Presented at the 2016 Nordic HF Radio Conference HF '16, August 2016, Fårö, Sweden.

WIDEBAND ALE - THE NEXT GENERATION OF HF

Eric E. Johnson
Professor Emeritus
Klipsch School of Electrical and Computer Engineering
New Mexico State University
Las Cruces NM, USA
ejohnson@nmsu.edu

ABSTRACT

To break the capacity barrier holding back HF from being seamlessly integrated with IP based networks, two developments are needed. First, a modulation method that achieves substantially higher data rates. Second, a link establishment mechanism that adaptively manages these wideband waveforms to use dynamically available spectrum while linking quickly to support TCP/IP communication. Wideband waveforms have been addressed in the recent releases of US MIL-STD-188-110 and US MIL-STD-188-141. This paper describes the development and capabilities of WBHF and Wideband ALE (WALE).

1 INTRODUCTION

There's an old saying the computer architecture community, referring to the interface between the processor and memory: "Throughput is easy (just add more pins); latency is hard." HF data communications faces a similar situation: we can get more throughput by increasing the channel bandwidth (if spectrum is available). However, reducing a major component of latency, link setup, is harder. We'll address both of these in this paper.

2 WIDEBAND HF DATA COMMUNICATIONS

For decades, HF radio offered only low data rates, limited both by technology and the convention of allocating HF spectrum only in 3 kHz channels. By the beginning of the 21st century, signal processing technology supported 9600 bps in 3 kHz fading channels, but it was clear that further increases in data rate would require wider channels. Wideband HF (WBHF) data waveforms were standardized in US MIL-STD-188-110C in 2011, updated in 2012. In this section we review the capabilities of the WBHF data waveforms.

2.1 WBHF-ENABLED APPLICATIONS

The higher data rates available with WBHF waveforms benefit any applications that must convey large amounts of data over HF channels. Of special interest, though, are applications that were not practical for HF channels before the WBHF era. A number of these were analyzed during the development of WBHF technology [1], including the possibility of sending real-time video over HF channels. In 2009, we had only estimates of WBHF performance. For this paper, we revisit an exciting new capability, the possibility of downlinking video from unmanned aerial systems (UAS), this time using actual WBHF specs.

We will again use H.264 compressed video streams (15 frames per second at a resolution of 160 x 120), sent via WBHF waveforms robust enough for skywave channels (Table 1). The

H.264 compression application is assumed to packetize the video stream to match the frame size used by the MAC layer (e.g., 300 bytes) to limit corruption of the video due to packet losses. If we allow a 1% packet loss rate, we can tolerate a bit error rate of around 3×10^{-6}.

As an interesting application for our video downlink study, we analyze a UAS flying in the South China Sea and returning video via WBHF to a receiving site near Subic Bay in the Philippines (Figure 1).

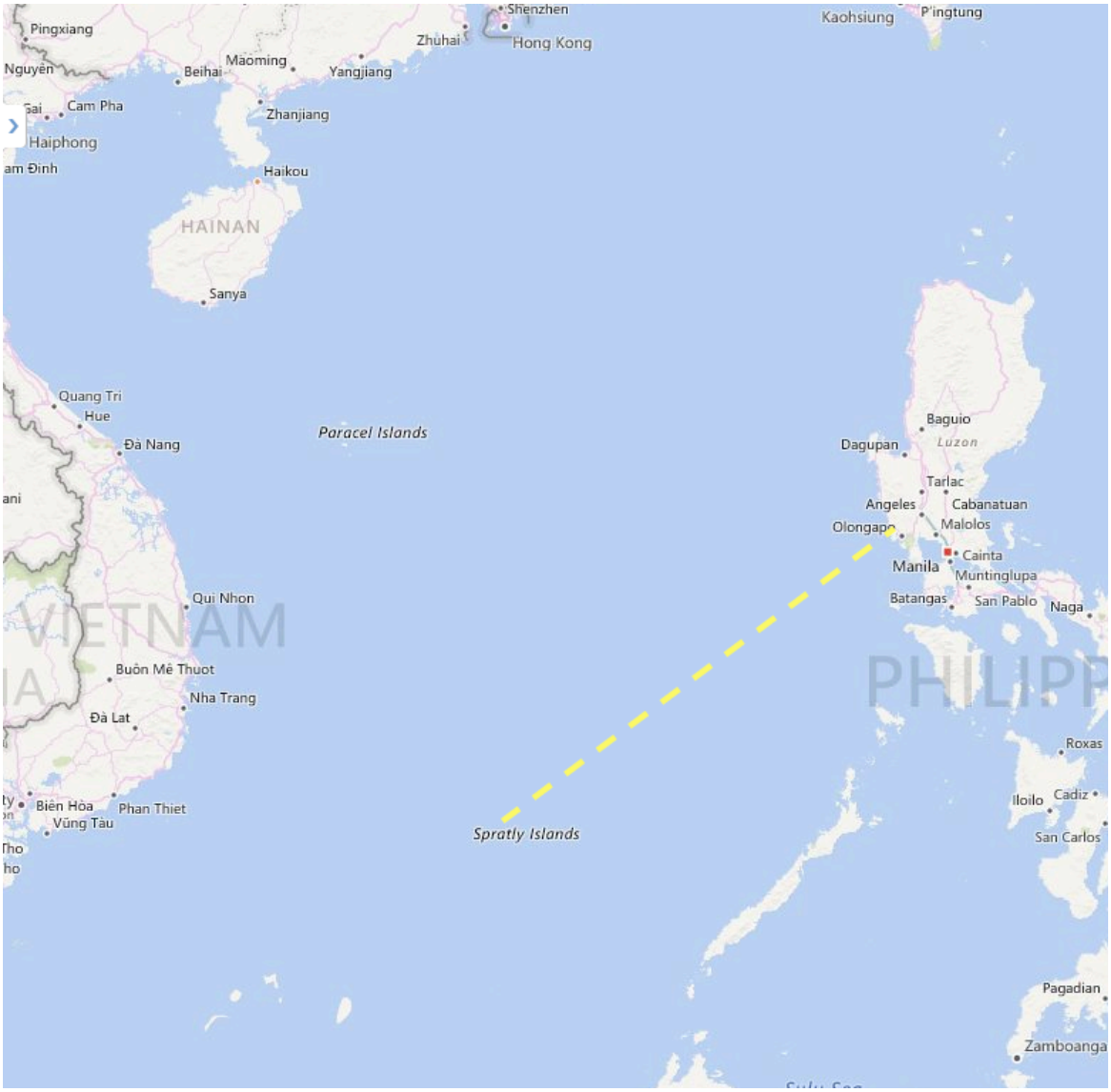

Figure 1. UAS Video Downlink via WBHF in South China Sea

As in the 2009 paper, we assume that the UAV carries a 1 kW HF transmitter. Current military UAS airframes (e.g., MQ-1B Predator or MQ-9 Reaper) are similar in size to small civilian aircraft (e.g., Cessna 172). Thus we would expect a UAS to have HF transmitting efficiency similar to the "Small aircraft" in Maslin's Figure 7.1 [2]: i.e., quite poor at lower HF frequencies, improving to about –5 dB at 8 MHz and above.

