IMPLEMENTATION OF SECURE VOICE (STU-III) INTO THE LAND MOBILE SATELLITE SYSTEM

John J. O'Connor, Jr.
National Communications System
701 South Courthouse RD, Arlington, VA 22204

Arvydas Vaisnys
Jet Propulsion Laboratory
4800 Oak Grove Drive, Pasadena, CA 91109

1 June 1992

ABSTRACT As part of its responsibilities, the National Communications System (NCS) investigates the use of new satellite technologies to satisfy National Security and Emergency Preparedness (NS/EP) requirements. One effort is the incorporation of a secure telephone unit (STU-III) based secure voice capability into the land mobile satellite service (LMSS) of the United States. As part of this effort, the NCS funds a task at JPL to perform system studies, analyses, and field trials of prototype equipment. The first experiment involving STU-III's in a mobile satellite application was accomplished by JPL in 1989 in Australia, using the Japanese experimental satellite ETS V. Subsequent work on this task includes laboratory testing of recently developed STU-III interfaces, refinements to mobile satellite link characteristics simulation, and interaction on system architectural issues with the American Mobile Satellite Corporation (AMSC), the licensed provider of LMSS to the United States. This paper describes the projected role of LMSS secure voice in satisfying NCS NS/EP requirements, and the issues remaining to be resolved before secure voice becomes an integral part of AMSC's services which are projected to commence in 1993.

1.0 BACKGROUND

The National Communications System, a confederation of twenty-three U.S. Federal agencies and departments (see Figure 1), is responsible for ensuring a responsive, survivable, and enduring telecommunications infrastructure exists to support critical government users during a wide range of crisis. Situations requiring NCS response vary from local natural disasters such as flooding and earthquakes to international incidents such as theater conflicts and nuclear war.

Figure 1

The Office of the Manager, NCS, (OMNCS) Office of Plans and Programs has the role of planning and implementing to meet the NS/EP telecommunications requirements of the member agencies. To this end, the Office of Plans and Programs has developed and implementing the National Level Telecommunications NS/EP Program (NLP). The NLP consists of the following three programs:

GETS - Government Emergency
Telecommunications Service
CNS - Commercial Network Survivability
CSI - Commercial SATCOM Interconnectivity

The NLP is directed by Presidential guidance toward enhancing commercial communications assets, notably the components that comprise the Public Switched Network (PSN), to meet NS/EP requirements. The GETS program improves call routing capabilities and signaling survivability. Items of focus include ubiquitous access and priority treatment of NS/EP calls.

CNS enhances terrestrial trunking between access tandem and interexchange carrier through the use of both fixed and transportable assets in the form of cable, fiber optics, and microwave. CSI utilizes commercial satellites as an alternative survivable route for the transmission of interexchange traffic, and provides the capability to recover upset satellites and to control the satellite.

5.5.1

Consideration of new technologies is measured against their ability to satisfy the NS/EP requirements for survivability, priority treatment, and security. In the event of a catastrophe, the measure of the government's ability to respond is dependent on coordination through use of telecommunications. This in turn is dependent upon the survivability of communications assets for coordination efforts. During a crisis, it has been demonstrated that telecommunications assets become congested with callers attempting to make contact with loved ones in the affected area. As a result, the potential of critical government calls being blocked increases; therefore, priority treatment becomes important. With the population of STU-IIIs in use (200,000+), directives that government communications be encrypted, and the needs of the intelligence community, it is important that secure communications is available.

While not an alternative to the PSN's ubiquitousness and capacity, the land mobile satellite service (LMSS) provides an attractive extension of the PSN in satisfying NS/EP requirements and maintaining the NCS policy of enhancing commercial assets. The LMSS service being satellite based and using small terminals is relatively immune to natural disasters and can provide ubiquitous coverage throughout the U.S. and coastal regions. Priority consideration can be accomplished through software enhancements features such as dial tone, traveling classmarks, and queuing. Being that the LMSS is an extension of the PSN, incoming PSN traffic to the LMSS will be subject to administrative controls including the priority features that are presently being addressed to the PSN by the GETS program. Priority treatment of traffic originating within the LMSS remains to be addressed in its architecture; this task should again benefit from the development of the priority treatment currently being done by the GETS program.

