Secure Voice for Mobile Satellite Applications

Arvydas Vaisnys, Jeff Berner
Jet Propulsion Laboratory
4800 Oak Grove Drive
Pasadena, California 91109
Phone: 818-354-6219
FAX: 818-393-4643

ABSTRACT

This paper describes the initial system studies being performed at JPL on secure voice for mobile satellite applications. Some options are examined for adapting existing STU III secure telephone equipment for use over a digital mobile satellite link, as well as for the evolution of a dedicated secure voice mobile earth terminal (MET). The work has included some laboratory and field testing of prototype equipment.

The work is part of an ongoing study at JPL for the National Communications System (NCS) on the use of mobile satellites for emergency communications. The purpose of the overall task is to identify and enable the technologies which will allow the NCS to utilize mobile satellite services for its National Security Emergency Preparedness (NSEP) communications needs. Various other government agencies will also contribute to a mobile satellite user base, and for some of these, secure communications will be an essential feature.

BACKGROUND

There is a trend toward digital implementation of voice in most mobile communications services. This includes the United States versions of Cellular Telephone, Mobile Radio, the land mobile satellite service (LMSS), as well as European developed systems such as CT2, and the various international mobile satellite services (MSS). While not necessarily the case for first generation systems, the data rate for future digital voice systems appears to be converging toward a 4.8 kbps compromise between quality and bandwidth requirements. A leading candidate for a voice encoding standard in the U.S. is the 4800 bps Code Excited Linear Predictive (CELP) voice coder defined in Proposed Federal Standard 1016.

Secure voice capability would be a useful addition to most mobile, small terminal, communications services in applications such as disaster communications and others where privacy may be important. Coincidentally, the mobile earth terminals (MET's) for all these services contain very similar functional blocks, which works in favor of a common secure voice interface. The options to be considered are whether the secure voice capability should be added as an external interface to the MET, or built into the MET.

MET FUNCTIONAL ELEMENTS

A generic MET contains the following elements: a voice codec, a coder/decoder for forward error correction (FEC), a modem, and a transceiver, as shown in block diagram form in Figure 1. In addition to these basic functions there is usually circuitry for call set-up, and an interface for external digital data, most likely at point A on the block diagram.

STU III FUNCTIONAL ELEMENTS

The STU-III (Secure Telephone Unit III) is a communications terminal unit that connects to the Public Switched Telephone Network (PSTN) and allows the user to make secure telephone calls.

In the non-secure mode of operation, a STU III operates as an ordinary telephone, using analog voice and all the signalling of plain old telephone service (POTS).

In the secure mode, the voice signal is digitized and compressed to a rate of 2.4 kbps using a LPC-10 algorithm. The compressed voice signal is then encrypted and is output on a subcarrier in V.26 format. During the secure call set-up there is also some signalling and echo canceler control using 2100 Hz tones, as well as digital hand shaking.

A functional block diagram of the present generation STU III is shown in Figure 2. It should be noted that the STU III has a key element of a MET, the voice codec, but that certain signal combinations, such as digitized clear voice and the encrypted voice data stream at baseband, are not available at the output.

The next generation STU III's, which will become available in late 1990, will include 4.8 kbps voice using the CELP voice coder defined in Proposed Federal Standard 1016. In the secure mode the output signal will be in V.32 format.

STU III INTERFACING

To interface the present generation STU III to a digital link, therefore, requires that its analog signals be digitized externally and the V.26 signal be restored to baseband by means of another V.26 modem. This can be accomplished by means of an adapter at both the mobile and the earth station ends of the link. Companies such as Electrospace, Inc., of Richardson, Texas, Stanford Telecommunications, Inc. of Santa Clara, California, and some of the STU III vendors have worked on the development of such an adapter.

Three options exist for interfacing the next generation STU equipment to a digital link. These options are for the MET end of the link. In all cases an adapter will still be needed at the satellite base station to provide the conversion between the digital data stream and the analog signals required by the PSTN.

One option is to develop a similar adapter, capable of operating at 4.8 kbps. Such an adapter would provide essentially identical functions at either end of the link.

