The Growing Family of Federal Standards for HF Radio Automatic Link Establishment (ALE)

Part VI: Federal Standard 1049— The Future of ALE Operation in Stressed Environments

Link establishment can include linking protection— authentication—with the addition of standard protocols.

Christopher Redding and Dennis Bodson, W4PWF

As part of an ongoing standards development effort within the federal government, a proposed standard has been developed to provide protection to the signaling in high frequency (HF) radios that implement Federal Standard 1045 (FED-STD-1045) for automatic link establishment (ALE).[1] FED-STD-1045 is the baseline standard in a series of federal standards which specifies interoperability and performance requirements for ALE radios. Included in the series is proposed Federal Standard 1049 (FED-STD-1049) entitled *HF Radio Automatic Operation in Stressed Environments*. Section 1 of FED-STD-1049, entitled "Linking Protection (LP)," specifies requirements for the mechanism employed to provide transparent protection to ALE signaling.

ALE allows stations to automatically establish links, determine the best available channel, and transfer digital orderwire messages. While ALE technology automates and expedites the linking process, it creates a potential vulnerability among stations to other linking transmissions. These transmissions can be in the form of an unintended caller imitating a legitimate ALE station or a simple playback of a previous transmission. In both scenarios, the true identity of the caller may not be known; therefore, some sort of authentication is needed. The linking protection mechanism that has been developed counters these unwanted intrusions, as well as provides a measure of confidentiality to the ALE addressing and orderwire message transmission. If the Amateur Radio community operates ALE-capable systems in the future, linking protection will be a feature that should be given serious consideration.

ALE Review

ALE technology enables radio stations to automatically initiate and establish bilateral connectivity. In the process of establishing links, a link quality analysis (LQA) is performed which allows the ALE radio to select the best available (frequency) channel. The ALE protocol also has the capability to exchange short digital text messages, even during the linking process.

The basic link-establishment process is accomplished via a three-way handshake between two or more stations. The three-way handshake consists of the call, response and acknowledgment, as shown in Fig 1. The calling station initiates the call by transmitting a series of 24-bit words containing a "To" preamble and the called station's address, and concludes with a word containing a "This Is" preamble and its own address. The called radio (or radios), which typically is scanning a number of channels, stops on the channel on which it hears the call and decodes the ALE words to determine if the call is intended for itself. The called radio answers with a short response beginning with two words containing the "To" preamble and the address of the calling station, and concludes by transmitting two words with a "This Is" preamble and its own address. When the original calling station receives this response, it is assured of bilateral connectivity and

[1] Notes appear on page 9.

Christopher Redding
12540 McKenzie Ct
Broomfield, CO 80020

Dennis Bodson, W4PWF
233 N Columbus St
Arlington, VA 22203

sends an acknowledgment to the called station, thus completing the three-way handshake for establishing the link. The time required for establishing a link is approximately 14 seconds (for stations scanning 10 channels at 2 channels per second). Also, note that orderwire messages can be inserted in any one of the three message sections of the handshake as indicated by the (▼) symbol in Fig 1. After a link has been established, the operator is signaled and voice or data communication can be initiated. Termination of a link is accomplished by the transmission of a "return to scan" signal or by the use of an internal timer, which automatically returns the radio to scanning or available status after a preset period of inactivity.

In block diagram terms, the ALE controller, shown in Fig 2, consists of three distinct modules: the ALE protocol module, the forward error correction (FEC) module and the ALE modem. The ALE protocol module incorporates standard protocols for link establishment, link quality analysis (LQA) and digital orderwire message transmission. The FEC module incorporates three error detection and correction techniques: Golay encoding/decoding, interleaving and deinter leaving, and triple redundancy/majority voting. The ALE modem employs 8-ary frequency-shift keying (FSK) modulation, with each of the 8 tones representing 3 bits of data. The resultant over-the-air data rate is 375 bits per second.

The protection module and its associated LP control module is added to the ALE system for protected operation. It is located before the FEC module so that the error-correcting power of the FEC module can be used to its full advantage.

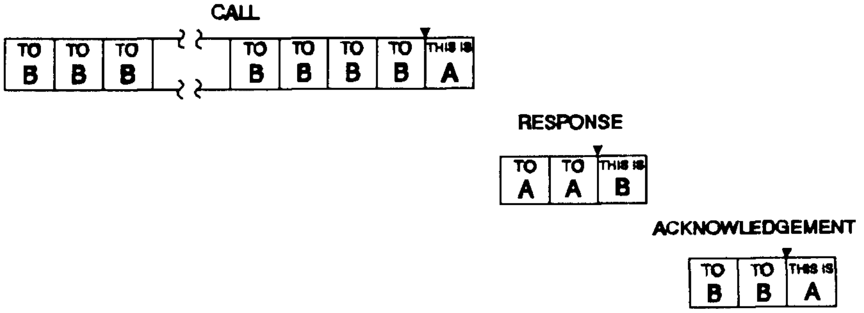

Fig 1—ALE three-way handshake.

