SECURE MILITARY COMMUNICATIONS CAN BENEFIT FROM ACCURATE TIME*

by

D. W. Hanson and J.L. Jespersen

Time and Frequency Division
National Bureau of Standards
Boulder, Colorado 80303

ABSTRACT

Some military communications systems have requirements quite different from civilian systems. Among others there is the necessity to protect military communications from detection, interception, exploitation, or disruption by adversaries, particularly during times of hostilities. There are a number of techniques available to protect communications against these threats. Some of them can benefit from unambiguous time information.

A hypothetical military communications system is used in this paper to discuss these protection techniques and to illustrate how time may assume a useful role in their operation. The paper will also cover sources external to the communications system from which the necessary time information may be obtained.

INTRODUCTION

Military communications must be capable of operating within environments more difficult than are experienced by civilian systems. During times of hostilities, adversaries will attempt to intercept, disrupt or manipulate messages. These threats must be protected against. The techniques used to achieve these protection levels often have large costs including dollars, technical complexity and labor intensity. One of these costs can involve the use of precise time information. (Throughout this paper all references to "time" must be understood as referring to the internationally accepted and disseminated Coordinated Universal Time or simply UTC). The use of time can be extremely beneficial for initial alignment of long PN (Pseudo Noise) codes used in encryption and the demodulation of the non-cw or broadband carriers used in what is commonly referred to as spread-spectrum communications. A good initial alignment of codes can significantly reduce the search times for a perfect match between the codes, at which point tracking of the incoming code can commence. This paper discusses this subject through an examination of the hypothetical military communications system of Figure 1. The communications system illustrated here may not accurately represent most present day operational systems. It should, however, for those systems using very long, non-self-synchronous PN codes, be adequate to focus on the discussions intended for this paper.

PROTECTION TECHNIQUES

Specifically; some military communication systems may require protection against one or more of the following threats:

1. Eavesdropping by either direct wiretap or radio intercept.

2. Message manipulation, deletion, or replay through active wiretap or radio transmission.

3. Detection, frequency estimation, and direction finding of the radiation.

4. Jamming.

The techniques used to achieve some degree of protection against these various threats can include the application of suitable encryption techniques and/or the use of non-cw or broadband carriers (in contrast to the very familiar use of the so-called cw carrier). The specific threats rendered less effective using one or both of the previously mentioned protection measures are summarized in Table 1.

PROTECTION TECHNIQUE THREAT	Use of encryption	Use of broadband carriers
Eavesdropping	x	x
Message manipulation, deletion, or replay	x	x
Radiation detection, frequency estimation, and direction finding		x
Jamming		x

TABLE 1

There are other techniques commonly used that can add protection against these threats and are mentioned here for completeness only. Ordinarily they have no relationship to time-ordered events and do not require any type of synchronization. They include the use of non-rf

*Contribution of the NBS, not subject to copyright.

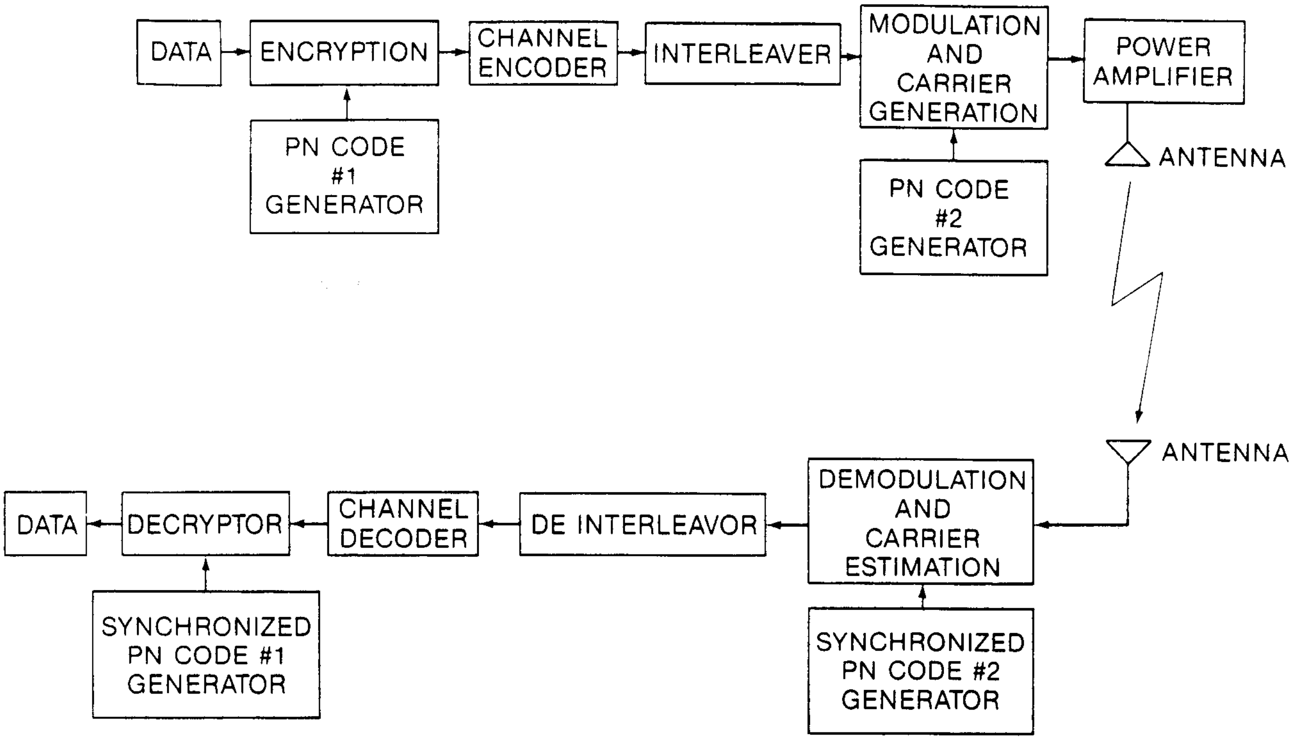


Figure 1. Generic Secure Military Communications System.

media, narrow antenna beams, sidelobe suppression and null generation, and the sending of false information or otherwise deceiving the enemy.

