2010 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
VEHICLE ELECTRONICS AND ARCHITECTURE MINI-SYMPOSIUM
AUGUST 17-19 DEARBORN, MICHIGAN

MOBILE, SECURED COMMUNICATIONS ENABLE NET-CENTRIC OPERATIONS

Dr. Amish A. Mehta
Vice President, Engineering
Ultra Electronics
Measurement Systems Inc.
Wallingford, CT

Andrew Cambridge
Chief Scientist
Ultra Electronics
Communications & Integrated Systems
Greenford, UK

Brian Gardner
Technical Director
Ultra Electronics Communications & Integrated Systems
Greenford, UK

ABSTRACT

The demand for mobile, secure communications has been and will continue to be a fundamental requirement for dismounted, urban and distributed operations in the field. It is imperative that soldiers on the front lines receive actionable information in a timely, secured and uninterrupted manner to increase force protection and effectiveness. In this paper, we describe a novel, high technical maturity (TRL 8+) communications link that offers the mounted and dismounted soldier secure, beyond line of sight, encrypted capability for weapons control and command & control of multiple platforms. An innovative spread spectrum waveform was designed from the ground up to deliver necessary functionality for reliable communications amongst multiple nodes with a data rate and range commensurate with battlefield scenarios.

INTRODUCTION

Knowledge is survival on the battlefield; knowing the location of friendly soldiers, enemies and the overall surroundings is paramount for dismounted, urban and distributed operations. The key to obtaining and maintaining this necessary knowledge is the ability to send and receive communications and have reliable situation awareness while in motion on land, in the air or at sea ([1,5]). The result is battlefield superiority through the ability to securely communicate via voice, video and data from any location while maintaining force maneuverability.

With the decreasing availability of the RF spectrum, it is critical to multi-task with any communications link. Reviews of existing data links and radios as well as interviews with Users identified several gaps in both performance and functionality for the unmanned scenarios faced in the battlefield. The User community is interested in addressing several key requirements for unmanned platforms in the modern battlefield: a) low latency for direct command

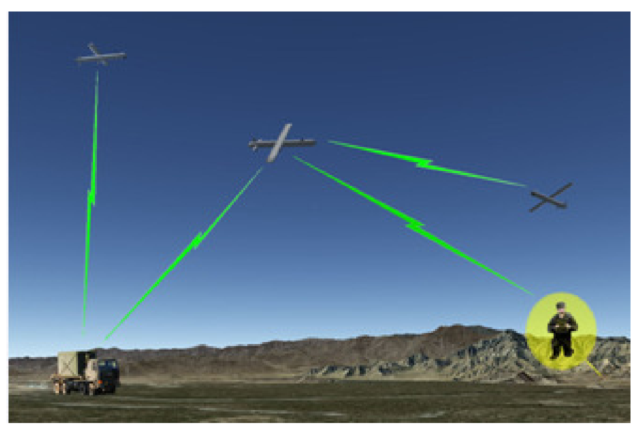

Figure 1: Desired Command & Control Data Link Concept

and control, b) low probability of intercept (LPI), c) low probability of detection (LPD), d) possible use of non-contiguous spectrum, e) long range implementation and f) Beyond Line of Sight (BLOS) networking capabilities.

It is important to note that "standard or traditional" data links implement methods of modulation (e.g., QPSK, OFDM) in which the symbol structure is inherently visible and potentially, the synchronization structure is visible as well. This presents a problem because interceptors could easily read the signals and hence jammers could jam the signal by simply attacking the identified synchronization. In addition, most secured radios today tend to implement frequency hopping methods that can also be tracked and intercepted.

The innovative, high maturity (TRL 8+) High Integrity Data Link (HIDL) was developed to satisfy these challenging, unique requirements of unmanned platforms operating in multi-path, cluttered environments.

HIGH INTEGRITY DATA LINK (HIDL)

The HIDL incorporates low probability of intercept (LPI), low probability of detection (LPD), jam resistance technology and multipath immunity to ensure that command & control (C2) functionality is not compromised in the battlefield. The external user interface is Ethernet, thus allowing the data link to be connected to standard processors for ease of use.

The innovative waveform employed by HIDL supports a network of nodes and implements a Time Division Multiple Access (TDMA) scheme; each node transmits on assigned timeslots and receives data on all other timeslots. In this schema, individual nodes may be given an allocation aligned with its functionality; for example, passive nodes may spend most of their time "listening" while those needing to transmit larger amounts of data can be given the majority of timeslots. Since the timeslots are naturally separated in time, this allows us to form simple networks that can relay various configurations for BLOS operations. This is an advantage over conventional frequency division approaches since no "backwards radios" are required at the relay nodes and the same radio can be used for all nodes.

