changing information to a comparatively large number of camps or other facilities.

The same sort of thinking applies also to urban business users, however in this case there are other alternatives, so the final penetration is likely to be somewhat less. It is, however, almost certain that market pull and entrepreneurial activity will ensure that such services are made available as soon as they become economic.

8.4.5 Professional Users

This category is limited to consideration of professional service TV and the two narrow-band private services considered in 8.4.4 above.

It is considered that professional service TV would require line manipulation scrambling.

Although the penetration figures given are comparatively high, 50% for remote and rural markets and 25% for urban markets, it is expected that these would be split between a fairly large number of different professions. The penetration of one specific professional service is therefore likely to be limited to a small number of subscribers with subsequent high individual costs. There is little information available at this time to determine whether or not this market will in fact be a viable one, and considering the comparatively low costs of the scrambling systems the key factors are likely to be space segment cost and specific professional market demand. It should perhaps be emphasized that what is being considered are economically self supporting systems rather than subsidized trials or tests.

On the other hand it is considered quite likely that professional organizations will make use of narrow-band information services and narrow-band data services. It is also possible that given economic viability, professional organizations such as those concerned with the welfare of the blind, will make use of narrow band audio for "talking book" services. In common with the business market these narrow-band services would make use of a modified form of audio-only scrambling at what will be, hopefully, low cost of both the satellite segment and the decoder.

8.4.6 Temporary U.S. Corporate Users

Telesat Canada has been approached by ComSat of the United States to lease channels on an interim DBS ANIK C satellite to distribute scrambled Pay TV services to cable systems in the United States. This service would be on a strictly interim basis prior to American DBS satellites coming into service.

While superficially this may appear to be a beneficial way of ensuring early high utilization of an interim DBS ANIK C, the possible "siphoning effect" should be considered in some detail.

Past experience has shown that American Pay TV programming is extremely attractive to Canadian viewers. As this service will be fully scrambled and is expected to be available to direct-to-home and other viewers, it is very likely that Canadians would subscribe to the service in a normal and legal manner, purchase ground stations and buy or lease descramblers. As it is likely that, given the current thinking of the CRTC (d), such a service will be available before full development of a Canadian Pay TV system via the DBS, the American system would attract much of the potential Canadian market. As Pay TV is seen as the catalyst or driving force for virtually all other DBS scrambled services, such siphoning could be critical to the overall concept of scrambled DBS services in Canada.

8.5 Conclusions

In analyzing the information gained while carrying out this task the following conclusions regarding the economic considerations of scrambled DBS systems were arrived at. They are not necessarily in order of importance.

- The economic consideration of scrambled TV services offered by a DBS are affected by many issues outside of the consideration of scrambling costs, methods and systems. (see Paragraph 7)

- Assuming a viable DBS system, and flexible and forward thinking regulation, there are currently at least two groups of technical systems that meet the requirements of an acceptable scrambling/descrambling system in Canada. These are the line manipulation systems and the audio-only encryption systems.

- As well as the decoder requirements defined in Section 4, economic considerations require that any DBS scrambling system shall be individually addressable, shall permit tiering, and shall have enbedded keying facilities.

- The audio-only scrambling system shows great promise of inexpensive use in a wide range of services.

- Technology is currently extremely volatile. The two main systems being considered have only been developed into low cost systems over the last six months or so. This rapid change is likely to continue.

- Any widespread economic DBS scrambling will require the support of a sophisticated computer based billing, connection and disconnection system of a complexity similar to those required by credit card organizations such American Express, but probably linked into a real time addressable scrambling system via the DBS.

- This requirement is likely to lead towards universality of the basic scrambling system with of course individual keys and addresses for each service or pay system entrepreneur.

- For economic reasons, and for the need to link in with the fee collection and addressing system, cable TV companies and other distribution systems are likely to use the same scrambling systems as used on the DBS.

- The two main systems being considered at this time are compatible with cable distribution systems and are not likely to cause problems when redistributed. This factor could lead cable companies away from "passive trap" pay security systems.

- If Telesat leases interim DBS ANIK C channels to ComSat or other U.S. organizations for the temporary carriage of scrambled U.S. programming, this could lead to a critical syphoning off of potential Canadian DBS subscribers.