In the generic military communications system of Figure 1, the digital data are encrypted by being combined with the output of a PN generator. The result is passed through a channel encoder and interleaver, both used to improve bit error rate performances, prior to being passed to the final stage consisting of modulation, upconversion, and power amplification. The carrier's characteristics (frequency, phase, or time of activation) are a function of the state of the second PN generator. The output of the power amplifier and antenna is propagated to a receiver where this process is, step-by-step, unraveled in reverse order. Demodulation requires a synchronized PN generator, that is, one which is tracking in phase with the transmitting PN generator delayed by equipment delays and the propagation delays between the transmitter and receiver. The details of how the synchronized PN sequence is, in fact, utilized in the final demodulation process depends on whether the PN sequence has controlled the frequency, phase, or time of transmission of the data. The principle remains the same, however, the generation of the receiver's PN sequence must be synchronized to that received. For example, in frequency hopping the frequency pattern produced by the receiver's synthesizer must be synchronized with the frequency pattern of the received signal, thereby producing at the output a dehopped signal at a fixed difference frequency. Decryption is likewise accomplished by a synchronized PN generator. Further details of these processes are given below.

Encryption provides protection against eavesdropping and message manipulation, deletion, and replay. There are a number of modes of operation for encryption systems. The only encryption mode of interest here is the one for which the keystream is independent of the plaintext. Independently keyed ciphers are known as synchronous ciphers since they require synchronization between the locally generated keystream and the ciphertext for successful deciphering. Most other encryption modes are self synchronous but do have other problems, such as error extension (or error propagation), or may be otherwise lacking in certain areas of security. A simple form of this independently keyed cipher system, better known as a output feedback mode (OFB) or key-autokey, is shown in Figure 2. Here the output of the cipher machine is fed back to the input of the cipher machine. The data is multiplied on a bit-by-bit basis by the output of the cipher machine to produce the cipher text. The inverse process occurs in decryption, provided that the PN codes involved are identical and properly aligned in phase.

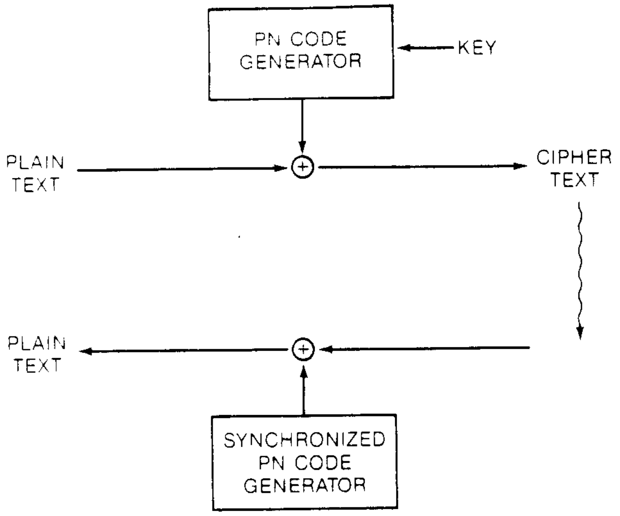


Figure 2. Synchronous encryption/decryption process

All threats mentioned in Table 1 can be protected against through the use of broadband carriers. A broadband carrier is defined in this paper as one in which the carrier's frequency, phase, or time of transmission is determined by a pseudorandom sequence. Broadband carriers considered here fall into three distinct categories: a frequency-hopping carrier, a time-hopping carrier, and a phase hopping carrier. The frequency-hopping carrier may be generated in the manner shown in Figure 3. The output is a signal whose carrier is hopped about in frequency in an apparently random manner but which, in reality, is determined by the output PN sequence generator, which is a deterministic process. This constant, apparently random, hopping in frequency of the signal, as illustrated in Figure 3, makes the successful execution of the previously mentioned threats much more difficult. The number of frequencies possible is n and the frequency used is determined from m bits, of the PN sequence where $2^m = n$, making prediction of the next frequency to be used extremely difficult.

The phase-hopping carrier is typically a system where the phase of the carrier is either zero or 180 degrees, depending upon whether the PN sequence bit is a zero or a one as shown in Figure 4. The PN sequence typically runs at a much higher rate than the data, usually 100 to 1000 times, with a correspondingly wider signal spectrum than that expected for the data alone. This spectrum is more difficult to detect or identify since it looks like noise, is broadband, and can be successfully transmitted between two friendly,cooperating terminals at carrier power-to-noise-density ratios much lower than required in conventional systems where bandwidths are conserved.

In the case of a time-hopping carrier, the time slots for transmission can be thought of as slots with many cells, only one of which will contain the transmission. The cell to be used in each slot is determined by the state of the PN sequence, thus appearing to be selected at random, as seen in Figure 5. A jammer, for example, must waste power by transmitting his jamming signal at times when there is no signal to jam. All threats to this type of communications system are made less effective due to the uncertainties associated with transmission times. There can also be hybrids of these three systems. For example, a time hopper which is also frequency hopped would potentionally be more resistant to all threats considered here.

CODE ALIGNMENT

In each of the protection techniques discussed above, the long, locally generated, pseudorandom sequence was assumed to be synchronized, or in phase, and tracking the incoming signal. As mentioned before, it is not always the case that the codes will be tracking or even close to being in phase synchronization. This might be the case because the receiver's operator has just turned on his radio while the network has been operating and using the code for a long time, possibly days; or the user's receiver might have malfunctioned, lost power or for some other reason need restarting. In any case, there can be instances where the user's code will be out of phase by a relatively large amount of time or, equivalently, a very large number of bits. The process of achieving coarse phase synchronization, which is a bit-by-bit search, can be prohibitively time consuming.