The second is to develop a STU III version that provides the digital encrypted voice signal as well as digitized secure call set-up signals as direct outputs. This would provide a simpler interface to the MET. One question to be resolved is whether the STU III or MET voice codec would be used during clear voice operation.

The third option is to develop an integrated STU III MET. The secure call set-up and encryption functions could be provided as an optional module to a common MET.

THE LMSS CHANNEL

In clear line-of-sight conditions, the LMSS channel can be impaired by multipath signal components and vehicle motion induced Doppler. The most serious problem, however, is caused by signal blockage due to roadside obstacles. An example time plot of satellite signal strength data, measured in a fairly benign rural environment, is shown in Figure 3. The signal dropouts are caused by trees, telephone poles and other obstacles, and can last significant fractions of a second at normal driving speeds. Signal loss can easily be greater than 10 dB and providing link margin to overcome this phenomenon under all conditions is impractical.

OPERATION OVER THE LMSS LINK

Links over this type of channel are generally protected with some type of FEC coding, including time interleaving to break up the signal dropout induced error bursts prior to decoding.

The amount of time interleaving that is practical in a duplex voice link, however, cannot protect the link from most of these dropouts. It is therefore important that the system be able to resynchronize rapidly. In more difficult environments such as suburban and urban locations, operational problems such as complete loss of link may result. For STU III operation, the signal dropout problem may result in frequently dropping out of the secure mode. Reestablishing the secure mode must be initiated manually and can become burdensome if needed often enough.

Link error protection and signal dropout mitigation are thus very important, especially while operating a secure link. This however can only be done to a limited extent. Certain environments will still be difficult to operate in, and this must be understood by potential users of the system.

ERROR PROTECTION

Error protection can be applied in layers. The MET FEC coder will apply an outer code to the composite data stream. The more critical signals, such as those involved in the call set-up process can be further encoded. Further protection of the critical bits of the voice codec output is also planned in some systems. For example, the proposed CELP codec employs an error correcting Hamming code within the voice frame.

In a non-secure voice MET there will be two basic phases of operation; the call set-up and the conversation phase. Call set-up may take place end to end over a dedicated request channel, or additional routing through the PSTN may be allowed by dialing over the assigned voice channel. Dial tones must of course be converted to digital codes, but they are generated so slowly that they can be reliably encoded.

In the case of a secure MET using a STU III, signal structure is even more complex because there are four additional signalling phases. These consist of a status phase, a crypto variable exchange phase, a crypto synchronization data exchange phase, and finally, the secure communications phase. These are described briefly below. More detailed information on the structure of these signals is contained in [1] and [2].

The status phase is used to set up the secure link. The secure call is initiated by one of the users pressing the "secure" button on the STU-III. That unit is now known as the initiator unit. The initiator sends a 2100 Hz tone (the 2100 Hz tone disables the echo suppression and echo cancelers on the telephone line). After some hand shaking, the initiator turns off the 2100 Hz tone. The two units then send signal patterns that are used to train the modem echo cancelers and the modem equalizers. This completes the first stage.

The crypto variable stage exchanges status and FIREFLY protected messages (FIREFLY is the encryption scheme). This is done to establish a cryptographic variable that is used by the STU-III's. The STU-III's perform several checks on the bits, including a parity check. If the data fails any of the checks, the secure call is terminated; these bits are not error correction coded. Next, the STU-III's exchange Random Component Cipher (RCC) messages. The RCC is FIREFLY encrypted and BCH encoded. Upon receipt, the RCC is BCH decoded and decrypted, and processed. If the message fails any of the processing parity checks, the call is terminated. Otherwise, the call proceeds to the next phase.

The STU-III's next exchange Crypto Synchronization (CS) messages. This occurs both at call set up and any time the call is interrupted. The CS is used to coordinate the selection of the secure mode, to align each STU-III's receive key generator to the other unit's key generator, and to coordinate the start of the secure transmission. Once the units are in sync, secure communications can begin. This is indicated by the STU-III "scrolling" messages about the CIK classification across the LCD display and then displaying the message "SECURE".

