Satellite Communications Network Control in the Presence of Electronic Countermeasures

Marc Spellman

Harris Government Satellite Communications Division, Melbourne, Florida

Follow this and additional works at: http://commons.erau.edu/space-congress-proceedings

Scholarly Commons Citation
http://commons.erau.edu/space-congress-proceedings/proceedings-1984-21st/session-3/5
ABSTRACT

Satellite communications networks have supplanted other over-the-horizon communications systems because of their high capacity and high reliability. A key characteristic of satellite communications systems is that all communication links within a network share a common transponder and thus have the potential for deleterious interactions. This in turn gives rise to the need for a network control function that can establish and ensure appropriate transmission characteristics for each terminal with the goal of maximizing the communications capacity available to all network members.

Because of the potential for electronic countermeasures in military satellite communications systems, an antijam mode of operations, which by its very nature is a reduced capacity mode, is often included in the network architecture. This in turn puts added burdens on the control function for the network. Both a clear mode of operation and an antijam mode of operation (often with different properties and characteristics) must be controlled and, furthermore, a timely mechanism for transitioning between the two modes must be provided.

In this paper the generic top level requirements are defined for a military satellite communications control system. The control system function is then divided into its key components and generic requirements are provided for each component. Alternative strategies for both communicator and jammer are discussed leading to the flow of events that would result in the transitioning of the SATCOM network in response to a changing ECM environment.

INTRODUCTION

In this paper the satellite network control system is examined first. For both a nonmilitary and military satellite communications network the control system rationale and requirements are presented. The control system is then subdivided into its component subsystems and qualitative requirements are provided for the subsystems.

Following this the strategies that are available to both the jammer and the communicator are discussed with respect to the operation and design of the control system.

To put all this in perspective the paper concludes with a typical flow of events that could successfully transition the network in response to a changing ECM environment.

Control System Rationale and Requirements

Briefly stated, the fundamental purpose for a satellite network control system is to allocate satellite resources in some optimum manner. The satellite resources to be allocated are the downlink EIRP and bandwidth and the allocations must be made to each SATCOM terminal participating in the network. The allocations take the form of designations on the uplink signal parameters for each SATCOM terminal.

From the network control point of view an optimum allocation is one where the capacity available for reliable information transfer through the satellite is maximized for each user. Given that there is an upper system capacity based on the satellite transponder and earth terminal designs, it is the function of the network control system to determine allocations that result in a total operating capacity that approaches the maximum system capacity available from the equipment while maintaining an acceptable level of link availability. To do this it must minimize wasted capacity and it must assure that the transmissions from network participants do not interfere and thus reduce system capacity.

How the control system both reduces wasted capacity and assures that network participants...
do not interfere with each other depends on the method by which the satellite resources are shared between the user SATCOM terminals. The method of sharing which is generally called the multiple access technique determines what parameters of the uplink transmissions must be controlled and based on the particulars of the specific network, how accurately they must be controlled.

There are three principal multiple access techniques; frequency division multiple access (FDMA), time division multiple access (TDMA) and code division multiple access (CDMA). There is no intent in this paper to compare the virtues or shortcomings of each but since the control system requirements are related to the multiple access technique, a brief consideration of the three approaches is warranted.

There are three principal multiple access techniques; frequency division multiple access (FDMA), time division multiple access (TDMA) and code division multiple access (CDMA).

Figure 1. Multiple Access Techniques

Frequency division multiple access assigns a portion of the transponder bandwidth to each network participant. The channel spacings on the uplinks are determined by the instantaneous bandwidth of the uplink transmissions and the required frequency guard bands as determined by the filtering characteristics in the earth terminals. From a control point of view it is obvious that uplink frequency assignments must be adhered to in order to avoid interference between users. In addition, since in an FDMA system all users are simultaneously present in the transponder, the uplink power for each user must be carefully controlled. This is necessary so that both potential intermodulation interference and power lost to intermods (due to nonlinearities in the satellite transponder) are avoided, and that potential user capacity is not lost to excessive link margins.

