ANNEX 5
LINKING PROTECTION FOR HF ALE RADIO NETWORKS

High Frequency (HF) radio communication has been important to the radio communicator for many decades. Automatic Link Establishment (ALE) is a modern addition to HF communication that is benefiting operators with ease of use. The HF ALE radio has added the automation of the connectivity or linking process to reduce the workload of the typical operator. HF ALE Radios have the ability to selectively call and link with one or more similarly equipped stations via the HF range of frequencies. Link establishment is the ability of an HF radio station to make contact, or to initiate a circuit between itself and another radio station, without operator assistance and usually under processor control. This feature has made the connectivity process more reliable and in some cases, links are made that formerly might have been impossible for the typical operator. All this automation has come with a small but sometimes troublesome price to pay. ALE automation has added *vulnerability of the station to disruption* as a possible cause of operational interference. This disruption can be by adversaries such as pranksters and other hostile parties. Linking protection (LP) is an optional feature that can be added to HF ALE radios to reduce or eliminate the threat that can be introduced by unauthorized users.

Data link sublayers

The FED-STD-1045A (1993) data link layer comprises three sublayers: (a) a lower sublayer concerned with error correction and detection (FEC sublayer), (b) an upper sublayer containing the ALE protocol (ALE sublayer), and (c) an optional protection sublayer between these FEC and ALE sublayers, as shown on Figure A5-1. In the FEC sublayer, redundancy with majority voting, interleaving, de-interleaving, and Golay coding (encoding, decoding) are applied to the 24-bit ALE words that constitute the (FEC sublayer) service-data-unit, in terms of the OSI Reference Model. The ALE sublayer includes protocols for link establishment, data communications, network management, and LQA, based on the capability of exchanging ALE words. Linking protection (LP) is placed in the intermediate "protection" sublayer, so that it may make full use of the error correcting power of the FEC sublayer while intercepting unauthorized attempts to communicate with the local ALE protocol entity to establish links (FED-STD-1049/1, 1993).

Linking protection

Linking protection (LP) is intended to prevent the establishment of unauthorized links or the unauthorized manipulation of legitimate links, and does this through an authentication process. Block diagrams of the data flow through unprotected and protected radios are shown on Figure 2. The blocks on the figure represent logical operations only, and do not necessarily represent distinct hardware modules. LP is achieved by scrambling ALE words under a private key which is changed at daily or longer intervals, and by using known "randomization" information (frequency, time, date, etc.) to vary the scrambled ALE words on a shorter basis (a "protection interval" or PI). The private key is entered directly into the scrambler via an appropriately protected circuit, and is protected during use by the design of the scrambler. The addition of LP to a radio involves adding the functions of a linking protection control module (LPCM), which implements the LP protocol, and a scrambler, which scrambles ALE words under the control of the LPCM. The security of the system is based upon the inability of an adversary to "spoof" the LPCM, and relies on the difficulty of discovering the key used to scramble the ALE words. Because of the wide range of applications for LP, several different scramblers are specified, but the LPCM is common to all LP applications, and includes a common denominator scrambler for assured interoperability of all protected radios. Note that the LPCM handles unclassified ALE words only (though these may be sensitive orderwire commands). Any classified traffic must be encrypted by a higher level cryptographic device. The resulting BLACK data may then be sent through the ALE controller or via a separate data modem (FED-STD-1049/1, 1993).

Protocol transparency

A principal consideration in implementing LP is that the presence of an LP module in a radio (or its controller) should have no impact on any protocols outside of the protection sublayer in the data link layer. In particular, this means that achieving and maintaining LP sync must occur transparently to the ALE waveform and protocols, and that scanning radios must be able to acquire LP sync at any point in the scanning call portion of a protected transmission if this transmission was scrambled under the key in use by the receiving station. Thus, LP modules may not insert sync bits into the data stream, and must acquire LP sync without the use of synchronization preambles or message indicator bits (FED-STD-1049/1, 1993).

Transmit processing

The LP module, in a sending station, scrambles each 24-bit ALE word to be sent using the seed data then in use (frequency, PI number, word number, etc.) and delivers the scrambled word to the FEC module (FED-STD-1049/1, 1993).