- Expeditious, broad thinking, innovative and progressive decisions on the part of CRTC are required to fullfill the promise of DBS to provide all Canadians with new and innovative services.

- Assuming that these decisions are forthcoming, scrambled Pay TV services supported by individually addressable fee collection connect/disconnect scrambling systems, show every sign of being economic.

- Assuming the economic success of public Pay TV services, educational TV, and private narrow band information, data and audio services are also likely to be viable. These services would all use a form of audio-only encryption security systems.

- The viability of professional service TV, public information services and pay audio are in some doubt.

9. POLICY CONSIDERATIONS AND CONCLUSIONS

The requirements of the contract state that policy sensitive issues, such as TV service to remote areas, and the fostering of standardization of Pay TV hardware, including the international compatability of signals should be considered.

Many of the policy matters affecting scrambled service on the DBS have already been discussed in some detail in Section 7. In addition Section 6 briefly indicates some of the problems affecting the provision of Pay TV to remote areas. This section will, therefore, identify and discuss in fairly broad terms only those policy sensitive issues identified in the contractual statement of work.

The first item identified is the provision of Pay TV to remote areas regarding durability and cost of systems. Work carried out in this study, particularly on the technical and systems aspects have indicated that technically acceptable comparatively low cost scrambling systems with acceptable levels of security are either currently available or will be available in the very near future. In addition a basic system suitable for distribution to both remote and rural areas have been identified with the proviso that "service man" installation and maintenance is not feasible. Electronic addressable systems are available and based upon current, somewhat limited experience, appear to be quite feasible. In addition, at the cost of some relaxation of control, and the possibility of a month or so "free" service, alternative control systems via the mail service are also possible. The economic study has identified the fact that to be viable it would appear that a fairly complex administration and control system, compatible to that used by credit card companies will be required for Pay TV systems.

The information gained during the study indicates therefore that the provision of Pay TV to remote areas is feasible with regard to durability of hardware, cost of service, feasibility of the system and probability of a reasonable economic return. The remaining major unknown is that of regulatory policy. This includes such variables as the permission to carry services that are considered to be economically viable, the licencing of such services prior to competition from the United States, the permission by the CRTC to carry scrambled services over a direct broadcast satellite and resolution of possible copyright problems. With regards to these matters, every indication received during the study is that unless these matters are resolved in an expeditious and far seeing manner, the viability of scrambled DBS services, including Pay TV, is likely to decrease significantly with time.

The second policy sensitive issue identified in the statement of work, is that regarding the use of multiple scrambling techniques and the potential for the development of a "universal solution" which would foster standardization of Pay TV hardware for both domestic and international signal compatibility.

The need for fairly secure service, the development of LSI chip technology, the need for large numbers of subscribers for a system to viable, and the need for a sophisticated administrative system all point to fairly large Pay TV organizations, and the subsequent trend

towards standardization. The sophisticated scrambling systems currently coming on the market and in development would permit a number of services and organizations to use the same basic scrambling system, and it is considered that after an initial "shake down period" this is the trend that the industry is likely to take. There is, however, in the mind of the authors, considerable doubt as to whether this standardization would extend to international service. Firstly true international compatibility is not considered to be feasible in the near future due to the various TV transmission systems in use throughout the world. With regards to compatability between Canadian and U.S. DBS equipment, this will depend to a very large extent, on whether or not the interim ANIK C DBS is used in Canada. If this is so, there could well be a trend away from compatibility of ground station equipment. With regard to compatibility of scrambling systems, again a great deal will depend upon who controls the Pay TV systems, and the policies adopted by the CRTC and the Department of Communications.

In summary the two major policy sensitive issues identified in the statement of work can be met from a technological, system and economic view-point but the political and other policy issues still remain to be resolved. There is unfortunately, at this time, little indication that these matters will be solved in an expeditious manner that would give a lead to the Canadian manufacturing and service industries in the provision of scrambled DBS service in an economic, efficient and effective manner.

10. RECOMMENDATIONS

From the information gathered and analyzed during the course of this study, the following recommendations are made:

- Any consideration of scrambled DBS services should take into account the external factors described in Sections 7 and 9 of this report, together with the assumptions made within Section 7. In particular the need for expeditious, broad thinking and innovative action on the part of the CRTC should be borne in mind.