Compatibility with secure telephone units imposes requirements on the communications system components which are used to establish the link between the satellite and a mobile earth terminal (MET). The link between the satellite and a MET can be very difficult to maintain in regions where natural or man-made obstacles produce signal blockage. Signal interruptions cause error bursts and difficulties in maintaining data synchronization. Coding and other techniques for error mitigation must be made sufficiently robust to maintain bit error rates and time delays within the limits imposed by the encryption equipment.

In a mobile link design, there will always be a compromise between the complexity of the equipment and the environment in which it can operate. For this reason, the early part of the NCS/JPL study concentrated on characterizing the mobile satellite link and evaluating the equipment designs available for implementing a viable secure voice service. As the LMSS approaches commercial service, the choice of the equipment, its integration into the system, and subsequent evolution to next generation LMSS and other digital mobile communications services are becoming urgent issues.

2.0 SECURE VOICE STANDARDS

One of the first assumptions to be made in the implementation of secure voice into the LMSS is that the STU-III will be the standard with which the LMSS facilities must be compatible. This is because of the existing investment in STU-III equipment. Since the LMSS will be tied into the PSN, compatibility with STU-III users on the PSN is necessary.

The STU-III communications terminal connects to the PSN and allows the user to make secure telephone calls over analog facilities. In the non-secure mode of operation a STU-III operates as an ordinary telephone, using analog voice and signaling 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 encrypted and output on a subcarrier in V.26 format. During the secure call set-up there is also some signaling and echo canceler control using 2100 Hz tones, as well as digital hand shaking, [1], [2].

The newest generation STU-III's, which have recently become available, include 4.8 kbps voice using the CELP voice coder defined in Proposed Federal Standard 1016. In the secure mode the output signal is in V.32 format.

A functional block diagram of a STU-III is shown in Figure 2. Because of its intended use over analog telephone lines, certain signal combinations, such as digitized clear voice and the encrypted voice data stream at baseband, are not available at its output.

Figure 2. STU III functional block diagram

A digital STU-III is currently being defined. This version of the STU-III may be easier to incorporate into the mobile terminal equipment of the LMSS or other wireless digital communications services.

3.0 STU-III INTERFACING

A functional block diagram of a LMSS MET is shown in Figure 3. The voice codec digitizes and compresses voice, but the data rate and compression algorithm may not be the same as used in the STU-III. The FEC codec provides error protection, usually by means of time interleaving and convolutional encoding. Here a compromise must be reached between link robustness and an increase in the link data rate. The modem

5.5.2

provides data modulation on to the carrier, again with some compromise between link robustness and bandwidth.

Figure 3. MET functional block diagram

To interface the analog STU-III to the digital LMSS MET, therefore, requires that its clear mode voice be digitized externally and the encrypted secure voice V.XX signal be restored to a baseband digital stream by means of another V.XX modem. The most direct way to accomplish this is by means of an adapter between the STU-III and the MET at the mobile, and between the STU-III or PBX interface and the modem at the earth station end of the link.

There are two options for handling the clear voice mode. One is for the adapter to include its own voice codec and output a digital data stream in both clear and secure modes into point A of the MET. The other alternative is to use the MET's voice codec in the clear mode, and only provide a digital data stream to the MET in the secure mode.

Alternative ways of integrating a STU-III into mobile equipment are to physically combine some of the elements of the STU-III with the elements of a digital, non secure voice terminal. This may become practical with the advent of a digital STU-III.

4.0 SYSTEM TESTING

System testing and evaluation of various commercially designed adapters has been done mainly in the laboratory, using a satellite link channel simulator. The channel simulator can set up any value of signal to noise ratio by adding Gaussian noise, produce fading by introducing multipath signals, and simulate other signal impairments such as blockage experienced in mobile links. Actual measured satellite signal strength data can be used to drive the simulator. A data base of satellite link measurements has been built up by the JPL mobile satellite experiment (MSAT-X) and NASA Propagation programs.

In another testing approach, bit error patterns of several modem types, operating under a range of link impairments, have been recorded. These patterns can be injected directly at the adapter to MET interface to provide very repeatable test conditions. In FY 92, the effort included generating simulations of several modem/codecs designs using a COMDISCO simulation package. When completed, these simulations will allow a much more rapid evaluation of modem and codec design options.