Receive processing

The receiver side of an LP module is responsible for achieving LP sync with transmitting stations, and for descrambling protected ALE words produced by the Golay decoder. In operation, when a scanning receiver arrives on a channel carrying valid tones and timing, the FEC sublayer (majority voter, de-interleaver, and Golay decoder) will process the output of the ALE modem and alert the LP receive module when an acceptable candidate word has been received. This occurs roughly once every 8 ms when the Golay decoders are correcting three errors or once every 78 ms when correcting one error per Golay word. The receive LP module must then descramble the candidate word and pass it to the receive ALE module, which will determine whether word sync has been achieved by checking for acceptable preamble and American Standard Code for Information Interchange (ASCII) subset. This task is complicated by the possibility that the received word (even if properly aligned) may have been scrambled using a different PI than that current at the receiver, requiring the receiving LP module to descramble each candidate word under several seeds. A further complication is the possibility, though small, that a word may satisfy the preamble and character set checks under multiple seeds. When that occurs, the valid successors to all seeds which produced valid words are used to descramble the next word and each result is evaluated in the context of the corresponding first word. The probability is extremely small that multiple PI possibilities will exist after this second word is checked. For example, if during a scanning call (or sound), a received word descrambles to TO SAM using seed **A**, and to DATA SNV using seed **B**, the next word is descrambled using the successors to those seeds, such as **A'** and **B'**. If the result of descrambling this next word under **A'** is not TO SAM, the first descrambling under seed **A** was invalid since the word following a TO word in a scanning call must be the same TO word. To be valid in a scanning call or sound, a word following DATA SNV must have three basic 38-ASCII subset characters (FED-STD-1045) and a THRU, REPEAT, THIS IS, or THIS WAS preamble (FED-STD-1049/1, 1993).

Time of day synchronization

Because LP employs protection intervals which are time-based, all stations must maintain accurate time of day (TOD) clocks. Practical considerations suggest that station local times may differ by significant fractions of a minute unless some means is employed to maintain tighter synchronization. Because the effectiveness of LP increases as the length of the PI decreases, there is a trade-off between security (or protection) and the cost of implementing and employing a time synchronization protocol. The approach taken here is to rely on operators to get station times synchronized to a common time source within one minute (± 30 seconds), and then to employ a protocol to synchronize stations to within one or two seconds (fine sync) for full linking protection. While it is possible to operate networks with only coarse (one-minute) time synchronization, this reduces the protection offered by this system against playback (tape recorder) attacks. Synchronization of local times for LP requires some cooperation between the protocol entity and the LP time base. For this reason, the LP module, which already has access to the time base for its normal operations, may appear to be the logical entity to execute the synchronization protocols, although these protocols are logically at a higher level in the protocol stack than the LP procedure. In this case, the LP module would need to examine the contents of received transmissions to extract relevant message sections. If, instead, the synchronization protocols are executed by the ALE entity, the division of function by level of abstraction is cleaner. One concept of how the coordination across the ALE-LP sublayer boundary may be effected in this case is as follows.

a. The transmit ALE entity informs the transmit LP entity of the anticipated time that each transmission will start, so that an appropriate seed will be used for LP.

b. The receive ALE entity informs the receive LP entity of the LP levels and key(s) valid on the current channel, and what combination of fine sync, coarse sync and non-protected transmissions are to be accepted. The first word of a new transmission delivered by the LP entity to the ALE entity is tagged to indicate the LP level, key, and sync mode used to descramble it.

c. For authentication of clear mode time exchanges, the ALE module must be able to call upon the LP module to scramble and descramble individual ALE words "off line."

d. The ALE module must have access to the LP time and time uncertainty values. This time may be kept in the ALE entity, but it must always be available to the LP module (FED-STD-1049/1, 1993).