Alignment of long codes may be done in a three-step process. Initial code alignment is defined in this paper as bringing the locally generated code close to phase alignment using external information, such as a time reference. Initial alignment is followed by coarse code alignment, which is the process of achieving alignment within plus or minus of one bit, where fine alignment or tracking, the third step, can be implemented using tracking circuits. (In spread-spectrum systems, it is common to call one bit of a PN sequence a chip with many chips making up one bit of data. In this paper, however, one symbol of the PN sequence will still be referred to as a PN bit, or simply a bit). Tracking circuits typically keep the codes in phase by a few percent of one bit. Tracking is necessary because of changing delays due to moving platforms supporting the communications

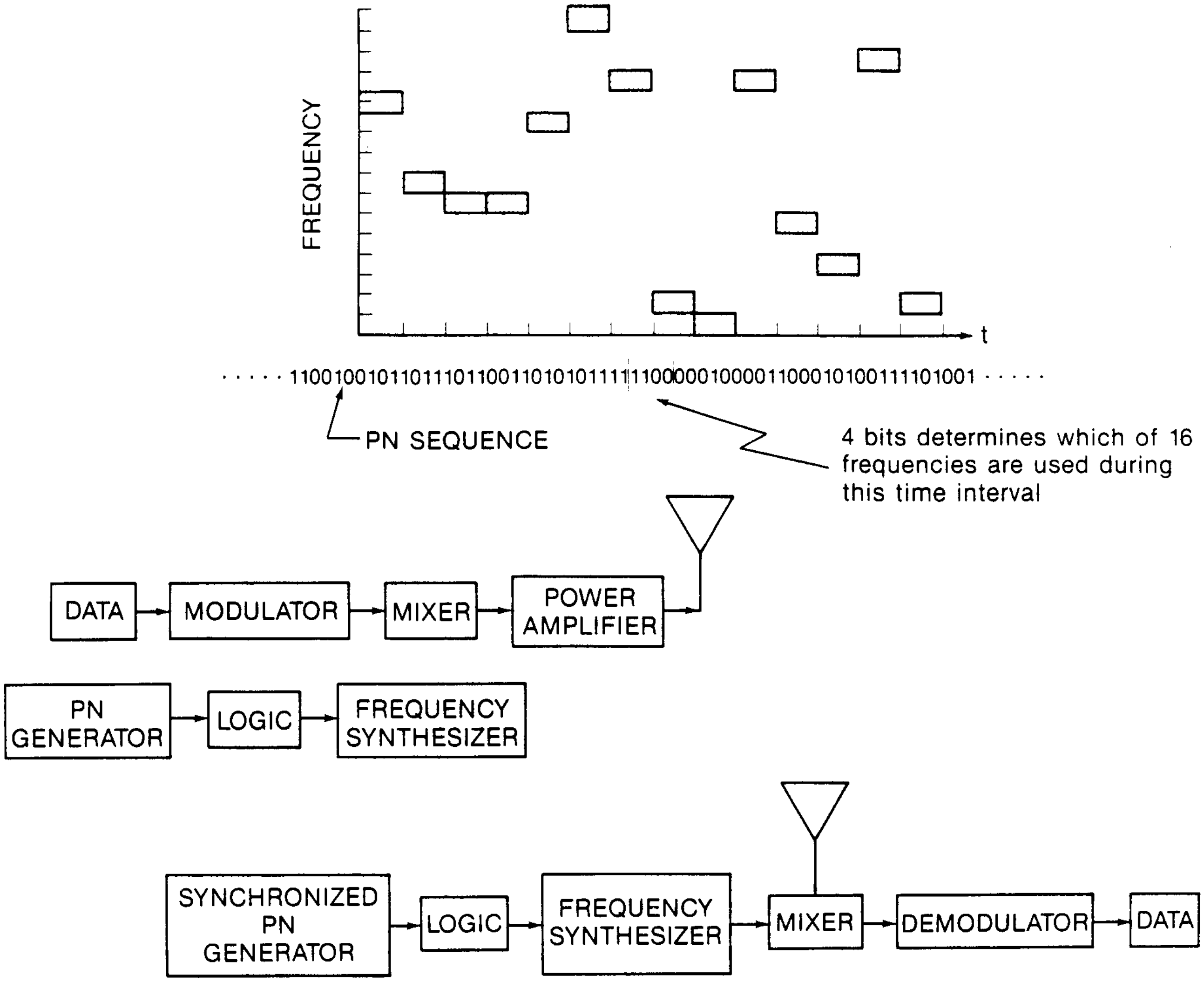


Figure 3. Frequency Hopping System

terminals and changes in the propagation paths due to environmental effects. Figure 6 illustrates these three steps. In Figure 6a, the PN sequence as generated at the transmitter is shown. It is a long code with a period of perhaps hours or even days and has been running continuously; since, a previously agreed upon start time and initial state and is being clocked with a suitably stable frequency source. The state of the PN sequence at any time can therefore be determined by knowledge of the time elapsed since it began running and the details of how it is generated, i.e., the keystream generator's initial state and construction. The transmitted keystream is presented to the receiver in the form of frequency, phase, or time of transmission changes and delayed in time by the intervening equipment delays and propagation delay as shown in Figure 6b. Figure 6c shows the locally generated sequence with an alignment error of approximately one second, a small time uncertainty easily achieved by reference to a good quality quartz wrist watch. Figure 6d shows the alignment error reduced by reference to a better time source, such as that broadcast by WWV or GOES. The alignment error is shown in Figure 6e to be further reduced to plus-or-minus one bit through a bit-by-bit search, as indicated by a correlation process where correctly decoded data appears in the baseband. The final phase of fine alignment or code tracking is shown in Figure 6f.

Continuing with the process illustrated in Figure 6, let us again assume that the receiver's internally generated code is not aligned or in