Time division multiple access systems assign a time slot in a master time frame to each earth terminal participating in the network. In the assigned time slot the earth terminal has exclusive use of the entire transponder bandwidth and power. The earth terminal operates in a burst mode with a symbol rate consistent with the transponder bandwidth. With respect to the control requirements, the time of transmission for each earth station must be carefully controlled since transmissions overlapping in time will obliterate each other and transmissions not fully occupying an assigned time slot mean wasted capacity. However, the power control problem of FDMA no longer exists since only one user is present in the transponder at any instant of time. The power control requirement is reduced to ensuring that a constant minimum EIRP, enough to saturate the transponder, is always exceeded. The value is independent of the transmitting terminal characteristics, the information rate being transmitted from the terminal and the number of terminals in the network.

Code division multiple access systems separate user signals not in time or frequency but with an additional signal modulation. An orthogonal PN code is phase or frequency modulated on each of the user uplinks, allowing a receiver with a matched replica code to receive the desired signal without interference from the other transmissions in the network. CDMA has the characteristic of multiple simultaneous users in the transponder as does FDMA, so excess margin on any link equates to reduced capacity for other users. The power control problem with respect to intermodulation interference, however, is not as severe because of the interference reduction properties of the signal structure. Like TDMA, there is a timing accuracy requirement; however, in CDMA it is on a link-by-link basis (receiver and transmitter for each link) rather than on a network-wide basis.

Of the signal parameters mentioned above, the control of frequency and time are rather mundane. That is not to say either is an easy engineering problem, but it is the control and selection of earth terminal EIRP and bandwidth that is really at the heart of the network control function. These earth terminal parameters specifically determine the satellite allocations.

Based on the above, one can formulate two key types of quantitative requirements that can be placed on a satellite network control system. The first is to maintain no greater than some stated link margin on every link in the network. This is a legitimate requirement since, while link margin is fine for the particular link (because it assures a greater availability of the link), it isn't fine for other network members or potential members. Excessive link margin reduces the capacity
available to all other users and potential users. The second requirement is a maximum acceptable response time in which the control system must correct a deviation from the designated link margin on any link in the network. This requirement would seem naturally to be a function of both the polarity and magnitude of the deviation as well as on the particular link experiencing the deviation. For example, a negative deviation from a prescribed link margin means a statistically less available link and therefore a short response time would appear appropriate. On the other hand a positive deviation from link margin which means a loss of potential network capacity might require a response time inversely related to the amount of lost capacity. Thus, for a given deviation (in dB's) longer response times might be acceptable for lower capacity links than for higher capacity links. Similarly, for a link of given capacity the greater the deviation the shorter the required response time.

"Control system requirements center about maintaining no greater than some stated link margin on every link in the network."

This fundamental issue of link availability versus network capacity takes on an entirely new dimension in a military satellite communications network. In this paper a military satellite communications network will be distinguished from a nonmilitary network solely by its potential to be a target for electronic countermeasures. As a target for ECM the well designed military communications system must include for each of its links an antijam or ECCM mode of operation. But such a mode by its very nature is a reduced capacity mode since it either uses power or bandwidth or both far in excess of what is necessary for information transfer in order to defeat the potential jammer. Therefore the tradeoff between link availability and system capacity is greatly magnified. If one initiates an antijam mode of operation too early there is a significant loss of capacity. If one initiates an antijam mode of operation too late there is no link availability. This substantiates the need for a timely mechanism for transitioning between modes. Complicating the situation further is the fact that with a jammer attacking the satellite transponder there is a definite question as to the capacity available to the network. Allocations must then be made in an environment far different than in the nonmilitary network situation which is characterized by a much more accurate data base.

Subsystem Definition

The control function can be divided into three separate subfunctions, each defining a related subsystem to perform an appropriate task. The three subfunctions are monitoring, allocation and communications and together they constitute the control process. Monitoring addresses the analysis of the downlink from the satellite. It is the information gathering process on which to base allocation decisions regarding the network participants. The allocation subfunction determines the key uplink signal parameters of EIRP, bit rate and if applicable, an antijam or clear operating mode for each of the SATCOM terminals in the network. The communication subfunction has the responsibility of communicating the allocation decisions made by the control system to each of the SATCOM terminals. This is pictorially shown in Figure 2.

"The three subfunctions that comprise the control process are monitoring, allocation, and communication."