The STU-III adapters tested at JPL included a developmental model Digital Transmission Interface (DTI) supplied by Electrospace, Inc., and a unit from Stanford Telecom. A newly developed unit from Ilex is being considered for evaluation.

Those units tested to date were tested with the MSAT-X developed TCM/8-PSK modems. In both cases the mode most sensitive to link impairments was the transition between clear voice and secure operation. The hand shaking that goes on between two STU's during this time needs better error protection. The MET is not aware which mode the equipment is in and applies uniform error protection to the data stream. Therefore any extra protection needed must be added by the adapter or the STU (next generation version). The results of the lab tests are available in [3] and [6].

5.0 FIELD TRIALS

The first field trials and demonstration of STU-III secure voice over a real digital mobile satellite channel took place in mid 1989, during a MSAT-X experiment in Australia. MSAT-X equipment, the Electrospace, Inc. adapter, and the Japanese experimental satellite ETS V were used in a system configured as shown in Figure 4.

Figure 4. Field Trial Configuration

The field trials in Australia showed that a secure link could be set up and maintained over a satellite link which was operating with very little margin and was subject to multipath signals and blockage by roadside obstacles. Details are available in [3] and [4].

The next planned phase of secure voice field trials is with the ACTS Mobile Terminal (AMT) being developed by JPL. The AMT is similar in concept to the L-band MSAT system, but will operate over the 20/30 GHz ACTS satellite. The purpose of the AMT project is to demonstrate LMSS system concepts in these higher frequency bands, as well as to evaluate the link impairments such as rain fade which are much more severe at higher band frequencies.

6.0 TRENDS IN DIGITAL COMMUNICATIONS SERVICES

When this task started several years ago, the LMSS appeared to be a separate unique digital facility. Recently there has also been a trend toward digital implementation of voice in terrestrial mobile communications services such as Cellular Telephone and Mobile Radio. While the LMSS can provide more complete geographical coverage, terrestrial services may be less costly. For this reason it may be cost effective for communications service users to subscribe to both satellite and terrestrial services, using terrestrial where possible, and only switching to satellite service where terrestrial coverage is unavailable. It is possible that some service providers will provide both types of service, and may even make switching between them transparent to the user.

In addition to the geostationary LMSS that is being implemented by AMSC, the NCS has evaluated several proposed low earth orbit (LEO) satellite systems with respect to their potential for meeting NS/EP functional requirements. Those proposed systems include IRIDIUM, GLOBALSTAR, ELLIPSO, ODYSSEY, and ARIES. Those systems would also require STU-III interface capability similar to Mobilesat. In addition, since they could also provide international coverage, interfaces might also have to comply with international digital standards.

The introduction of a secure voice requirement into each individual communications service raises separate issues in each. Secure voice in a transparent, multi-service operation may be a difficult requirement to meet. In addition, if U.S. domestic systems are linked to international networks, then the process of including standards for secure voice becomes more complex.

An alternative for NCS secure voice capability is a private network using leased bandwidth from AMSC. This simplifies the issues of intersystem compatibility, but the advantages of wider interconnectivity are lost. These tradeoffs and the issues involved in multi-system interconnectivity need to be examined.

7.0 CONCLUSIONS

The NCS effort at JPL has shown that STU-III based secure voice for the LMSS is viable and has defined the range of link conditions under which it will operate. It has also determined some areas where current equipment could be improved. There remain some specific issues on how to incorporate secure voice into the AMSC system. It is also not too early to start looking at the next generation LMSS and other digital communications services.

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. Berner, J., and Vaisnys, A., Evaluation of Secure Communications Equipment Over a Mobile Satellite Link, November 30, 1989, Internal JPL Report.
4. Berner, J., and Vaisnys, A., Secure Voice For Mobile Satellite Applications, Proceedings International Mobile Satellite Conference, (IMSC '90), pp.723-728, 1990.
5. Dean, R., Transitioning from Analog to Digital Communications: An Information Security Perspective, Proceedings International Mobile Satellite Conference, (IMSC '90), pp.142-145, 1990.
6. Frazier, W., and Vaisnys, A., Laboratory Testing of STU-III Telephones Over a Simulated Mobile Satellite Link, Internal JPL Report, June 1991.