- That additional work be carried out to ascertain the likely acceptance of audio only encryption of movie type Pay TV services. Such a study could include the positions of both Pay TV licencees, cable television and other terrestrial distribution companies and of course the potential subscribers themselves. This work could include a detailed study of any specific work being carried out in this area and estimates of time scales and costs.

- That continuing study should be made of the extremely volatile DBS scrambling technolgy by a long term, say one year, low key watching brief on the development and likely markets for the scrambling systems identified in this study as possible candidates for DBS scrambling systems, together with any new approaches that are developed.

- That further study be carried out to ascertain the detailed synchronization requirements for a multi-point fed DBS scrambling system with full electronic addressing.

- That a further study should be made of the back-up organization needed to ensure the economic viability of a nation wide, individually addressed, DBS scrambling system.

- That a detailed study be undertaken on the possible impact on a Canadian DBS system of the lease of interim DBS ANIK C channels to American Pay TV organizations.

* * *

DOCUMENTARY REFERENCES

1. The Canadian Association of Broadcasters. Planning for DBS: The Private Broadcasters' Perspective. September 1981.

2. The Canadian Cable Television Association. The Retailing of Subscription (Pay) Television. 1981.

3. Telecommunications Regulatory Service. Technical Requirements for the Certification of Scrambled TV Systems. TRC 59, Issue 1, May 1, 1981.

4. Stephan, K. Examining Scrambling. Communications Engineering Digest, July 1981, pp. 22-34.

5. Telesat Canada. Study of the Use of Anik C for Direct-to-Home and Community Television Distribution Services, Brief Discussion Paper. May 1981.

6. Pritchard, W.L. and C.A. Kase. Getting Set for Direct-Broadcast Satellites. IEEE Spectrum, August 1981, pp. 22-28.

7. Canadian Radio-television and Telecommunications Commission. Pay-Television Background Research Paper: Pay-Per-Program Pay Television. March 1978.

8. Statistics Canada. Telephone Statistics. Catalogue 56-203 Annual, 1979.

9. Statistics Canada. Cable Television. Catalogue 56-205 Annual, 1980.

10. Parkinson, Peter and Associates Limited. Cable Pay-TV Technology 1981. Cable Telecommunications Research Institute, March 1981.

11. Dodds, D.E., G. Wacker and M. Neudorf. Subjective Evaluation of Delta Codecs in Quality Music and Sound Broadcast Distribution. Department of Communications, March 1981.

12. Canadian Cable Television Association. The Right to Receive? Special Report, CCTA, May 1981.

13. Telesat Canada. Study of the Use of Anik C for Direct-to-Home and Community Television Distribution Services. September 1981.

14. Extract from Pay TV Licence Submission of Premiere Alberta Television Limited to CRTC, July 1981.

15. Extract from Pay TV Licence Submission of First Choice Canada Incorporated (Don MacPherson) to CRTC, July 1981.

16. Canadian Radio-television and Telecommunications Commission. Private Low-Power Radio Rebroadcasting Stations for Remote Areas. CRTC Public Announcement, July 13, 1976.

17. CRTC Decision 81-25 on Extension of Service to Remote and Underserved Communities, April 14, 1981.

18. Committee on Extension of Service to Northern and Remote Communities. The 1980's: A Decade of Diversity; Broadcasting, Satellites and Pay-TV. CRTC, July 1980.

19. Canadian Broadcasting Corporation Annual Report 1980/81.

20. Wallingford, R. Pay TV Security Analysis. IEEE Transactions on Cable Television (USA) Vol. CATV-3, No. 2, April 1978, pp. 56-69.

21. New Satellite Security System Could Stem "TVRO Fever". Cable Communications Magazine, Vol. 47, No. 10, October 1981, pp. 17-18.

22. Dassler, A. Fred. What Are They Doing to Direct Broadcast Satellite Services? Telecommunications, November 1981, pp. 29-32.

23. Hanas, O.J., P. den Toonder and F. Pennypacker. An Addressable Satellite Encryption System for Preventing Signal Piracy. IEEE Transactions on Consumer Electronics, Vol. CE-27, No. 4, November 1981, pp. 631-636.