In attempting to develop some generic requirements for each of the three subsystems, the initial considerations go to apportioning the control system response time and maximum allowable link margin requirements to each of the subsystems. With respect to response time, a portion of the total budget must be ascribed to each of the three subsystems. A finite time is necessary to process the received satellite downlink and determine the appropriate received signal characteristics. Similarly, time is necessary to complete the allocation process which is a calculation intensive task based upon a stored data base and the monitoring results. Finally, the communication subfunction needs a time allocation that must consider the limited data rate likely for control communications as well as the need to communicate possibly a different message to each of the earth terminals in the network.

The requirement for a maximum allowable link margin on each link in the network will impact the monitoring subsystem and the allocation subsystem. The monitoring subsystem is impacted because it has the requirement for gathering the data on which an estimate of existing link margin will be made. The allocation subsystem is impacted because it must include the calculation capability that makes the link margin estimate as well as relate the required change in earth terminal uplink parameters to the desired change in link margin.

Figure 2. The Control Process
More can be said about the requirements for each of the subsystems in the cases of both a nonmilitary and a military satellite network control system. For the monitoring subsystem, the basic requirement is the accuracy to which downlink signal power can be measured. With respect to the measurement of downlink power, an output from the monitoring subsystem that can support a decision on whether or not the satellite transponder is saturated is an important monitoring subsystem requirement. When, as in the case of a military system, the potential for jamming is introduced, an immediate additional requirement should be placed on the monitoring subsystem and that is to support jammer identification and characterization. The first step in that process is to be able to distinguish the effects of an equipment failure from the effects of a jammer. Once that can be accomplished additional jammer characterization requirements, such as determining if the jammer is time varying or stationary in time, if the jammer is an uplink jammer or a downlink jammer, and what frequency channels the jammer is attacking, are all legitimate requirements.

The allocation subsystem is also significantly more complex for the military network than for the nonmilitary network. First, anytime a jammer is introduced the potential for a continually time varying network status is a real situation. The allocation subsystem must be able to react quickly and, even more important, must know when not to react at all. In addition, the jammer introduces a degree of uncertainty as to the available capacity left for the network, thus further complicating the allocation process.

Finally, with respect to the communications subsystem, the military SATCOM control system must provide a degree of antijam protection for the control link at least equivalent to that of the communications links that must be controlled. This will ensure a control capability at all times when the communications links are operable.

**Strategies for Communicators and Jammers**

The strategies for the communicator in a military satellite network center first about the alternatives available from which the network architecture can be selected and second about the various possible responses to the onset of jamming.

The prime consideration in selecting the network architecture is again the fundamental tradeoff of the availability of a particular link versus the potential capacity of the entire satellite network. It is apparent that there are two different operating modes for the military SATCOM network, a clear mode and an antijam mode. The clear mode of operations is characterized by the desire to maximize the communications capacity of the network by reducing link margins to the greatest degree possible. This desire is predicated by the reality that most military satellite communication networks rarely if ever operate in an environment characterized by a determined jammer and therefore typically operate like nonmilitary networks. The antijam mode of operations on the other hand is characterized by an extremely significant reduction in the available capacity in order to assure a communications capability even in the face of the most determined jammer. This approach is justified since the scenarios that give rise to determined jammers are precisely those where link availability becomes most essential.

"The prime consideration in selecting the network architecture is the fundamental tradeoff of the availability of a link versus the potential capacity of the entire network."

There are some alternative network structures as shown in Figure 3 and therefore strategies to effectively provide both operating modes. One approach is to use the same modem equipment to provide both the clear and the AJ operating modes and adjust operating parameters of the equipment to transition between modes as a result of control system directives. This naturally is not as easy as it sounds, since it puts the full transition burden on the control system; but it does have the advantage, if the transition can be done smoothly, of matching the right mode to the right scenario.

![Figure 3. Alternate Architectures](image)

An alternate approach that greatly reduces the burden on the control system is to transition the network between modes, not as a result of a reaction to jamming as determined by the network control system, but rather as a reaction to the potential for future jamming as determined by an assessment of the political and military situation. The penalty paid here is the lost capacity either prior to the onset of jamming or if the jamming never occurs.