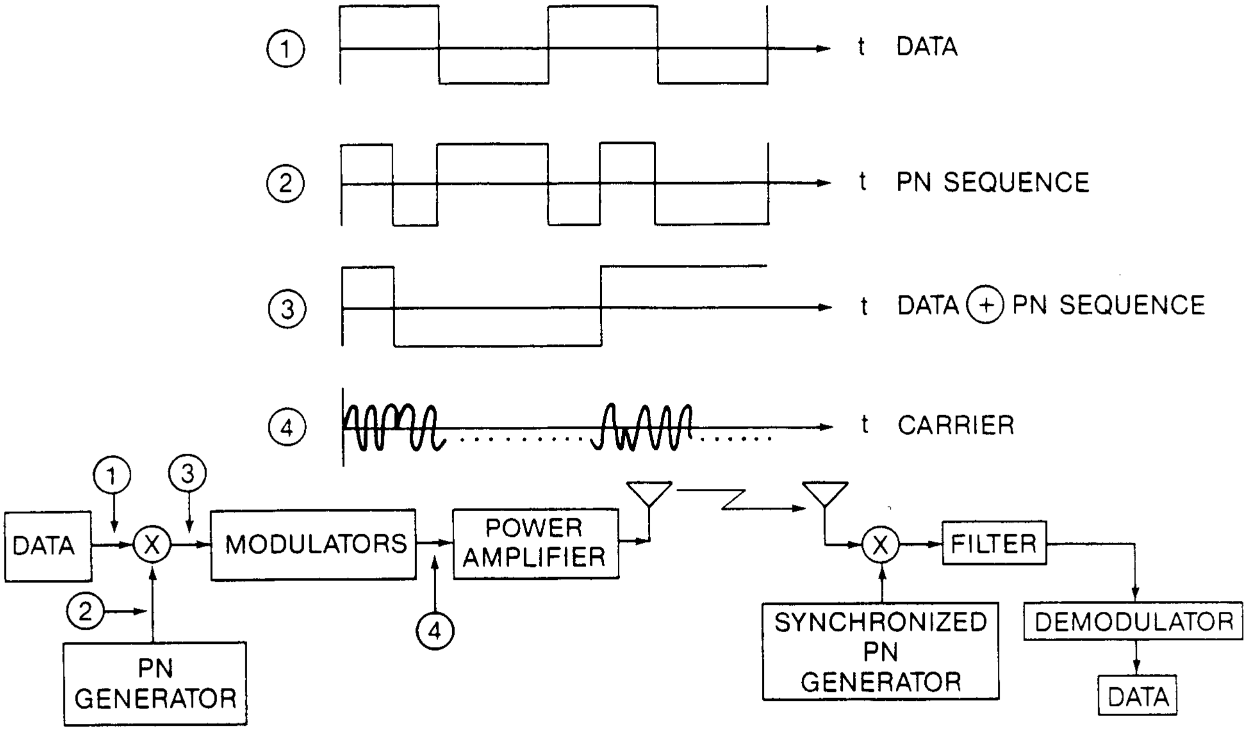


Figure 4. Phase Hopping System

phase with the transmitted code as received. Also assume that the two codes are misaligned by no more than one second and that the PN code rate is one million bits per second. The code misalignment is then, at maximum, one million bits. A search for coarse alignment could, at maximum, extend over two million half bits, assuming we increment in half-bit steps. If each search and integrate operation took ten milliseconds, then the entire search process could take more than one hour. A better approach would be to initially synchronize the codes to one millisecond using WWV or WWVH as references or to a even greater accuracy of 50 microseconds as can be obtained from the GOES or TRANSIT satellites. These levels of initial synchronization would narrow the maximum search time for coarse synchronization to 40 seconds with WWV or WWVH and 2 seconds when using the GOES or TRANSIT satellites. Remember that the above discussions assume that the equipment and propagation delays have been properly accounted for with relatively small uncertainties. These search times are also a function of the carrier power-to-noise density ratios. The calculations presented above are typical of signal levels for an existing satellite-to-earth transmission link.

TIME REFERENCES

Obtaining and maintaining accurate time (UTC) generally means one has a clock and some means to set it. The choice of clocks to use is a function of the precision desired and time interval between clock updates using some external source. The usual means of setting the clock is to use a receiver designed to receive one of the many official time broadcasts or navigation signals which contain time information that can be related to UTC time. Which system(s) one chooses to use depends upon how many resources one is willing to devote to the task, geographical location, signal availability and reliability required, an accuracy. Since it is unusual that any one source of time will be totally suitable, many find it desirable to have the capability to obtain time from a number of different sources--a particularly important feature during times of hostilities when some of these sources may be put out of operation by enemy actions.

Table 2 shows some of the important characteristics of the more readily available and useful sources of time. The first source on the table is the high frequency radio broadcasts of WWV and WWVH, both operated by the National Bureau of Standards (NBS). The NBS high frequency signals are available at 2.5, 5.0, 10.0, and 15.0 MHz from both WWV and WWVH, which are located

SYSTEM ISSUE	WWV *or* WWVH	Loran-C +WWV	Navy Navigation *Satellite* System (Transmit)	Geostationary Operational Environmental Satellite (GOES)	NAVSTAR Global Positioning System (GPS)
ACCURACY	1 ms	1 μs (ground wave)	25 μs	50 μs	0 25 μs (C/A code only)
UNAMBIGUOUS UTC TIME CODE	Yes	None	No (partial)	Yes	Yes
COVERAGE	Global	See Figure 8	Global	Western Hemisphere (Figure 10)	Global
STATUS	Operational	Operational	Operational	Operational	Fully operational by 1988-1989
OPERATIONAL TIME	Continuous	Continuous	20 minute passes every few hours—requires internal clock to "flywheel" when satellite not in view	Continuous	14-18 hours per day—will be continuous when fully operational
RECEIVER SYSTEM COSTS	$100-1000	$12.000	$12.000-21.000	$2500-5000	$25.000—cost expected to decline significantly during next 5-10 years
OPERATOR	NBS	Department of Transportation	*Department of Defense*	U.S *Department of* Commerce/NBS	Department of Defense
ANTENNA PACKAGE SIZE	*whip < 1 meter*	loop 1 meter in diameter or whip	whip < 1 meter	< 1 meter	3 cm high, 2 cm diameter
LONG TERM PROSPECTS	Excellent	GAO recommends use of GPS when fully operational	Likely phase out when GPS operational	Excellent	—may be *degraded* or *denied during* national emergencies
OTHER COMMENTS	Similar services offered by numerous other countries	skg-wave coverage may provide 50 μs over greater areas	Receiving system requires user to select satellites for use.	Totally automatic operation of *receiving system*	Subscription fees have been suggested