The receiving antenna is assumed to be a log-periodic with 12 dBi gain, sited on one of the undeveloped seaside mountains near Subic Bay in the Philippines for low manmade noise. The path length to the vicinity of the Spratley Islands is about 462 nmi (856 km).

MIL-STD-188-110C Notice 1 [3] Table D-LII, specifies the required SNR for 10^{-5} BER in an ITU-R "Poor" channel. Adding 1 dB to these values to achieve $3x10^{-6}$ BER, the SNR requirements for waveforms of interest in a 24 kHz channel would be as listed in Table 1.

Table 1. SNR Requirements for $3x10^{-6}$ BER in 24 kHz Fading Channels

Data Rate (bps)	24 kHz SNR Required
51,200	24
38,400	20
25,600	15

A VOACAP plot of propagation for our link in September with SSN 70, is shown in Figure 2. (Other months/solar activity are similar.) The data rates available could support live video from the UAS all day, though the challenges of the pre-dawn hours might reduce the achievable data rate then to only 19.2 kbps.

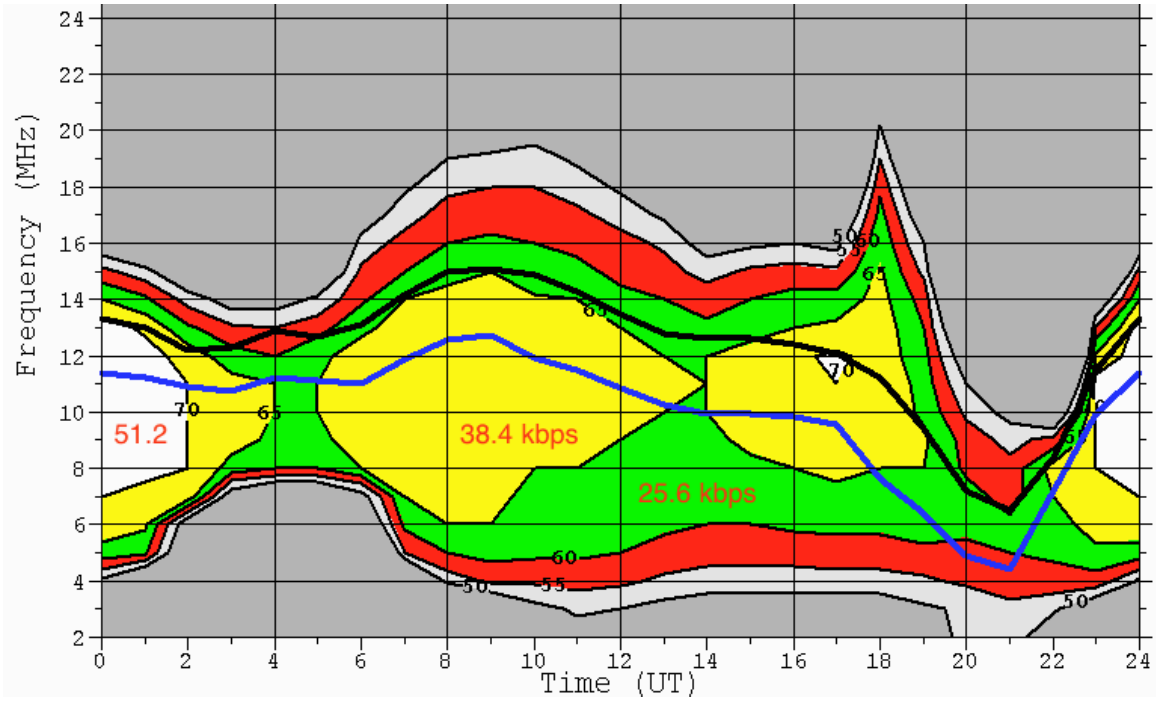

Figure 2. VOACAP Predictions for September, SSN 70
(Local Time = UT + 8)

2.2 WAVEFORMS

The MIL-STD-188-110C approach to using more than 3 kHz for a logical data channel is simply to use a wider contiguous channel. The initial set of waveforms was defined for channels ranging from 3 to 24 kHz; today this approach has been extended for channels up to 48 kHz.

Since interference from other users (voice or data) could impinge on parts of a WBHF channel (Figure 3), WBHF waveforms were defined for a range of reduced channel bandwidths, in 3 kHz increments. This supported an adaptive future capability [4] to sense the radio environment during link establishment and select a WBHF waveform that will occupy whatever portion of an allocated channel is actually available at link setup time (Figure 4).

Figure 3. Partial-Band Interferers

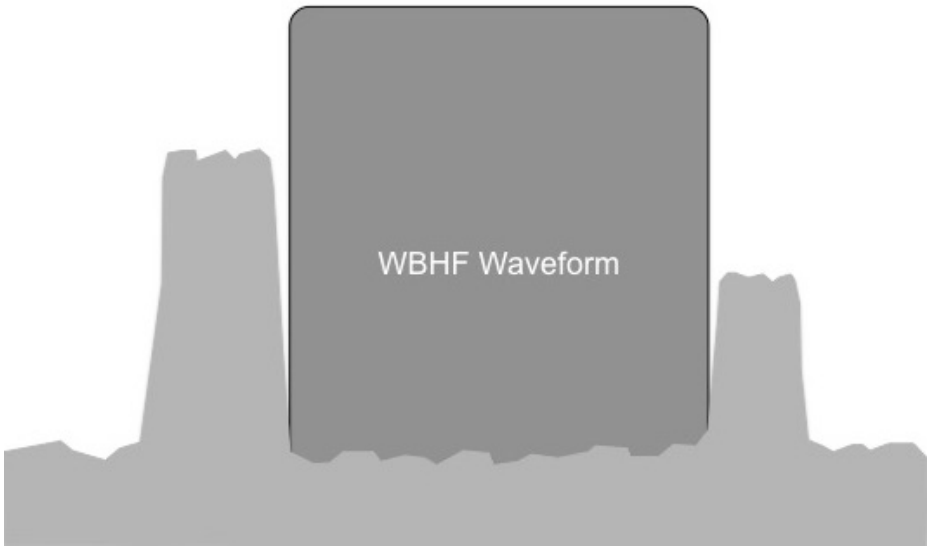

Figure 4. WBHF Adapts to Available Spectrum

The WBHF data rates for channel widths up to 24 kHz are listed by Waveform ID (WID) in Table 2. Waveforms will also be standardized for 30, 36, 42, and 48 kHz channels in the next revision of the standard, with data rates correspondingly scaled up from those in Table 2.