Once the link is secure, the user can end the call by either hanging up, which disconnects the link between the STU-III's, or he can push the "Non-Secure" button, which returns the units to non-secure communication. If the units drop out of sync, the CS messages are sent again.

As was mentioned previously, the outer coder will use time interleaving in combination with some type of error correcting code. The JPL MSAT project has chosen a trellis code for this application. Golay codes have been studied for this application in Land Mobile Radio [3]. The type of coding and modulation to be specified by the American Mobile Satellite Corporation (AMSC) and other LMSS system providers has not yet been specified.

MSAT MET DESIGN

The MSAT MET was designed with a combination of coding and modulation which provides robust performance over a LMSS channel, yet minimizes bandwidth requirements. The FEC and modulation functions are implemented within the modem and use time interleaving and combined rate 2/3 trellis coded modulation (TCM)/eight phase differentially encoded phase shift keying (8DPSK). This allows a 4.8 kbps data stream to utilize a 5 kHz wide channel.

The time interleaving helps break up the error bursts caused by signal drop-outs. Another feature of the modem is the use of differentially coherent demodulation. This and a very stable clock results in instantaneous recovery after a signal dropout. The ability of the symbol clock to coast through long signal dropouts greatly diminishes the need for interleaver and voice codec resynchronization.

PROTOTYPE SYSTEM TESTING

A prototype system was tested in mid 1989 by JPL, using MSAT equipment and a developmental model Digital Transmission Interface (DTI) supplied by Electrospace, Inc.

The test set-up consisted of a pair of STU III's, DTI's, and MSAT MET's (with the voice codecs bypassed). The STU III output data rate was doubled to 4.8 kbps by bit stuffing in order to match the data rate of the MSAT equipment. No additional error protection, other than provided by the MSAT system, was implemented due to schedule constraints.

Testing was accomplished in two stages, first in the laboratory, then in the field in Australia using the Japanese experimental satellite ETS V. Field testing in Australia was done in conjunction with a scheduled MSAT-X field test.

Testing in the laboratory was accomplished using a satellite channel simulator which can be used to add Gaussian noise, produce signal fading by introducing multipath signals, and simulate other signal impairments. The actual measured satellite signal strength data of Figure 3 was also used to drive the simulator and ensure that the system would work in the field.

Minimum signal to noise ratio conditions for secure call set-up and secure call maintenance were investigated. The secure call set-up phase was more sensitive to channel impairments. Once a secure call was established, the signal to noise ratio could be lowered and the link was more tolerant of impairments such as signal dropouts.

In Australia, a secure link was set up and maintained over a satellite link which was operating with very little margin and was affected by multipath and blockage by roadside obstacles. Details of the testing are available in [4].

SUMMARY AND CONCLUSIONS

Several options exist for incorporating secure voice into LMSS MET's. Ideally, STU III functions should be incorporated directly into LMSS MET equipment. Special attention must be paid to error protection of the signalling that is part of secure call set-up and operation.

The LMSS channel is very difficult to quantify because its characteristics can vary so much from region to region. A great deal of propagation data has been gathered by both the JPL MSAT Project and NASA Propagation Program. It is available to anyone working in the area of mobile satellite MET design. Use of this data will allow the testing of proposed modulation and error protection techniques under realistic operating conditions.

ACKNOWLEDGEMENT

The research described in this paper was carried out by the Jet Propulsion Laboratory, California Institute of Technology under a contract with the National Aeronautics and Space Administration.

REFERENCES

1. *FSVS-210, Revision E, FSVS Signaling Plan-Interoperable Modes*, 26 February 1988.

2. *FSVS-220, Revision B, FSVS Terminal Performance Specification*, 26 February 1988.

3. **Rahikka, D. J., Tremain, T. E., Welch, V. C., Campbell, Jr., J. P.**, CELP Coding for Land Mobile Radio Applications, *ICASSP'90*, Albuquerque, New Mexico, April 3-6, 1990.

4. **Berner, J., and Vaisnys, A.**, *Evaluation of Secure Communications Equipment Over a Mobile Satellite Link*, November 30, 1989, Internal JPL Report.