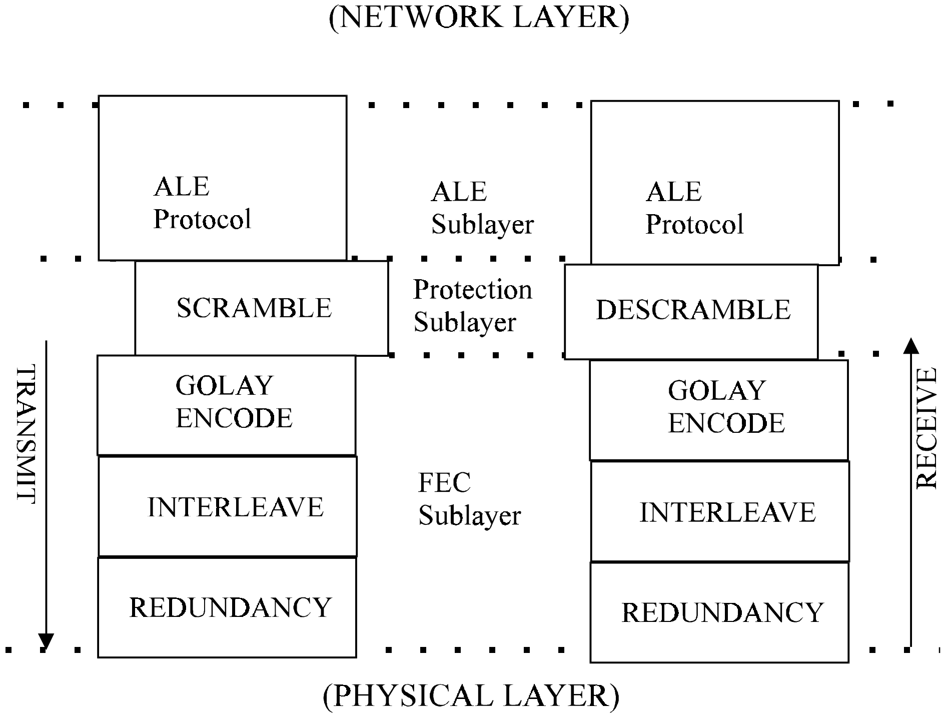
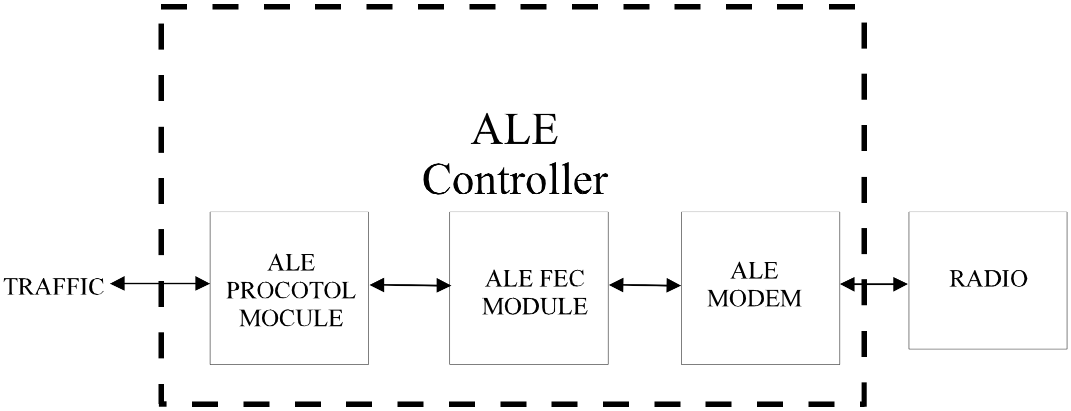
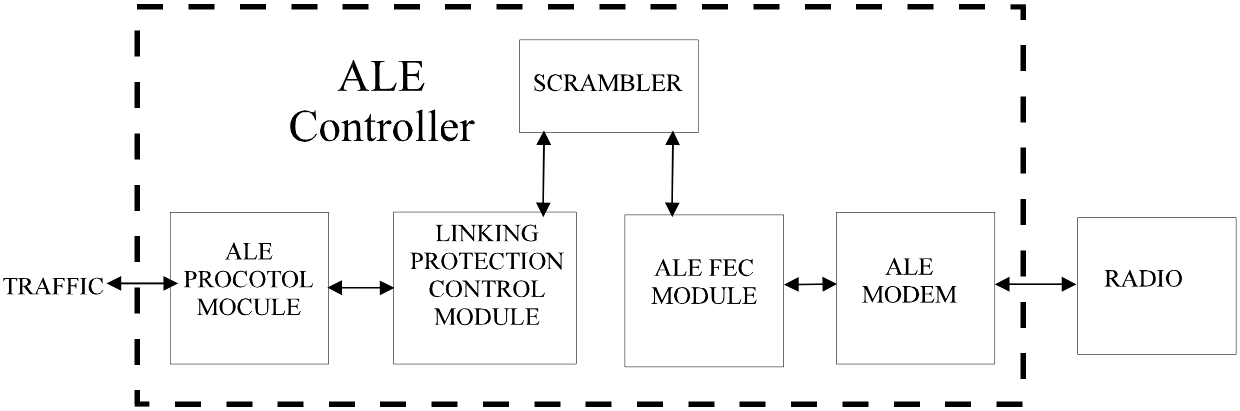


FIGURE A5-1

Conceptual model of data link layer protocols in FED-STD-1045



A. DATA FLOW IN A RADIO WITHOUT LINKING PROTECTION



B. DATA FLOW IN A PROTECTED RADIO

FIGURE A5-2

Data flow in a system without and with linking protection