Table 2. WBHF Data Rates Listed by Waveform ID (WID):

WID	Modulation	3 kHz	6 kHz	9 kHz	12 kHz	15 kHz	18 kHz	21 kHz	24 kHz
0	Walsh	75	150	300	300	300	600	300	600
1	BPSK	150	300	600	600	600	1,200	600	1,200
2	BPSK	300	600	1,200	1,200	1,200	2,400	1,200	2,400
3	BPSK	600	1,200	2,400	2,400	2,400	4,800	2,400	4,800
4	BPSK	1,200	2,400	-	4,800	4,800	-	4,800	9,600
5	BPSK	1,600	3,200	4,800	6,400	8,000	9,600	9,600	12,800
6	QPSK	3,200	6,400	9,600	12,800	16,000	19,200	19,200	25,600
7	8PSK	4,800	9,600	14,400	19,200	24,000	28,800	28,800	38,400
8	16QAM	6,400	12,800	19,200	25,600	32,000	38,400	38,400	51,200
9	32QAM	8,000	16,000	24,000	32,000	40,000	48,000	48,000	64,000
10	64QAM	9,600	19,200	28,800	38,400	48,000	57,600	57,600	76,800
11	64QAM	12,000	24,000	36,000	48,000	57,600	72,000	76,800	96,000
12	256QAM	16,000	32,000	48,000	64,000	76,800	90,000	115,200	120,000
13	QPSK	2,400							

3 WIDEBAND ALE

The speed of the WBHF waveforms enhances the data carrying capabilities of HF links in two interesting cases:

- Long-running, high-bandwidth applications such as real-time video over HF become feasible, as seen above.
- Messaging applications can become much more interactive.

In the latter case, however, the time to set up a link can dominate the time to send a packet, so we will need a faster ALE to achieve the promised efficiency. For sending even moderate-size files, current ALE technologies have fallen far behind the speed of WBHF. For example, Figure 5 depicts the approximate time required to transfer the 139 kB map shown in Figure 1 using the WID 10 waveform in various bandwidths, with second-generation (2G) technology used to set up and manage the data link. (3G ALE is slightly faster.)

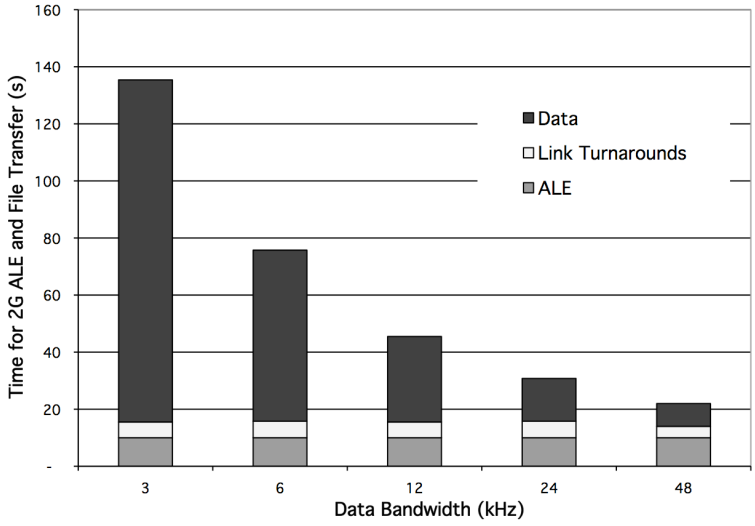

Figure 5. Time to Transfer 139 kB using 2G ALE and WBHF

Note that for 12 kHz channels and wider, the time for link setup adds 50%–100% overhead to the data transfer time; for small Internet messages, the overhead would be even worse.

It's clear that we need a new wideband ALE (WALE) that both sets up links faster than existing ALE technology and can select an appropriate data waveform and wideband channel for use on the links it establishes. The following sections of the paper present a current snapshot of the WALE (a.k.a. 4G ALE) technology, which is still in development. Be aware that some features and terminology may change before WALE is standardized[1].

3.1 LINK SETUP INCLUDING SPECTRUM MANAGEMENT

The WALE (4G ALE) system uses waveforms derived from the WBHF waveforms for its transmissions, and draws ideas from both second- and third-generation ALE for its protocols.

3.1.1 WALE Addresses

Among the many changes adopted in 3G ALE compared to 2G was the switch from ASCII call signs to binary addresses in ALE protocol data units (PDUs). We continue to use binary addresses in 4G ALE, but have increased the address size to 16 bits. This is to accommodate a desire to be able to assign fixed addresses not only to all stations active in a network, but to all stations that could participate in contingency situations. For example, there are over 5,000 aircraft in the USAF, and we would like to be able to assign each one a static WALE address.

3.1.2 Spectrum Management

The International Telecommunications Union (ITU) allocates spectrum to services (e.g., Ground Mobile) on either a *primary* or *secondary* basis. Stations of a particular service are then assigned frequencies in the allocated spectrum. From the ITU Radio Regulations [5]:

> Stations of secondary service:
>
> a) shall not cause harmful interference to stations of primary services to which frequencies are already assigned or to which frequencies may be assigned at a later date;
>
> b) cannot claim protection from harmful interference from stations of a primary service to which frequencies are already assigned or may be assigned at a later date;
>
> c) can claim protection, however, from harmful interference from stations of a same or other secondary service(s) to which frequencies may be assigned at a later date;

Thus, *stations using a WBHF channel on a secondary basis* (as indicated in the station's data fill) must not cause interference to ongoing transmissions on any portion of that channel, and must therefore restrict their spectrum use for the new link to unoccupied portions of the channel.