Still another approach is feasible if separate modem equipment is used to provide the clear...
and the AJ operating modes. This would allow simultaneous operation of both the AJ and the clear mode of operation. The approach would proceed with the few most critical channels assigned to the AJ mode of operation and all the other channels assigned to the clear mode of operation. The capacity of the network would only be slightly degraded due to self-interference between modes. The availability of the AJ links in the face of a jammer, while not as great as it would be if the bulk of the terminal EIRP was not allocated to the clear traffic, is still protected by the processing gain inherent in the AJ mode. The transition process in this architecture does not involve the establishment of new links or the reassignment of users from one mode to another but merely the switching of the terminal EIRP from the clear mode transmission to the antijam mode transmission.

"Three possible responses to jamming are to increase EIRP, reduce data rate and initiate an antijam operating mode."

Independent of the architecture there are some general responses that are available to the communicator once a jammer attacks the satellite. The possible responses include actions relative to the satellite as well as actions relative to the earth terminals. For the satellite, if there is antijam spatial processing on board, its use to reduce the jammer power incident on the transponder is one available response. A second response at the satellite would be an attempt by adjusting the gain control of the transponder to keep the transponder out of saturation independent of the jammer EIRP. This naturally depends on the particular transponder design as well as the jammer size.

At the earth terminals there are three responses that are apparent: an increase in EIRP, a reduction in data rate, or the initiation of the antijam operating mode. The appropriate response is naturally dependent on the specifics of the jamming attack.

From the jammer's viewpoint, there are alternative strategies available as well. In considering these strategies, the first point to realize is that the legitimate and realistic goal of the jammer is not to eliminate the ability to communicate but to reduce the ability to communicate. For both communicator and jammer, their abilities are not absolute but relative. The jammer must make the decision as to the strategy that minimizes the communicator's information transfer capability while requiring the commitment of a minimum amount of resources on his part. For example, all other things being equal, uplink jamming has the potential of taking down multiple links while downlink jamming takes down only one link. One approach that might be effective for a jammer, depending upon the design architecture of the control process, would be to initiate an action that causes the communicator to transition his network. During the transition period it is likely that communications must be interrupted. Once the network transitions, the jammer can cease his action, thus "tempting" the communicator to reconfigure to the higher capacity network state that existed prior to his initial action. If the communicator does, there will be another interruption in traffic after which the jammer can repeat the process. This is an oversimplified example of a potentially rewarding strategy open to the jammer. How rewarding the strategy can be made to be is a function of the requirements placed on the control system with respect to maximizing system capacity and the reaction time of the entire network to control system directives.

"The realistic jammer objective is to reduce, not eliminate, the ability to communicate."

Other alternatives available to the jammer include his transmission bandwidth, whether he attacks the control link or the communications links and whether he attacks clear links only or if he attacks AJ links as well. There are some general considerations with respect to each of these options.

The issue of the jammer bandwidth depends closely on whether antijam links, which nominally require the entire transponder bandwidth, or clear links are being attacked. In general, there is no rationale for a jammer to spread his energy across an entire transponder since he will then be no more effective against a clear link as he would be against an antijam link.

With respect to attacking the control function rather than the communications links, this is a strategy that can potentially achieve a jammer's objective of minimizing communications via a minimum commitment of resources. Communications will eventually break down without an adequate control function and the control function might very well be susceptible to a low power downlink jammer at the control terminal.

The issue of attacking AJ links as well as clear links depends on the degree to which the jammer is committed to minimizing the communication capability and his ability to commit resources. It is apparent that the jammer has already achieved a degree of success by forcing the communicator into an AJ operating mode and it is also apparent that a greater degree of jamming resources is necessary to bring down the AJ links than was necessary to bring down the clear links.

**Transitioning**

The process of transitioning a satellite network in response to an ECM attack is
naturally dependent on both the communications and control architectures of the individual network. Since it is extremely difficult to define a general approach to network transitioning, an example of a network transition process will be presented for a particular network with the following set of characteristics:

a. The clear (no ECM) operating mode has all users operating on nonprotected communication links.

b. The protected communication links operate in the clear without traffic at a minimum EIRP in order to minimize interference with the clear links but sufficient to maintain lock at each receiver.

c. In the clear the control link is a fully protected link operating both at a minimum data rate and minimum link margin between a single control terminal and each of the earth terminals that are included in the network.

d. All protected links include an automatic reacquisition capability whereby the links can reacquire after a loss of signal of duration denoted as the reacquisition window.

e. The monitoring capability of the control system is located at the control terminal and is capable of identifying and characterizing jammers.