24. Pay-TV Hearings, The Players and What They Proposed. Broadcast Technology, November/December 1981. pp. 34-35.

25. Landfear, D. Build This Pay-TV Decoder. Radio-Electronics, January 1981, pp. 41-44.

26. Summary of CCTA Plenary Session on DBS Given at the May 1981 Convention in Quebec City.

27. Computer Predicted EIRP Contours for COMSAT DBS System.

28. Mangulis, V. Security of a Popular Scheme for TV Pictures. RCA Review, Vol. 41, September 1980, pp. 423-432.

29. Spears, G. and Lynette Gillis. Prospects for Television in Northern Ontario: A Social Impact Evaluation of the Direct Broadcast Satellite Field Trial. TV Ontario Office of Project Research Report No. 22-1981, February 1981.

30. Changes Announced to Facilitate Reception from Canadian Satellites. DOC News Release, Ottawa, December 31, 1981.

31. Poubeaud, J.J. "Cryptage" du son pour la télévision à péage. TLE No. 460, Janvier 1981, pp. 29-30. (original in French; translation included)

32. Resource Development Installation Licence Order. CRTC Public Notice 1981-79, 19 October 1981.

33. Barnes, J.W. Service Information Sheet. Canadian Satellite Communications Inc., November 1981.

34. The Canadian Cable Television Association. The Retailing of Subscription (Pay) Television. 1981.

Dodds, D.E., G. Wacker and M. Neudorf. Subjective Evaluation of Delta Codecs in Quality Music and Sound Broadcast Distribution. Department of Communications, March 1981.

35. Landfear, D. Pay-TV Decoder. Radio-Electronics, January 1981, p.p. 41-44.

36. Peter Parkinson & Associates Limited. Cable Pay-TV Technology 1981. Cable Telecommunications Research Institute, March 1981.

37. Stephan, K. Examining Scrambling. Communications Engineering Digest, July 1981, p.p. 22-34.

38. Telecommunications Regulatory Service. Technical Requirements for the Certification of Scrambled TV Systems. TRC 59, Issue 1, May 1, 1981.

39. Canadian Communications Regulation and Policy. Vol. One, No. 8, January 1982.

* * *

INTERVIEW REPORT REFERENCES

a) Dr. George Cormack, Director of Engineering, Canadian Cable Television Association, 16 November 1981

b) Miss Susan Cornell, Director of Public Affairs, Canadian Cable Television Association, 16 November 1981

c) Mr. Wayne Stacey, Executive Vice-President, Canadian Association of Broadcasters (CAB), 17 November 1981

d) Mr. Vince Lee-Chong, Director, Cable, Radio and TV Operations, Planning and Development, CRTC; and Mr. Andrew Kolada, Director (Technical), Broadcast Planning and Development, CRTC; 25 November 1981

e) Mr. John Feltmate, Planning Officer, Cable TV, Radio and TV Operations, CRTC, 28 November 1981

f) Mr. John Shewbridge, Vice President Planning, Canadian Broadcasting Corporation (CBC), 7 December 1981

g) Mr. Nick Hamilton-Piercy, Vice President Engineering, Rogers Cablesystems Inc., 6 January 1982

h) Mr. Marcel Cherrett, Chief Engineer, La Sette, Montreal, 7 January 1982

i) Mr. Nick Hamilton-Piercy, Vice President Engineering Rogers Cablesystems Inc., 12 January 1982

j) Mr. H. John Underhill, Vice President Operations, Canadian Satellite Communications Inc., 13 January 1982

* * *

COMPUTER SEARCHES

The data base SCISEARCH was searched for (Pay OR Paid OR Subscription OR Scrambling) AND (Television OR TV). Three references were retrieved from 1981, two from 1978-80, and 1974-77 yielded no results.