---

[1] The HF Radio Technical Advisory Committee (TAC) was formed in the 1980s to advise the DoD on emerging developments in HF radio technology. Recently, TAC members developed the WBHF technology and drafted the WBHF specifications in Appendix D of MIL-STD-188-110C. The TAC is now engaged in developing and specifying the WALE technology described here, planning to standardize WALE in the next revision of MIL-STD-188-141.

3.1.3 Equipment Capabilities

4G ALE is intended to be useful for a wide range of applications, including legacy systems without WBHF modems. For interoperability over such a range of systems, WALE includes an exchange of Equipment Capability (EC) codes during the link setup handshake (Table 3):

Table 3: Equipment Capabilities Codes

EC Code	Max Channel BW	WBHF "Block"
0	3 kHz	1
1	12 kHz	2
2	24 kHz	3
3	48 kHz	not yet standardized

3.1.3 Sub-channel Vectors

WALE manages contiguous channels up to 48 kHz wide. The state of the channel is described using 16-element vectors.

- For 48 kHz-capable equipment (EC = 3), each element refers to a 3-kHz sub-channel.
- Otherwise, each element of the vector refers to a 1.5-kHz sub-channel.

WALE transmissions always use a 3-kHz waveform sent in the upper sideband of a carrier centered in the assigned WBHF channel (Figure 6). For 48 kHz-capable equipment, element 8 in the vector refers to the sub-channel carrying the WALE transmission; otherwise, the transmission occupies two sub-channels (elements 8 and 9 in Figure 6).

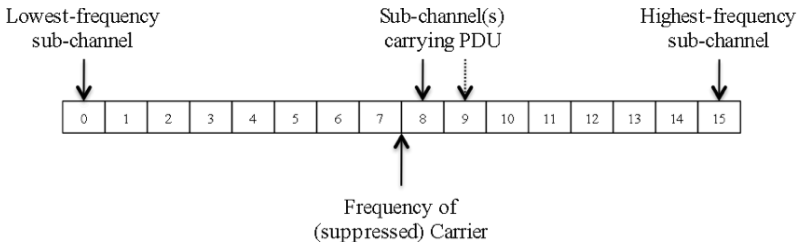

Figure 6. WALE Sub-channel Vector

Two types of sub-channel vectors are sent in WALE PDUs:

- *Availability report*: carried in a link setup Request to indicate those sub-channels that the calling station is authorized to use, and that are suitably free of interference. Each element in the vector is one bit. 0 indicates an available sub-channel.
- *Interference report*: carried in a link setup Confirm to indicate the level of interference (compared to the received signal level) measured by the confirming station in each sub-channel. 0 indicates no interference, 1 indicates a low level of interference, and 3 indicates strong interference (2 is reserved).

3.1.4 WALE Link Setup

Using the WALE protocol, stations will set up a WBHF link via a handshake on a 3 kHz "calling" channel. WALE link setup requires two or three short transmissions:

- First, the caller sends a WALE Request PDU that identifies the calling and called stations, the spectrum available to the caller (an Availability Report), its EC, and the type of traffic it wants to send.
- A called station will then evaluate the interference characteristics of the entire wideband channel centered on that calling channel. It will respond with a WALE Confirm, which includes its EC, a detailed Interference Report, and the SNR measured on the received transmission.

After this two-way handshake, if the stations are a secondary service on this channel, the WBHF channel for the link is the largest contiguous range of sub-channels that is assigned and free of interference at both stations (Figure 7).

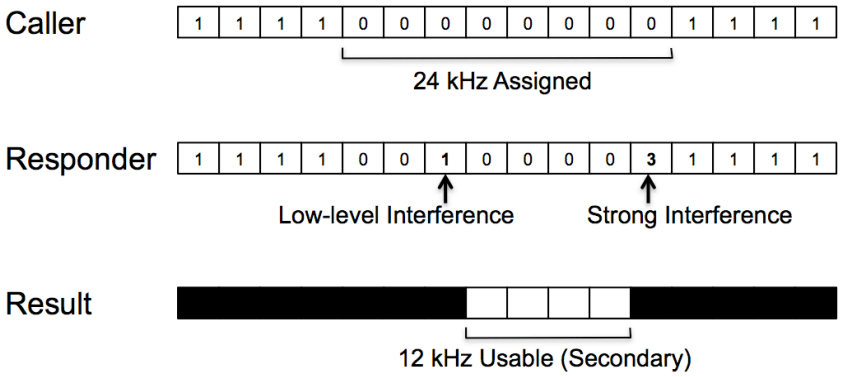

Figure 7. Example Computation of WBHF Channel for a Secondary Service

However, if the stations are a primary service on the channel, they can also use portions of the channel where only a low level of interference is reported by the other station (Figure 8).

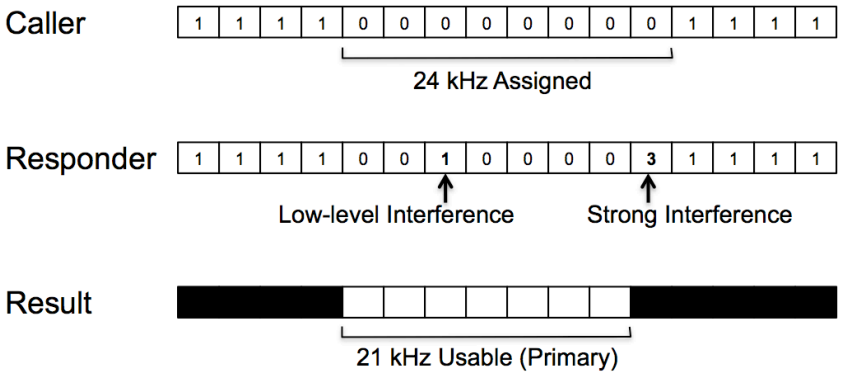

Figure 8. Example Computation of WBHF Channel for a Primary Service

After a two-way handshake, then, both stations know which sub-channels should be used for caller-to-called transmissions, and the caller can immediately begin sending data. In this case, the called station will use that same WBHF channel for its data link responses.

However, if the calling station needs to steer transmissions from the called station to a different set of sub-channels, it will send its own WALE Confirm to the called station before starting its WBHF data transmission. From this second Confirm PDU in the handshake, the called station will compute which sub-channels to use for its transmissions to the caller.

3.2 SIGNAL STRUCTURE

3.2.1 4G ALE Word

The 4G protocols use a 96-bit protocol data unit (PDU). As noted above, addresses are 16-bit binary words, and all PDUs include a 16-bit CRC for error detection. A plan for the WALE PDUs is shown in Figure 9.