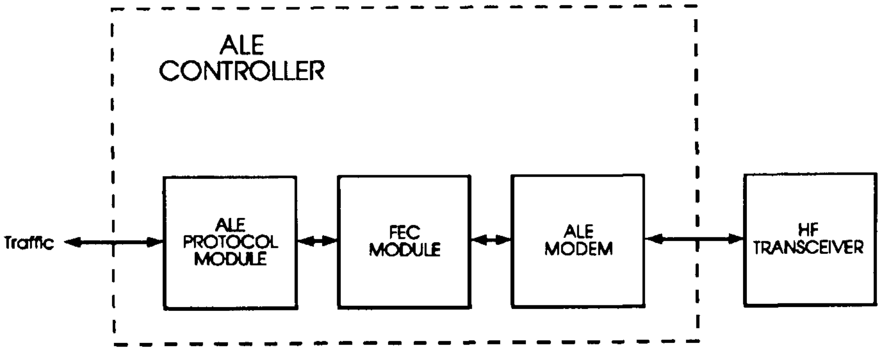

Fig 2—ALE system block diagram.

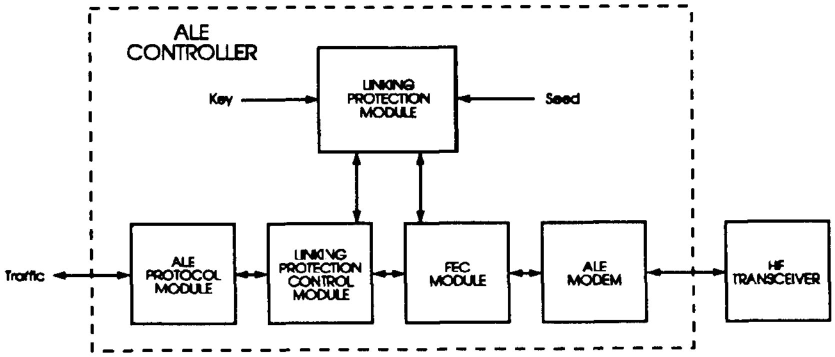

Fig 3—Protected ALE system block diagram.

Linking Protection

Linking protection is a mechanism for preventing other stations from establishing unintended links or interfering with the establishment of legitimate links. It is achieved through an automatic authentication process. Authentication is provided by processing the linking data through an appropriate algorithm before transmission, and processing the received linking data through the same algorithm. Verifying the identity of the sender is the primary objective of LP, but can also provide address and digital orderwire message protection. The digital order-wire message capability, embedded within the ALE signaling, can also be protected by the LP mechanism. Linking protection makes it extremely difficult for another station to play back previously recorded valid messages or generate new messages that the receiver will accept as valid. Additional information on this topic is given by Redding and Johnson.[2]

Protected ALE transmissions are protected by the use of an appropriate algorithm, a key variable and seed information. A block diagram of a protected ALE system is shown in Fig 3. Protection is performed on each individual 24-bit word. The seed, consisting of a known 64-bit time-of-day (TOD) code and the frequency-of-transmission information, is used to vary the protection function on a short-term basis. The minimum incremental change in the time-of-day used in the seed is referred to as the protection interval (PI). Because of the time-related protection interval, previously recorded messages that are played back will appear as unintelligible information to the receiver, and will be treated as such. Use of time and frequency varying information as an input to the protection function means that no extra synchronization bits or preambles are required in protected ALE transmissions. Although this protection method requires no overhead bits, it does require stations to keep accurate time and periodically transfer the timing information for synchronization maintenance.

A method for stations to obtain synchronization is required since protected radios operate on time-based protection intervals. The method developed is based upon an incremental two-step process. The first step, termed coarse synchronization, relies on stations synchronizing their clocks to within one minute of each other. After coarse synchronization is obtained, a time synchronization protocol is utilized to obtain fine synchronization by distributing timing-related information. The fine synchronization times range from 60 seconds to 2 seconds or less, with the lowest protection level employing a single PI of 60 seconds.

Several levels, or strengths, of LP have been specified so that the majority of users are provided with sufficient protection. Protection levels are distinguished by the strength of the algorithm and the length of the PI (ie, the protection increases as the PI decreases). Because of the unique requirements of LP, special algorithms have been developed for unclassified users. Linking protection can be implemented in hardware or software depending on the particular requirements of the procuring organization. The lowest level of LP can be easily implemented in software; therefore, its costs are kept to a minimum for the user who requires only this minimum level of protection.

The LP function only protects the linking process and any digital information transferred during that process; after a successful link is accomplished between two or more stations, no protection exists. Separate auxiliary higher-speed modems can be utilized after the initial ALE process if desired.

Although not applicable to Amateur Radio, data encryption capabilities for inclusion within the ALE radios are being developed in proposed Federal Standard 1049 Section 3. Details of FS-1049/3 will be presented at a later time when the technology is developed, implemented and tested.

Summary

Protection of the ALE signaling results in protection of the linking function, as well as providing a degree of privacy to the ALE addresses. The transparency of LP provides various benefits such as establishing a link in the same amount of time as that of nonprotected systems, and allowing a receiver to acquire synchronization at any point in a transmission. These features require additional cost and overhead due to the addition of accurate clocks and over-the-air time synchronization protocols, but the user is given a choice between cost and privacy by the multiple levels of linking protection.

Acknowledgments

This work was supported by the National Communications System (NCS) and the National Telecommunications and Information Administration/Institute for Telecommunication Sciences (NTIA/ITS).

Notes

[1] *Federal Standard (FS) 1045, Telecommunications: HF Radio Automatic Link Establishment* (1990), GSA, Office of Information Resources Management.

[2] Redding, C., and Johnson, E. E., "Linking Protection for HF Radio Automatic Link Establishment," *MILCOM '91*, pp 9.1.1-49.1.5 (Oct 1991). □□