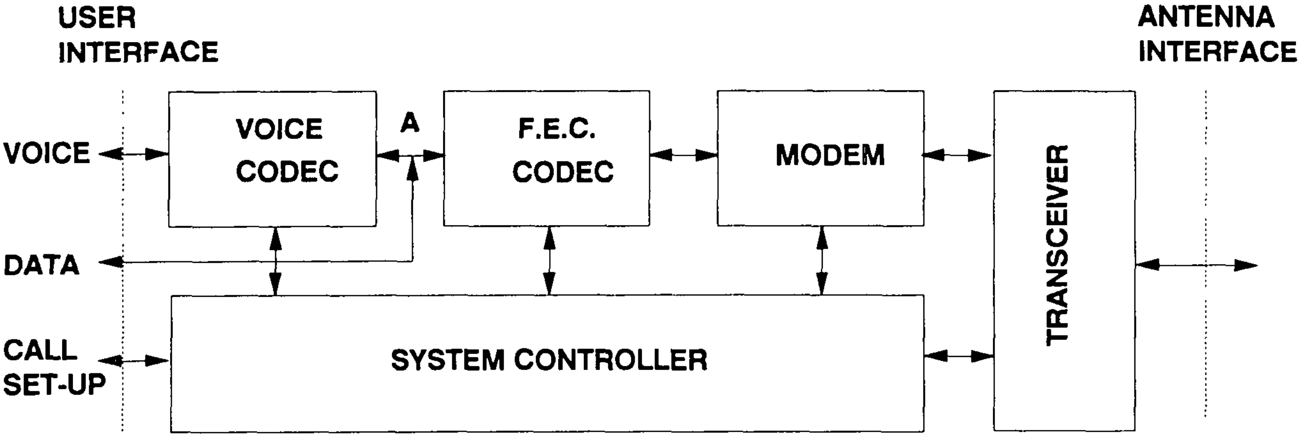

Figure 1. MET functional block diagram

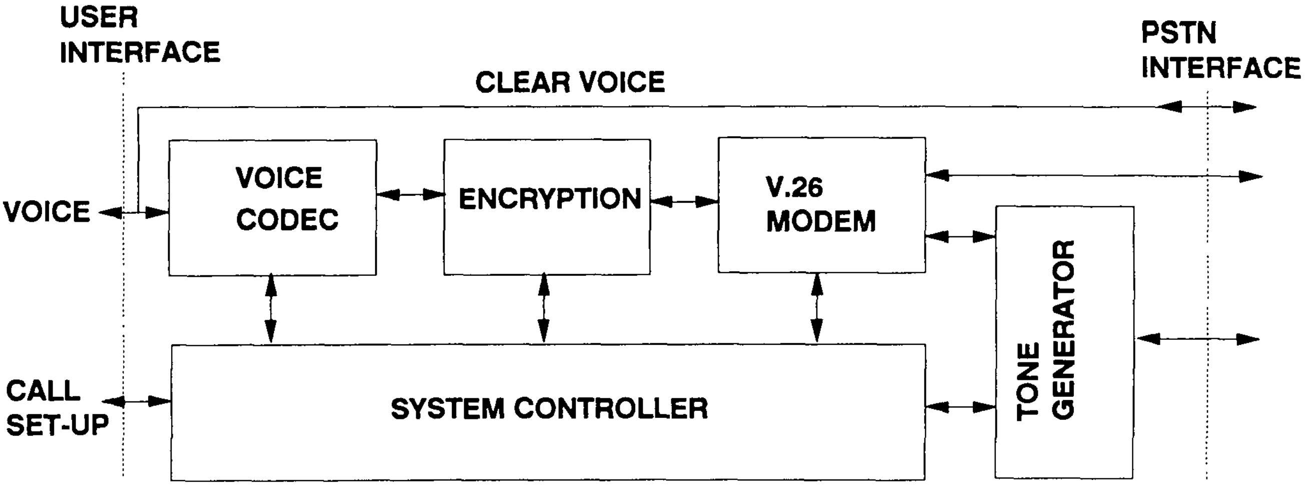