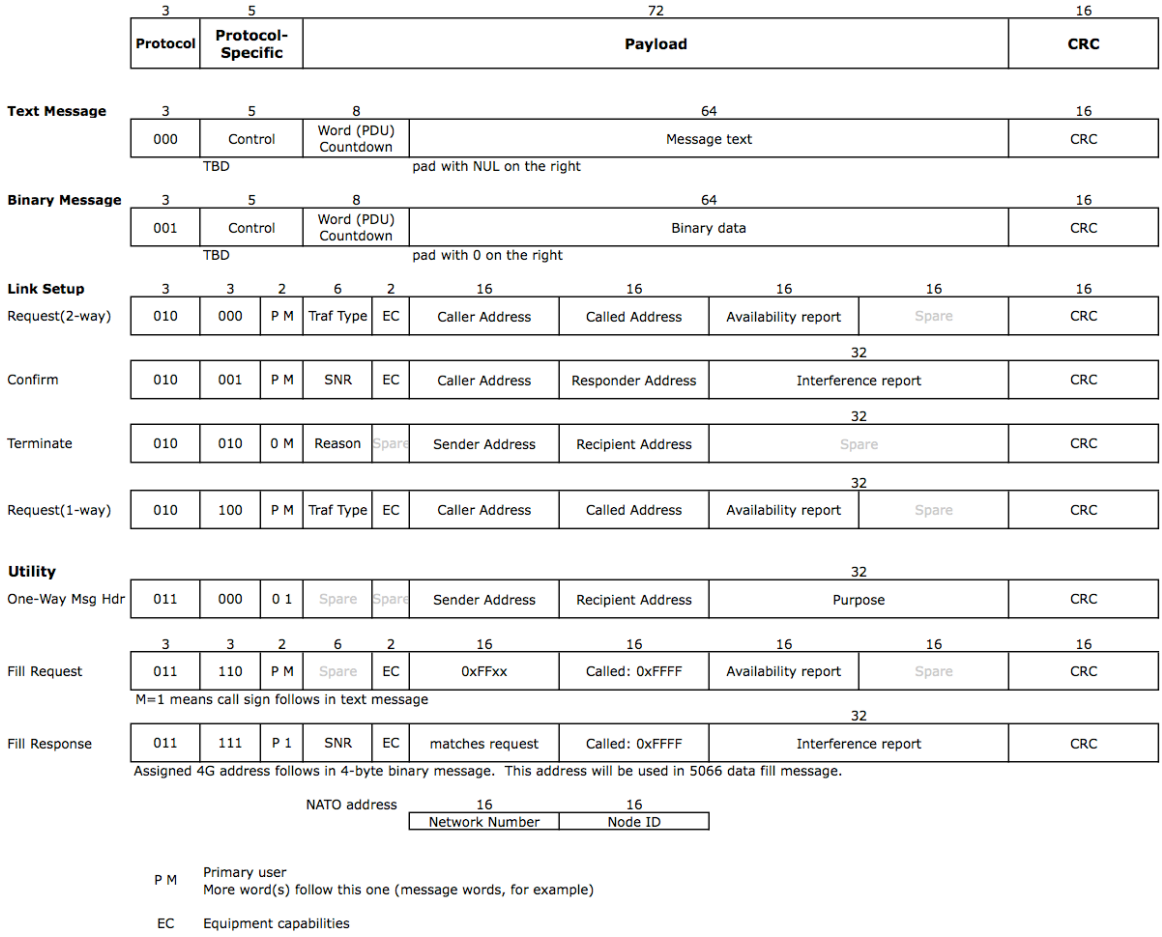

Figure 9. Plan for WALE PDUs

3.2.2 WALE Waveforms

Two interoperable modes are planned for sending these PDUs, both using 3 kHz waveforms:

- The "Fast" WALE waveform is intended for very fast link setup in voice-quality channels. Derived from the 600 bps WID 3 waveform, FEC puncturing brings the rate of the Fast WALE waveform to 750 bps.
- The "Deep" WALE waveform is designed for operation in the most challenging channels, including SNR < 0 dB. It employs a GMSK (constant-envelope) waveform with Walsh coding, and operates at 75 bps.

The choice between Fast or Deep WALE can be made on a call-by-call basis because receivers listen for both types of calls. Typically, the Fast WALE waveform is used to set up voice or high-throughput data links, while Deep WALE is used only when its robustness is needed.

Both waveforms include a 240 ms preamble. With time for Transmit Level Control (TLC) and Automatic Gain Control (AGC) settling and the preamble, the on-air duration of a Fast WALE PDU is about 395 ms; the Deep WALE PDU lasts about 1.547 s.

3.3 SCANNING OPERATION

One of the foundations of HF radio automatic link establishment is that stations not in a link will continuously scan a pool of frequencies listening for calls. A calling station selects a frequency from that pool for its call.

If the calling station knows the scanning schedule of its desired destination station (synchronous scanning), it can send a very short call on the selected frequency at exactly the time that the called station will be listening there. However, if stations are scanning asynchronously the call must much longer so that the called station(s) will encounter it at some point during the scanning cycle; thus "scanning" calls in asynchronous networks are typically much longer than synchronous calls.

- 2G ALE systems usually operate in asynchronous scanning mode, and employ scanning calls that can last 10 seconds or more depending on the size of the pool.
- 3G ALE systems normally operate in synchronous mode, with calls lasting about 1 s *after waiting for the called station to dwell on the desired channel.*

The time to set up a link using ALE includes a short "listen before transmit" interval to ensure that the chosen channel is not occupied, followed by the time for the call and one or two additional short transmissions in a link-setup handshake. Of course, the first attempt may not succeed, so additional calls and handshakes may be required before the link is available.

WALE offers both synchronous and asynchronous scanning options. In the synchronous mode, a call is simply a single WALE Request PDU. In an asynchronous call, however, the Request PDU must be preceded by a scanning call that will capture asynchronously scanning receiver(s).

In a break from previous generations of MIL-STD ALE, the scanning call portion of an asynchronous WALE call *is not addressed*; that is, the address(es) of the called station(s) are not sent during the scanning call. Instead, the scanning call consists of repeated "TLC blocks" (13.3 ms each) or WALE preambles (240 ms) [6].

Using an unaddressed scanning call has interesting consequences:

- The scanning call consists mostly of known bit sequences in short repeating blocks. This permits rapid detection of a call, and therefore very short scanning dwell times. While dwells as short as 26.7 ms are theoretically possible, we expect that initial 4G systems will offer a dwell time of about 200 ms.
- Because the scanning call is unaddressed, all scanning stations are captured and held until the WALE Request (which contains an address) is received. This is a drawback, but the short dwell times result in short scanning calls, so this is mitigated.