Table 2

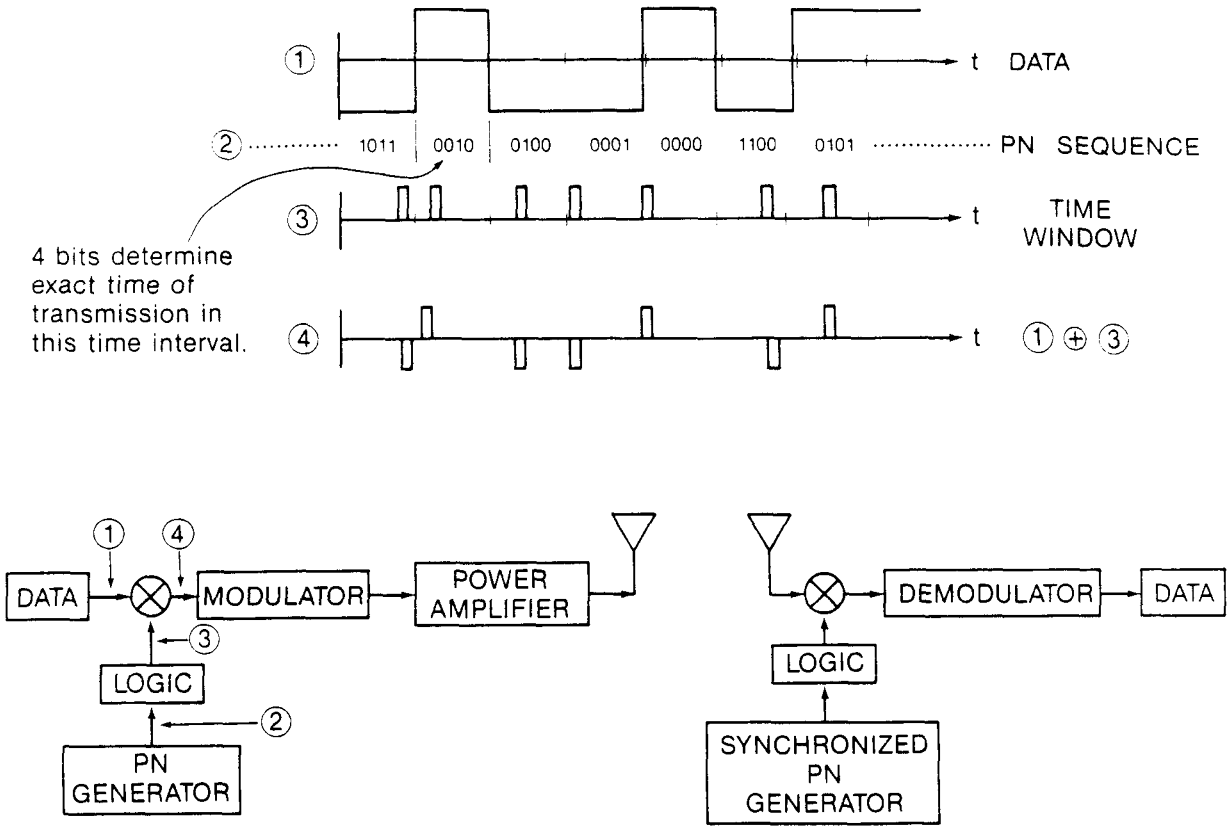

①
t
DATA
② 1011 0010 0100 0001 0000 1100 0101 PN SEQUENCE
③
t
TIME WINDOW
4 bits determine exact time of transmission in this time interval.
④
t
① ⊕ ③
DATA
MODULATOR
POWER AMPLIFIER
LOGIC
PN GENERATOR
DEMODULATOR
DATA
LOGIC
SYNCHRONIZED PN GENERATOR

Figure 5. Time Hopping System

near Fort Collins, Colorado and Kauii, Hawaii. Additionally, a time signal is also available at 20.0 MHz. from WWV only. These signals are generally available throughout the world using relatively inexpensive equipment. Voice announcements of time and a time code are included. Many other countries also offer similar HF time services, many on these same frequencies, with different formats and in many cases only during limited hours of the day. The accuracy of high frequency time signals is generally about one millisecond, provided that the propagation times are correctly determined--usually by calculation. Figure 7 illustrates the format of WWV and WWVH.

LORAN-C stands for LOng RAnge Navigation and is a hyperbolic navigation system operating at 100 kHz. For timing use, good ground wave coverage is available in large areas of the Northern Hemisphere. An approximate ground wave timing coverage is illustrated in Figure 8. The timing coverage is considerably greater than that for ground wave navigation coverage (not shown), since only one station needs to be received rather than three, as required for navigation. Using the ground wave, time accurate to one microsecond is possible provided that UTC time accurate to five milliseconds is initially available for resolving ambiguities. This additional requirement is necessary since an unambiguous time message is not included. The use of WWV for this initial timing purpose is quite common.

The U.S. Navy's Navigation Satellite System or, as it is better known, Transit is a system of five or six low-altitude, polar orbiting satellites providing navigation signals. Due to the nature of the system the satellites also provide time information in the navigation message that is required for proper processing of the navigation data. These satellites generally are in view of any point on the earth's surface for a few minutes up to as many as 20 minutes, with intervals between satellite passes of two to three hours. The orbits are illustrated in Figure 9. The time signals are accurate to 25 microseconds provided that the time is initially known to within 15 minutes of the UTC time scale, as required to resolve ambiguities due to the incomplete time message.