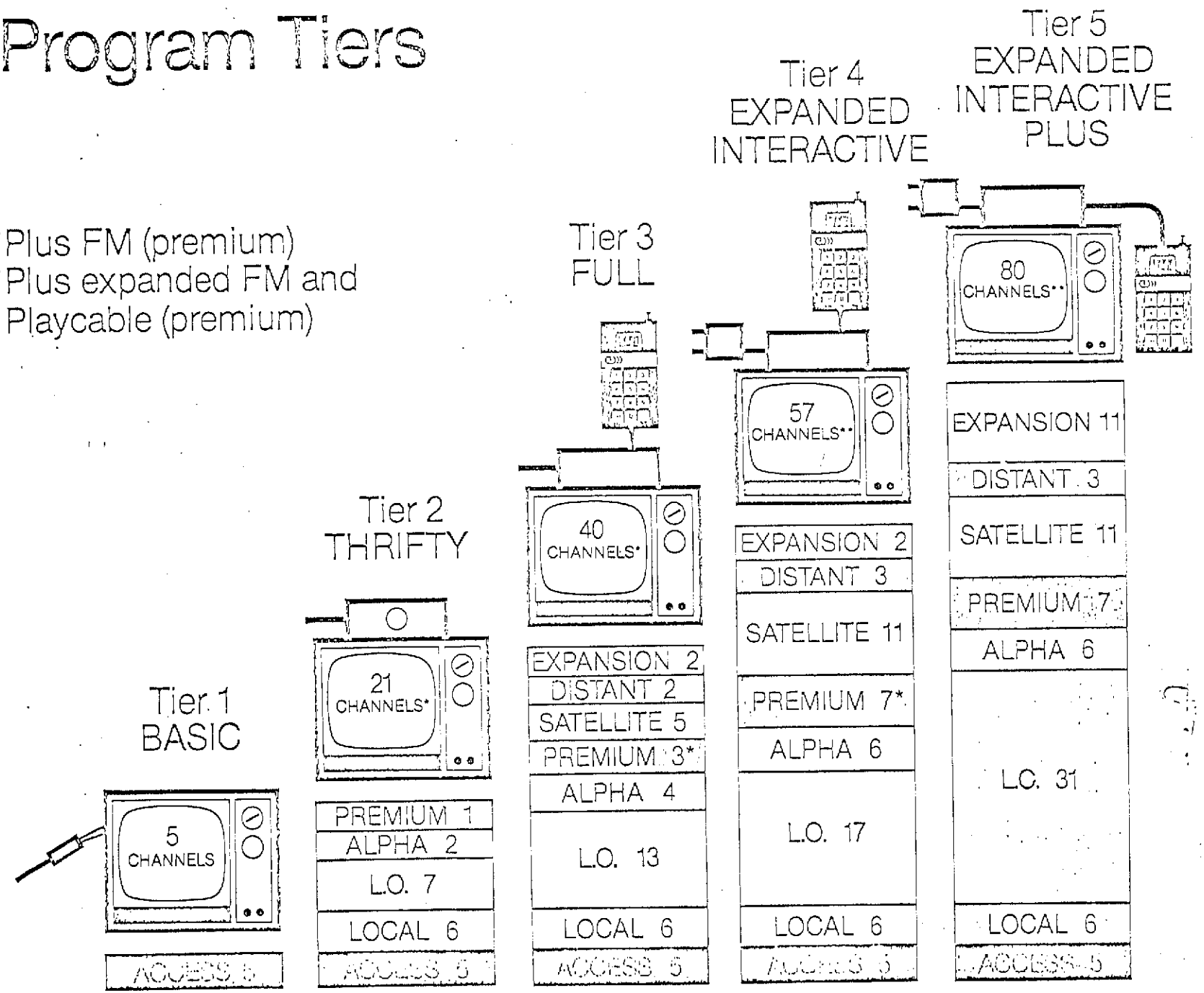
The data base INSPEC was searched originally for Scrambling AND (TV OR Television), limited to title only. This resulted in one reference from 1978-81 and one from 1969-77.

INSPEC was then searched for (Pay OR Paid OR Subscription OR Scrambling) AND (Television OR TV). This yielded 66 references from 1969-77 and 56 from 1978-81.

* * *

Program Tiers

*Plus FM (premium)
**Plus expanded FM and Playcable (premium)



APPENDIX D

THE TIERING SYSTEM

Tier 1: Basic Service

This tier is provided without recurring charge to the subscriber as a public service. A onetime installation charge will be made after which the subscriber will be able to freely view the five access channels to be controlled by the Portland Community Cable Information Corporation (PCCIC). Subscribers to this tier will be provided with a single A-1 cable drop, and channel converters will not be necessary to receive service. The provisions of this tier will enable the PCCIC to maximize exposure of its programming within the Portland Community.