For example, in an asynchronous network with 10 channels and a scanning dwell time of 200 ms, the time to set up a link using a 2-way handshake is about 3.5 s:

Listen Before Transmit	0.600 s
Scanning Call	1.760
Request PDU[2]	0.368
Link Turnaround	0.200
Confirm PDU	0.395
Link Turnaround	0.200
TOTAL	3.523 s

The linking speed of asynchronous WALE is so fast that WALE will be an attractive upgrade even for 2G voice networks that don't need spectrum management for WBHF data. For example, consider the large 2G asynchronous voice network that has been used as a benchmark for each generation of HF ALE (most recently in a MILCOM 2015 paper [7]). In this classic scenario, a global network of high-power HF stations supports global air traffic, with daily flights as indicated in Figure 10.

Figure 10. AMC 100 Scenario – Flight Map

[2] TLC time is included in the Scanning Call.

In this "AMC 100" simulation, aircraft fly during local daylight hours, and each crew places voice calls to the ground network roughly once per hour. The calls last around 5 minutes each. A performance metric of interest to air crews is how long it takes to get a link.

Updating the results presented at MILCOM to reflect use of a 96-bit WALE PDU, we see that 4G ALE (WALE) links substantially faster than either 2G or 3G ALE. Figure 11 shows the cumulative fraction of all links established as a function of elapsed time.

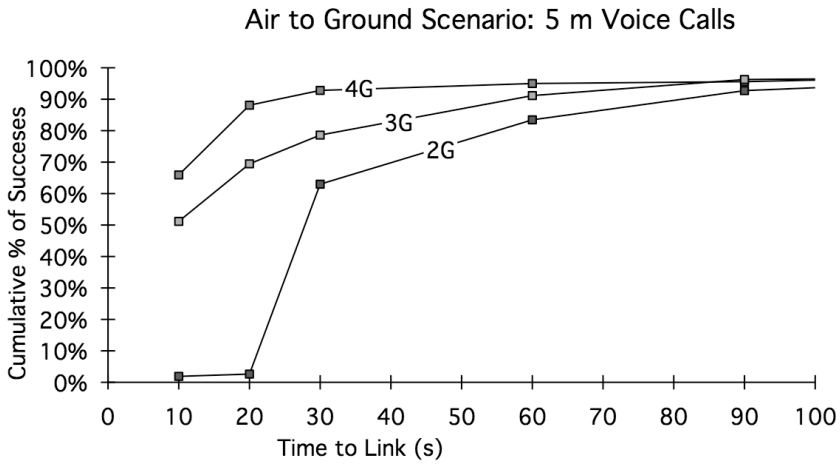

Figure 11. Linking Times in Asynchronous Network (AMC 100 Scenario)

3.4 STARING OPERATION

The MILCOM 2015 paper [7] discussed an intriguing area of current research in HF radio link establishment: stations that "stare" at their assigned frequency pool rather than scanning. This offers the possibility of nearly instantaneous link establishment [8], especially when WALE is employed.

Scanning operation includes several inherent delays that reduce performance:

- Asynchronous networks require a scanning call long enough to capture scanning receiver(s).
- In synchronous networks, the call can be short, but it can't be sent until the desired receiver is listening on the selected channel.
- In either case, a listen-before-transmit (LBT) interval is required before placing the call because the calling station is usually not aware of current channel occupancy.

If ALE receivers stare simultaneously at all of their assigned calling frequencies, rather than scanning, we eliminate all three of these delays. The first two vanish because a desired receiver is always available on the selected channel, so the very short WALE call can always be sent immediately. LBT is no longer needed because a calling radio is always and continuously aware of channel occupancy on all of its assigned channels.

The challenge is, of course, that until recently it was not feasible for HF communications sets to simultaneously listen on multiple channels. Now, however, Kyynel [9] is offering a radio that can stare at the HF band, and researchers in Sweden [8] have described a multi-channel receiver using software-defined radio (SDR) technology.

Repeating the linking time computation from above, but using staring instead of scanning, the time to set up a link using a 2-way WALE handshake is reduced to less than 1.2 s:

Listen Before Transmit	–
Scanning Call	–
Request PDU	0.395 s
Link Turnaround	0.200
Confirm PDU	0.395
Link Turnaround	0.200
TOTAL	1.190 s

If we compare linking time in the AMC 100 simulation scenario, we see (Figure 12) that even in a real-world scenario with fading, noise, and congestion, staring WALE establishes most links in under 2 s.

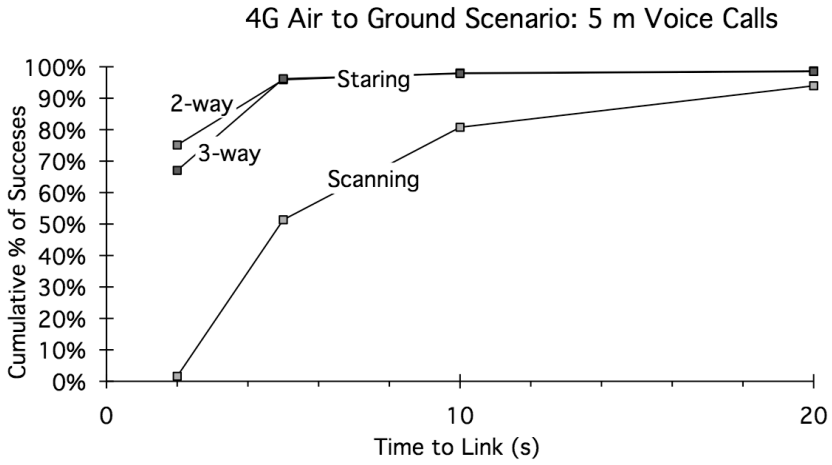

Figure 12. AMC 100 Linking Times in Staring *vs* Scanning Networks

In addition to reducing the time required to set up an HF link, both scanning and staring WALE can also significantly reduce congestion on HF channels by shortening or eliminating the scanning call portion of calling and sounding transmissions [7].

3.5 OTHER PROTOCOLS

3.5.1 Messaging

So far we've illustrated the ability of 4G to operate in the minimalist mode familiar to 3G users: one quick PDU in each direction will set up a link. Fans of the built-in messaging of 2G, however, will be pleased to find that the 4G suite offers text messaging similar to 2G Automatic Message Display (AMD), as well as a similar binary message capability.