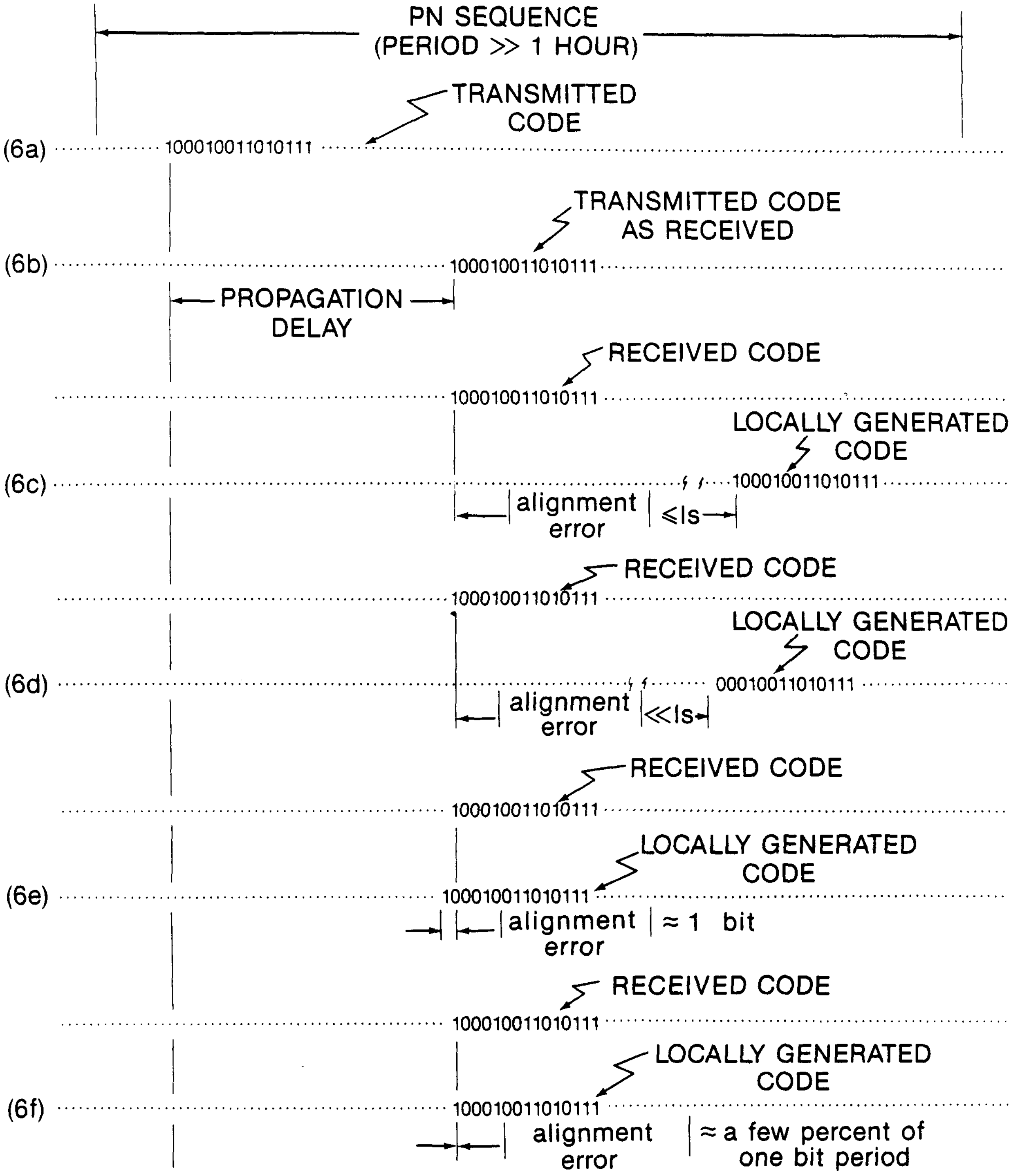
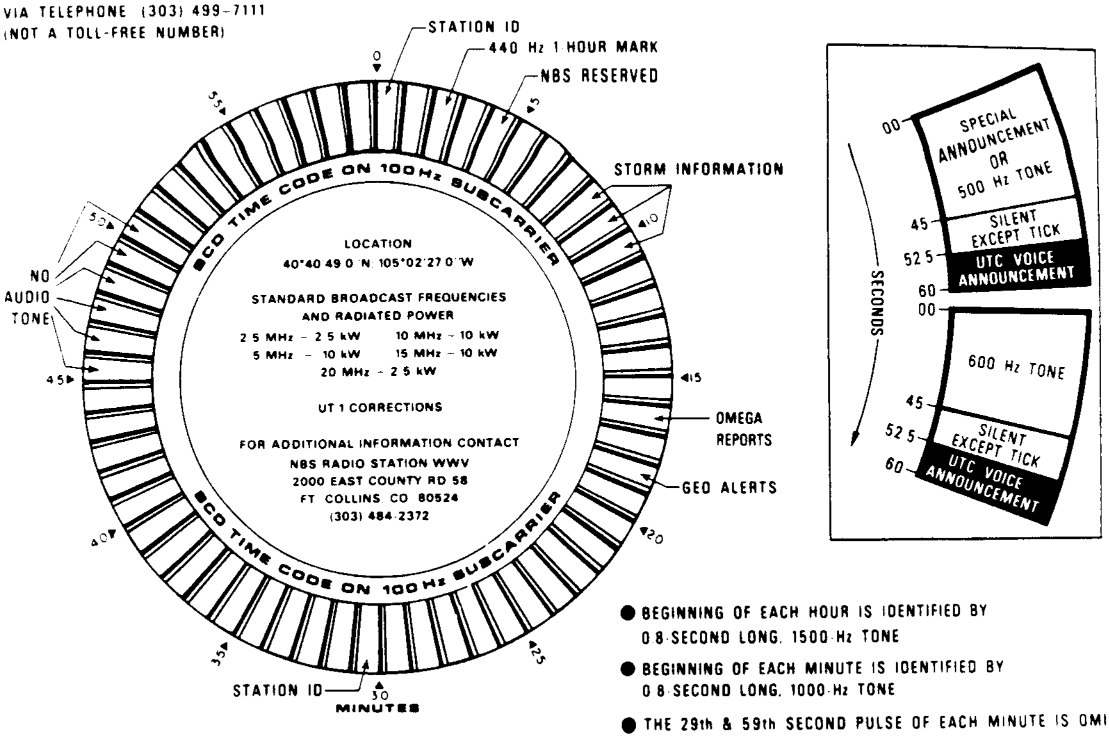