Figure 2. STU III functional block diagram

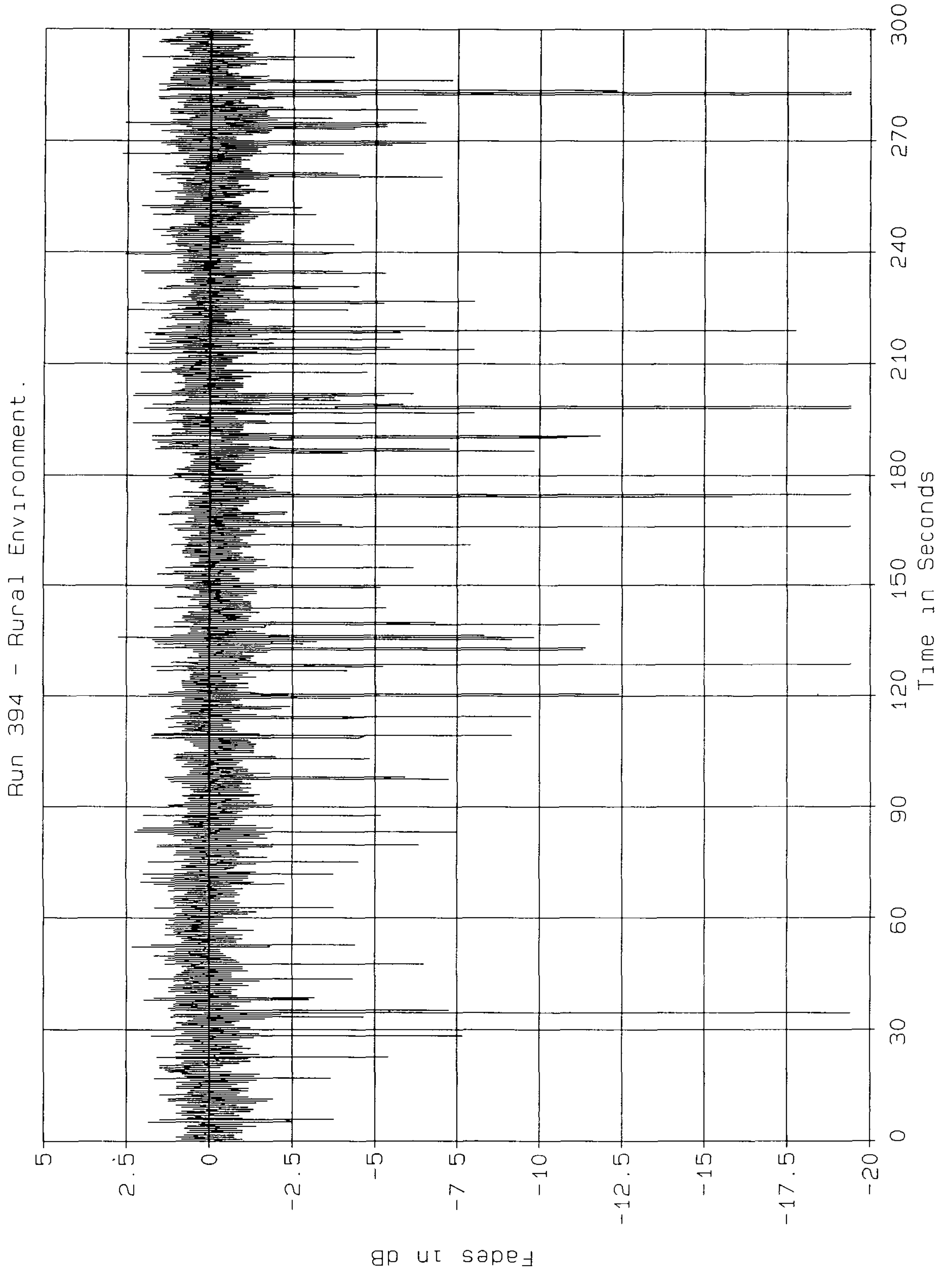

Figure 3. ETS V Satellite signal strength measurement.