The message words shown in Figure 9 can each carry up to 8 bytes of a message. Multi-word messages use the Word Countdown field, which is decremented in each message word sent so that the count is zero in the final word of the message. Message words can be appended to any of the Link Setup PDUs by setting the "M" bit in that PDU; that bit is set to indicate that

more words follow. (This eliminates the "last word wait" uncertainty in variable-length 2G transmissions).

After a link is set up, messages are appended to a One-Way Message Header utility PDU so that the source and destination addresses are present on each message.

3.5.2 Late Net Entry

A special-purpose link setup handshake is provided for stations desiring to enter the network. The entering station sends a Data Fill Request, which is addressed to a default address 0xFFFF since the entering station may not know a valid address of a station that can provide a data fill. The entering station selects an address in the range 0xFFxx as its sender address. It may append a text message to the Fill Request that indicates its call sign (for recording the mapping of call signs to binary addresses).

The Fill Response takes the place of a WALE Confirm in this handshake, including an Interference Report that is used to set up a WBHF channel that will carry the data fill message. A binary message is appended to the Fill Response; this message contains the STANAG 5066 address that will be used in conveying the data fill.

TOD requests similar to the corresponding 3G protocol will also be included in the 4G suite.

4 LINKING PROTECTION

Linking protection (LP) is intended to foil unauthorized attempts to interact with automated radios, either to establish unauthorized links or to interfere with the establishment of legitimate links. LP does not address jamming or similar techniques, which are best countered by TRANSEC, nor is it intended to replace the COMSEC function of traffic protection. LP protects the *linking* function, including related addressing and control information.

The original LP scheme for protecting 2G ALE was developed in the late 1980s, and has been in use since that time. However, the cryptographic security of the SODARK algorithm used in 2G and 3G LP has lately come into question, so as part of the 4G project we are revisiting the LP system design.

4.1 REQUIREMENTS

Linking protection uses a cryptographic algorithm and secret key to *authenticate* ALE words sent over the air. ALE words are encrypted before transmission. A protected ALE receiver decrypts each incoming transmission and ignores any result that violates the ALE protocol or error checking. Thus, an adversary who wants to "spoof" a victim receiver must guess a bit pattern that will pass these checks *after decryption*. The adversary's task becomes increasingly difficult as the ALE word size increases.

The requirements applied in the original development of LP are still relevant:

- **Transparent to ALE Protocols.** The waveforms and protocols must be identical for the protected and unprotected modes of operation. In particular, LP must not require the transmission of any additional bits for synchronization or similar purposes.

- **Self-Synchronizing**: A scanning receiver must be able to acquire crypto sync even if it arrives on the channel after the start of a scanning call.
- **Minimum Impact on Scanning Dwell Time**: Scanning receivers should be able to authenticate incoming calls without needing to scan more slowly.
- **Channel- and Time-Varying**: Ciphertext produced from identical plaintext should vary from channel to channel at any time instant, and should also vary periodically on the same channel, so that protected stations are protected from "tape recorder" attacks.
- **Time of Day Tolerance**: The LP system must support varying degrees of synchronization, from wrist-watch accuracy to GPS synchronization.
- **Moderate Computational Requirements**: The cryptographic algorithm should require only simple operations.
- **Block Algorithm**: The algorithm must operate on blocks the same size as ALE PDUs. The new algorithm must be scalable so that it can be applied to 24-bit ALE words (2G and 3G Robust LSU), 48 bits (other 3G PDUs), and 96 bits (WALE PDUs).

In light of these requirements, the current LP mechanism seems sound. We just need a drop-in replacement for the SODARK algorithm.

4.2 HALFLOOP ALGORITHM

As a successor to the SODARK algorithm, which has been used in various versions to protect ALE since 1991, we have adapted Advanced Encryption Standard (AES) techniques to encrypt the various PDUs used in 2G, 3G, and 4G ALE. The resulting algorithm, tentatively named HALFLOOP (one way of pronouncing "HFLP" an acronym for High Frequency radio Linking Protection), will work on the following block sizes:

- 24 bits (2G ALE words and 3G RLSU PDUs)
- 48 bits (other 3G PDUs)
- 96 bits (4G PDUs)

4.2.1 HALFLOOP Operations

As in AES, the HALFLOOP algorithm operates on a rectangular array of bytes, which is termed the "state." The plaintext and ciphertext words of our various ALE PDUs are formed into state arrays as shown in Figure 13:

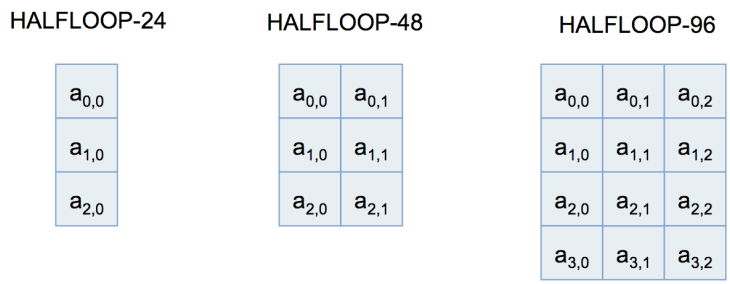

Figure 13. HALFLOOP State Arrays

Encryption and decryption involve several "rounds" of applying the following operations to the state. The operations are illustrated using the HALFLOOP-96 state, but the operations on smaller arrays are similar.

- SubBytes uses an 8-bit S-box (substitution transformation) originally designed for Rijndael. (This is similar to the substitution operation in the SODARK algorithm, but uses a different S-box.) The Rijndael S-box was specifically designed to be resistant to linear and differential cryptanalysis.

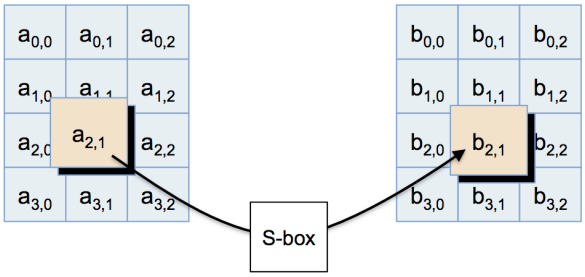

Figure 14. HALFLOOP SubBytes

- RotateRows rotates the rows of the state to the left by different numbers of bit positions.