Tier 2: Thrifty Service

Each higher tier includes all programming services offered in lower tiers. The thrifty tier thus incorporates the basic tier and adds to it 17 programmed video channels providing a low cost, 21 channel service which blends access and local broadcasting with local origination. All local television stations will be distributed with signal quality that guarantees perfect reception. Seven locally originated services are offered including community-focused and informational programming addressed at areas like health, education, the environment government, and to minority or disadvantaged groups. In addition the tier provides a community information service and offers two premium services, a mini Pay-TV service and a comprehensive FM radio service. Subscribers require a channel converter which sits on top of the television set.

Tier 3: Full Service

CSP's full service provides subscribers with 40 channels and adds two distant TV "Superstations" and five other satellite-fed services to the Tier 2 menu. Five additional local origination channels and two additional premium channels are offered as well as several customized alpha-numeric services. The tier features several composite satellite/local origination channels where CSP's own programs are "wrapped around" satellite services to provide specialized channels dedicated to viewing audiences such as children, senior citizens, arts enthusiasts, movie buffs, sports fans and others. The tier also features limited pay-per view teletheatre options and interactive services for subscribers electing to pay an incremental charge. The tier features a converter unit and a remotely controlled keypad which provide viewing convenience and easy channel selection.

Tier 4: Expanded Interactive Service

Tier 4 moves the CSP subscriber directly into the future by providing access to a range of special interactive services in addition to an expanded menu of programming services. The tier offers 57 channels via dual cable drops, adding 17 fully programmed video channels to Tier 3 service. These include more satellite and local origination services, several composite satellite/local origination channels, alpha-numeric channels, superstations and premium services including video games. Many of the locally originated channels offered on this tier are interactive, allowing the subscriber to engage in a variety of activities through CSP's customized two-way response system that is more fully described in Section 14. In addition many of the locally originated services offered at lower tiers become interactive to the Tier 4 subscriber, providing a new dimension in the viewing experience. This tier also features a unique interactive service on two special channels. Known as time-shared Telidon, this service has been specifically designed for Portland and introduces, for the first time in the U.S., Canada's revolutionary Telidon information retrieval system. The tier is accessed by the same converter unit and keypad as Tier 3 but a home terminal transmitter is provided at no extra charge to permit full interactive capability. Both A-1 and A-2 cables are used to deliver Tier 4.

Tier 5: Expanded Interactive Plus Service

The ultimate in viewing choice and diversity, Tier 5 adds an incredible 23 channels to the Tier 4 line-up, including channels dedicated to fully interactive teleshopping and Telidon services. These services push the state of the art in cable service technology beyond its current limitations, providing genuine viewer-controlled search and retrieval alternatives and opening up the world of teletext and videotex service. While several of the Tier 5 channels will be activated at time of system launch, others will be gradually brought into service as subscribers become more aware of these services and potential information providers in Portland begin to utilize the teleshopping and Telidon facilities, creating viable levels of demand. Tier 5 will be delivered by both A-1 and A-2 cables and will use the same delivery hardware as Tier 4.

* * *

APPLICATIONS OF ONEWAY FUNCTIONS

"Oneway functions" are used to protect the security of time-shared computer password lists. In that application a password $\underline{P}$ is given to a user. On reception of $\underline{P}$, the computer forms $f(\underline{p}) = \underline{W}$ and compares $\underline{W}$ to its list of "indirect" passwords. If $\underline{W}$ is legitimate, time-shared service is made available. The strength of the system is found in the security of the list of indirect passwords $\{\underline{W}\}$. If one or all of these $\{\underline{W}\}$ are stolen, it is still not possible to calculate all or one of the $\{\underline{p}\}$ because $f^{-1}(\underline{W})$ is not computationally feasible.

That same idea could be used to "authorize" a subscriber's control unit. Periodically, all indirect passwords $\{\underline{W}\}$ could be broadcast, and each subscriber control unit would make a comparison with its particular indirect password $\underline{W}$ as calculated from the subscriber's password $\underline{p}$. Only if a valid comparison were made would the unit continue to function.