Figure 6. States of Code Alignment

WWV BROADCAST FORMAT

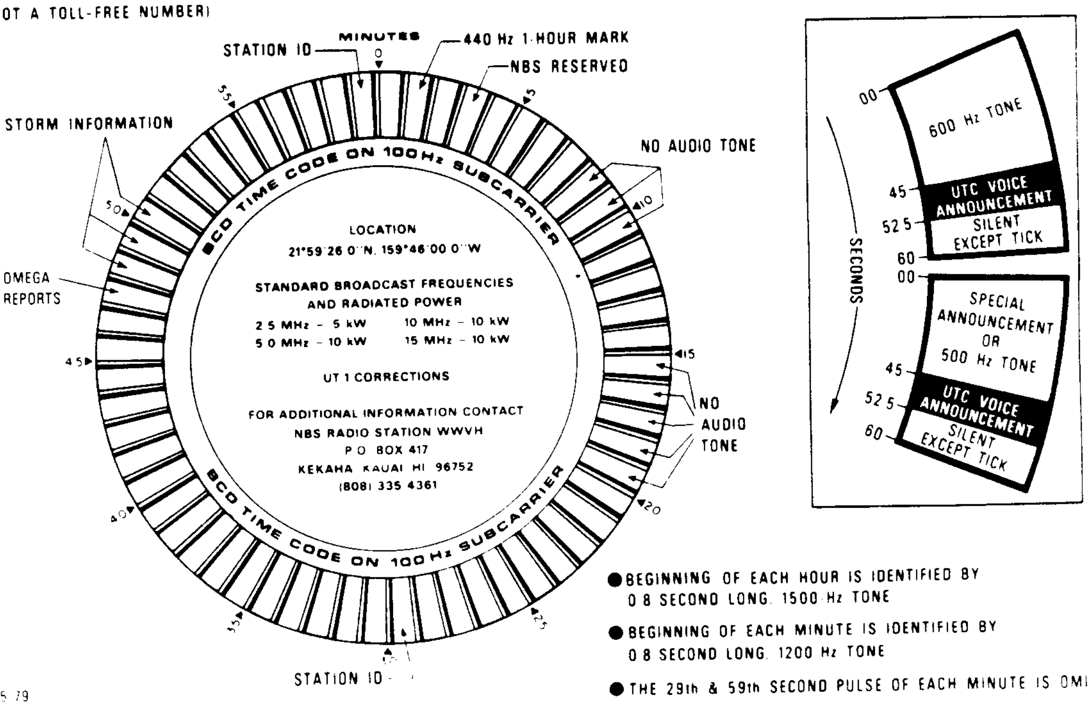
VIA TELEPHONE (303) 499-7111
(NOT A TOLL-FREE NUMBER)



- ● BEGINNING OF EACH HOUR IS IDENTIFIED BY 0 8-SECOND LONG. 1500-Hz TONE
- ● BEGINNING OF EACH MINUTE IS IDENTIFIED BY 0 8-SECOND LONG. 1000-Hz TONE
- ● THE 29th & 59th SECOND PULSE OF EACH MINUTE IS OMITTED

WWVH BROADCAST FORMAT

VIA TELEPHONE (808) 335-4363
(NOT A TOLL-FREE NUMBER)



- ● BEGINNING OF EACH HOUR IS IDENTIFIED BY 0 8 SECOND LONG. 1500 Hz TONE
- ● BEGINNING OF EACH MINUTE IS IDENTIFIED BY 0 8 SECOND LONG. 1200 Hz TONE
- ● THE 29th & 59th SECOND PULSE OF EACH MINUTE IS OMITTED

5 79

Figure 7. The Hourly Broadcast Schedules of WWV and WWVH

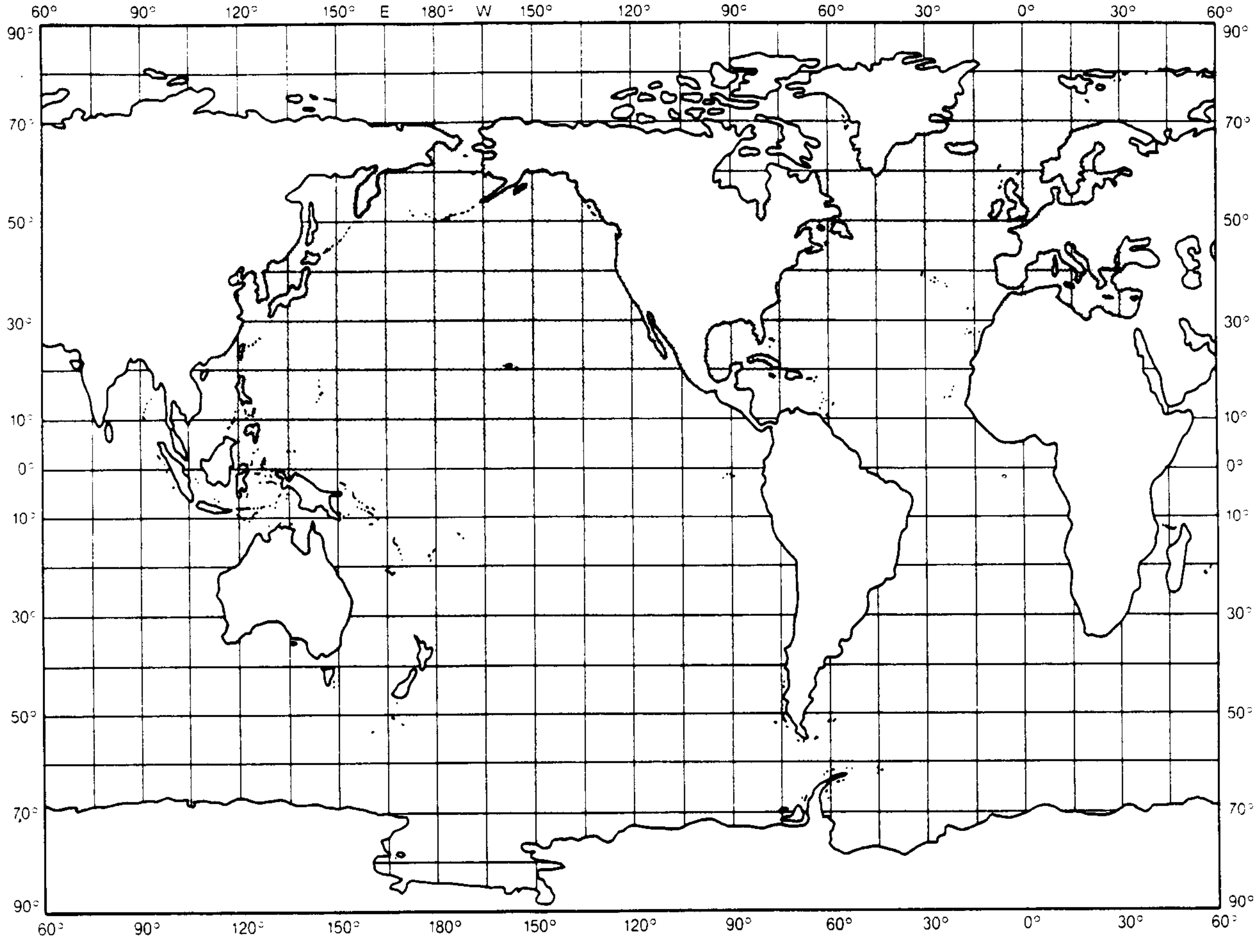


Figure 8. Loran-C, Ground Wave Timing Coverage

The GOES satellites are two U.S. meteorological satellites in geostationary orbit which also provide time signals. These time signals are generated by NBS and relayed through the satellites, which are located on the equatorial plane at 135 and 75 degrees west longitude. From these locations a continuous time signal is available to North and South America and the major parts of the Atlantic and Pacific Oceans. The coverage is shown in Figure 10. These signals are generally accurate to 50 microseconds and available in the form of a continuous digital time code.