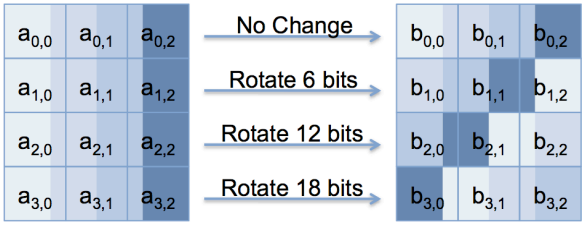

Figure 15. HALFLOOP RotateRows

- MixColumns combines the bytes in each column using an invertible linear transformation: each column is treated as a polynomial over GF(2^8) and is then multiplied modulo x^4+1 with a fixed polynomial. For HALFLOOP-96, we have four bytes in the column, and can use the Rijndael 4-term polynomial $c(x) = 3x^3 + x^2 + x + 2$. The smaller arrays have only three bytes per column, so a 3-term polynomial is needed; we use $c(x) = x^2 + 2x + 9$.

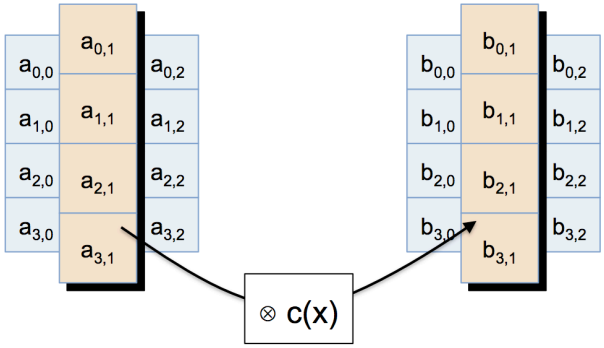

Figure 16. HALFLOOP MixColumns

- AddRoundKey adds (modulo-2) one byte of subkey with each byte of the state. The sub-key for each round is generated from the main key using a key schedule (see 4.2.2 below).

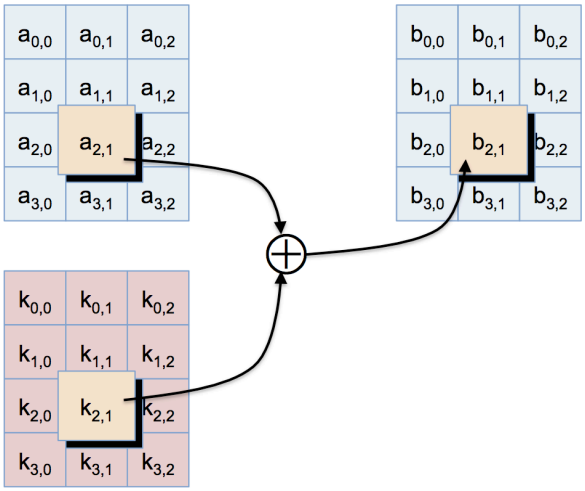

Figure 17. HALFLOOP AddRoundKey

The number of rounds to be used in each variant of the HALFLOOP algorithm hasn't yet been finalized, but all of the HALFLOOP variants are likely to use ten rounds, as in AES-128.

4.2.2 HALFLOOP Key Schedule

In general, a key schedule is employed to expand the main key via cryptographic transformations to produce a longer keystream. That keystream is then partitioned for use in the iterative rounds of the algorithm. Of course, the security of the system depends upon the length of the key before expansion.

One of the shortcomings of the SODARK algorithm was that it used a short key, 56 bits, which was deemed adequate in the late 1980s since it matched the key length of the Data Encryption Standard (DES) of that era. For HALFLOOP, we will use the same keying system as AES, whose key sizes range from 128 to 256 bits. The US Government has determined that any of these key sizes is "sufficient to protect classified information up to the SECRET level" [10] after the implementation is reviewed by cognizant authorities. For HF linking protection, a 128-bit key should therefore be adequate.

The HALFLOOP key schedule is derived from the Rijndael/AES key schedule. The only modification is that a "seed" that contains a word number, the current time-of-day and the frequency of a protected transmission is added modulo-2 (exclusive-OR) to the first 64 bits of the main key before that key is expanded.

4.2.3 4G Linking Protection

Unlike previous generations of HF ALE, the scanning call portion of asynchronous-mode WALE calls does not contain station addresses, so *the scanning call portion of asynchronous-mode WALE calls is not encrypted.*

Link setup PDUs are encrypted using the HALFLOOP algorithm. In the seed, the word number is always 0 in a Request (1-way or 2-way), 1 in a Confirm from the called station, 2 in a Confirm from the calling station, and 3 in a Terminate.

5 CONCLUSIONS

In this paper, we have described the emerging fourth generation of HF radio data communications technology. The WBHF waveforms increase available data bandwidths in HF channels up to 240,000 bps (in 48 kHz channels). Setting up and managing WBHF links will use the new WALE protocol, which dynamically adapts the use of wideband channels to avoid interference and optimize throughput.

WALE is capable of setting up links so quickly (1 to 2 s) that we can contemplate using and releasing HF channels efficiently even for short text messages, as well as for streaming and interactive Internet applications.

REFERENCES

[1] E.E. Johnson, "Performance Envelope of Broadband HF Data Waveforms," *Proceedings of MILCOM 2009*, IEEE.

[2] N. Maslin, Figure 7.1 "Frequency dependence of aircraft antenna efficiencies," in *HF Communications: A Systems Approach*, Plenum Press, London, 1987.

[3] MIL-STD-188-110C w/Change 1, *Interoperability and Performance Standards for Data Modems*, US Department of Defense, 3 January 2012.

[4] W. Furman, E. Koski, and J. Nieto, "Design Concepts for a Wideband HF ALE Capability," *Proceedings of IRST 2012*, York, UK, March 2012.

[5] ITU Radio Regulations, Article 5, Section II "Categories of Services and Allocations," ITU, Geneva, 2012.

[6] M.B. Jorgenson, R.W. Nelson, and J.A. Lahart, "The Next Generation of ALE – Getting The Most Out of WBHF," *Proceedings of the Nordic HF Radio Conference HF '13*, August 2013.

[7] E.E. Johnson, "Staring Link Establishment for High- Frequency Radio," *Proceedings of MILCOM 2015*, IEEE, October 2015.

[8] R. Berg and H. Bergzén, "Instantaneous Channel Access for 3G-ALE Systems," *Proceedings of the Nordic HF Radio Conference HF '13*, August 2013.

[9] T. Vanninen, et al, "Cognitive HF – New Perspectives to Use the High Frequency Band," *Proceedings of CROWNCOM 2014*, Oulu, Finland, June 2014

[10] CNSS Policy No. 15, Fact Sheet No. 1, "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information," June 2003.