Since $f^{-1}(\underline{W})$ is not feasible to compute, it would not be possible to steal a valid password from the broadcast $\{\underline{W}\}$. So that a subscriber would be motivated to keep his $\underline{p}$ secret, the control units would record (for later billing purposes) the password used to activate the unit. Billing would be to the password holder, not to the individual leasing the unit. Perhaps the password $\underline{p}$ could be recording magnetically on a plastic card used to activate the control unit, thereby transferring the security from the password to the card.

In this approach all control units would be the same, identification for billing would be via the plastic card and knowledge of f need not be secret.

* * *

A SERVICE SUBSCRIPTION SYSTEM

In order that TV signals transmitted by satellite not be stolen it is necessary that the signals be scrambled or encrypted. A reasonable level of descrambling difficulty must be attained if the scrambling is to prevent theft and, if subscribers are buying descrambling services, their descrambling units must be designed to prevent tampering.

All scrambling and encryption methods require a key to allow descrambling or decryption. This may simply be knowledge of the method but, in more useful techniques, the key varies dynamically with time. The problem in scrambled TV via DBS is the transmission of the proper keys to the subscribers in the absence of the physical connections and feedback path always present in cable TV systems.

Initial considerations suggest the need to be able to directly and uniquely address each subscriber via the satellite to activate the appropriate service level, or to have communication via the telephone system for activation and monitoring in pay TV systems. Here a service subscription system is suggested which requires neither unique addressing nor utilization of the telephone system. The economic advantages of such a system are considerable.

The system is an application of modern cryptographic science which assures the security of the transmission of the keys necessary to control the descrambling process. Also essential is the security of the electronic control unit (hereafter called the converter) which is positioned between the receiving antenna and the subscriber's TV set. This unit is assumed to be encapsulated or sealed so that tampering is not possible. There is no need, however, for any secrecy regarding the scrambling and encrypting systems and the design of the converter. Only the keys need be secret.

A number of variations are possible and we shall begin with the simplest where there is one service, DBS TV, which is to be paid for by subscription: the subscriber, in return for his fee payment, receives a converter which descrambles the signal. Hidden in the converter is the descrambling key which must be kept secret from the subscriber as he might well give it away to others so they would not have to pay.

That system is fine if the key is never changed, but then long term security would be minimal; better that the key change from time-to-time. A monthly key change could allow monthly, daily or even hourly change in the detailed descrambler algorithm, assuming the received TV signal to contain basic (but not overly precise) timing information. Such a change could be entered into the converter by the subscriber himself. Each monthly bill delivered by mail would contain the next month's new key to be entered by the subscriber. However, this key would be encrypted by a unique double key so that only that particular, subscriber's converter could decode it into the actual key.

In this way the monthly key is of value only to the subscriber and security would be maintained. As a safe guard, the key could be a month or two early in case of poor mail service or late payment. In the event of a mail strike the TV display could be used to give subscribers contingency information because the converter would have one other function, namely to automatically shut-down if a new key was not entered. The shut-down could be timed for (say) two months after the last new key was entered, and the timer would have to be energized by a battery or charged capacity or in case of accidental or deliberate interruption of power to the unit.

In the case of Pay TV, the converter would have the additional capacity to store use data for billing purposes. In this system, the subscriber on receipt of his monthly bill with half the current double key, would activate a readout device. This readout would be entered onto the form to be returned with the monthly payment, and decoded by the system operator to identify the last month's TV usage by that subscriber. (The monthly bill might also contain a second code for entry into the device which would be decoded and compared to the last reading which was activated. If the readings did not compare, the converter would enter its shut-down phase. However, this precaution to assure accurate meter reading would probably not be necessary as the reading is encoded so the effects of alterations would not be readily apparent to the subscriber. Check bits could also be of use here.)

It is possible that full fledged encryption would not be needed. For example, a word unique to the subscriber could simply be added to the monthly key and send that to him in plaintext. If the unique word were stored in the converter, the monthly key could be recovered but only by that converter. That might well be sufficient security.

In summary, a system is proposed which would require neither unique (electronic) addressing, nor a telephone link, nor a meter reader. Both Pay TV and tiered services could be accommodated.

* * *