The NAVSTAR Global Positioning System (GPS), prior to the cancellation of all scheduled shuttle launches after the loss of the Challenger with three Navstar satellites aboard, was to be fully operational by 1988 or 1989 with 18 satellites in 12-hour, highly inclined orbits. At present there are seven satellites providing limited service. The full constellation of satellites will broadcast navigation and time information on a continuous basis to the entire earth. These satellites, unlike LORAN-C and Transit, provide an unambiguous time message that can be related to UTC. The time signals are to be freely available to civil users on an international basis at the highest level of accuracy consistent with U. S. national security interests. Recent statements by the DoD appear to place this level at one-quarter microsecond by using the C/A code. The signals are available on two frequencies using two codes, the coarse/acquisition or C/A code and the precise or P code. Higher levels of accuracy will be possible using both the C/A code and the P code. The P code, however, will be subject to restricted access.

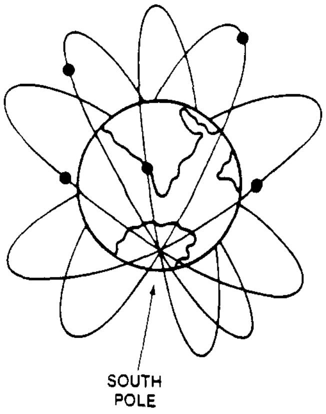


Figure 9. Five Transit Satellites in Polar Orbit

CONCLUSIONS

The use of broadband carriers and encryption techniques to protect communications from specific threats can benefit from accurate time. We have shown how search times needed to align codes can be reduced from hours to seconds when the accuracy with which absolute time is known is improved from a few seconds to 50 microseconds. Sources of accurate time were discussed in terms of accuracy, cost, geographical location and signal availability.

REFERENCES

1. NBS Special Publication 432, "NBS Time and Frequency Dissemination Services", Sandra L. Howe, editor, NBS, Boulder, Colorado (September 1979).

2. NBS Special Publication 559, "Time and Frequency Users' Manual", George Kamas and Sandra L. Howe, editors, NBS, Boulder, Colorado (November 1979).

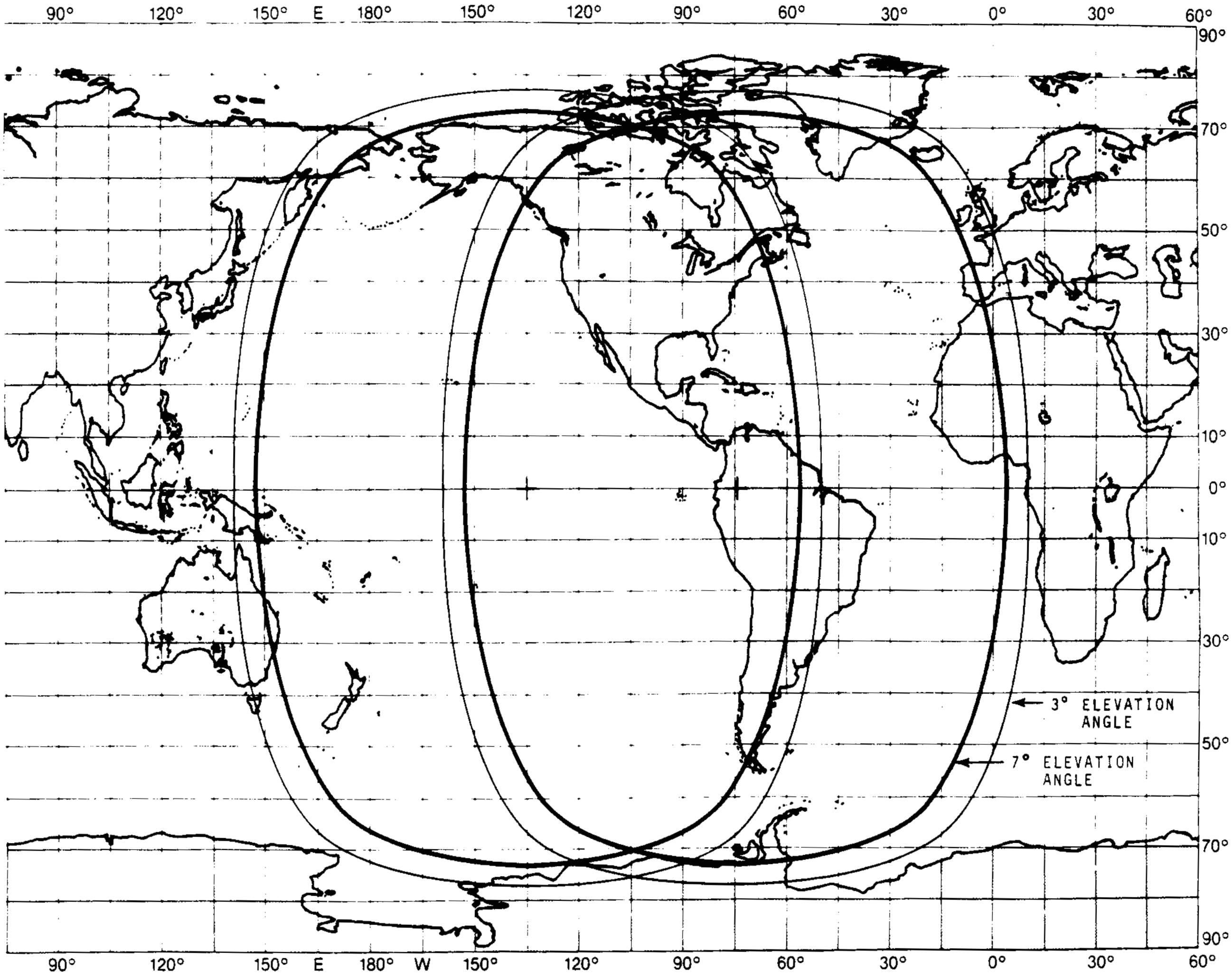


Figure 10. Coverage of GOES Satellites