The transition from a non-ECM to an ECM environment for a network with the above characteristics would proceed as follows:

Step 1: An uplink jammer begins transmission

Step 2: The clear links that are attacked lose the capability for information transfer and if the jammer is of sufficient magnitude the antijam links will lose lock also.

Step 3: The monitoring function of the control system identifies the presence of jamming and must determine the appropriate response depending on the assessment of the jammer magnitude.

Note: If the jammer was of sufficient magnitude to force the AJ links into reacquisition, it is likely that a reduction in bandwidth and/or an increase in EIRP for the failed clear links will be of little value. The step to be taken then is to reallocate EIRP from clear links to AJ links.

If the AJ links remain locked, the initial response would appear to be a reduction in data rate and/or an increase in EIRP for the clear links.

For the remaining steps assume that the jammer was sufficient to knock the AJ links into reacquisition.

Step 4: The controller increases the EIRP for the protected control link to a level sufficient for all network participants to reacquire the control link.

Step 5: The controller now directs network participants to abandon the clear operating mode for the AJ operating mode, thus allocating terminal EIRP to the AJ links.

Step 6: The AJ communications links between network participants automatically reacquire (as long as the above steps are accomplished within the reacquisition window).

Step 7: The controller directs minimum operating data rates on all AJ links initially along with peak terminal EIRP's if the jammer has already driven the satellite into saturation.

Step 8: Based upon close coordination with the satellite controller and based also on the output from the monitoring process, the network controller can attempt data rate increases on the AJ links.

Conclusions

In summary, this paper has pointed out the importance of network control for all satellite communications systems. In the case of a military satellite communications system, the importance is compounded by the threat of an ECM attack and the preventive measures typically taken by the MILSATCOM system. The control system complexity for the military SATCOM system depends principally on the degree to which link margins are attempted to be reduced (network capacity increased). In one extreme where a system is designed solely with regard to link availability and thus with no emphasis on system capacity, the control system has little or no complexity. On the other hand, when a system is designed to adapt capacity depending on the current scenario, the network control system and particularly the monitoring portion of it can become extremely complex.
Mr. Spellman is a systems engineer with Harris Government Satellite Communications Division in Melbourne, Florida. His principal responsibilities are in the system level design of military satellite communications equipment with particular emphasis on antijam applications.

Prior to joining Harris Corporation, he worked for Analytics Inc., and ITT Defense Communications. There his work included communications systems studies, antenna analysis and design, and satellite transponder design.

Mr. Spellman received a B.S.E.E. degree from the Polytechnic Institute of Brooklyn in 1965, an M.S. degree in electrical engineering from Syracuse University in 1967, an M.S. degree in management science from Newark College of Engineering in 1971, and an M.B.A. degree in corporate finance and economics from New York University in 1975.

He is a member of Eta Kappa Nu, Tau Beta Pi, and Beta Gamma Sigma and has had published a dozen technical papers on topics including spread spectrum communications, radio wave propagation, portfolio theory and investment analysis, network synchronization and antenna design.
FDMA All users are on all the time but are separated in frequency.

TDMA All users are on at different times but when on utilize the entire available bandwidth.

CDMA All users on all the time and each uses the entire bandwidth.
MONITORING
RECEIVE SATELLITE
DOWNLINK SIGNAL
PROCESSING TO DETERMINE
CHARACTERISTICS

ALLOCATION
COMPUTATIONS BASED ON
RECEIVED MONITORING
INFORMATION AND STORED
DATA BASE

COMMUNICATION
TRANSMITTING
THE ALLOCATION
DECISIONS

CONTROL TERMINAL

RECEIVE

TRANSMIT

COMPUTER
MOST CRITICAL USERS

AJ MODEM

SUM/SPLIT

TRANSMIT/RECEIVE

BULK OF USERS

CLEAR MODEM

CONFIGURATION 1

ALL USERS

DUAL MODE MODEM

TRANSMIT/RECEIVE

CONFIGURATION 2

APPROACH A: SWITCH MODEM PARAMETERS BASED ON THE DETECTION OF JAMMING

APPROACH B: SWITCH MODEM PARAMETERS BASED ON THE POTENTIAL FOR NEAR TERM JAMMING

13169-4