Timeslots in the HIDL TDMA scheme are of short duration that enable end-to-end low-latency; of paramount importance when setting up stable loops for real-time control applications. The HIDL waveform provides the user significant adaptability when implemented on a Software Defined Radio (SDR). For example, it is possible to simultaneously trade off spectrum usage, data rate (e.g., variable rates can be made available) and integrity according to application requirements.

Waveform Description

The HIDL waveform is a variant of Orthogonal Frequency Division Multiplexing (OFDM) ([2 - 4]) in which signaling is simultaneously achieved on multiple parallel frequencies. OFDM is the technology behind Asymmetric Digital Subscriber Line Broadband (ADSL), WiFi, and 4th generation mobile phones.

With OFDM, a large number of parallel frequencies are each simultaneously modulated, with separate data at a low symbol rate, to achieve a high aggregate data rate. As a consequence of the low rate on each carrier, OFDM can be made highly resistant to multipath, in which not only does a radio receive the intended signal, but also the reflections of it a short time later. Traditional modulation schemes, especially when working at high data rates, pose challenges in multipath mitigation whereas OFDM has a natural robustness against this type of degradation.

The variant of OFDM used for the HIDL waveform incorporates an innovative spread spectrum scheme that ensures a noise-like appearance in both the time and frequency domains as shown in Figures 2 and 3. This is critical because it allows the radio's spectrum to be precisely tailored for efficient exploitation of available resources and thereby reduces the spectral density making the signal difficult to detect. The spreading and overlapping pulse structure allow the waveform to, in essence, self interfere. An enemy will not know the spreading code and therefore will not be able to recover the symbols because the symbol and synchronization structures are not evident in the signal. In addition, the mapping from bits to symbols is highly randomized.

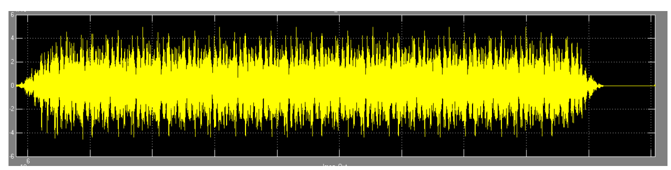

Figure 2: Typical Waveform over a Timeslot

By maintaining a certain level of spreading, the benefits of spread spectrum are thus assured including anti-jam, LPI (due to hidden symbols) and LPD (due to noise-like features).

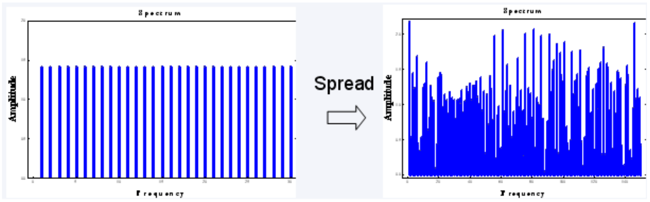

Figure 3: Spreading for Anti-Jam and LPI

The User data has Forward Error Correction (FEC) applied thus enabling good Bite Error Rate (BER) performance. Supplementing the spread spectrum is a pseudo-random interleaving and randomization operation applied to the FEC data prior to transmission. This not only protects against burst errors in the propagation channel, but also guards against unintended interception of the data.

There are several desirable waveform properties of HIDL: a) one hundred (100) timeslots available for allocation between transmitters thus allowing for different data rates for different platforms and relay capabilities; b) bandwidth between 1 and 20MHz can be allocated as desired to tailor implementation for high data rates (e.g., video), maximum range or multi-user environments (e.g., use of non-contiguous frequencies); c) range up to 200nM (e.g., antenna and bandwidth dependent) and d) data rates > 5Mbps.

Encryption

Overall system security, implementing the HIDL waveform, can be further enhanced by the use of encryption, which may be hosted within the communication link (e.g. AES-256, Blowfish) or addressed via additional modules to accommodate specific user and mission needs. We also have the option of transmitting Encapsulated Security Payload (ESP) packets either in transport or tunnel modes as necessary.

SUMMARY

The HIDL system is based on a new NATO Command and Control standard (STANAG 4660 [6]) for interoperable C2 data links and uses an innovative multi-carrier, noise-like waveform.

Implementing spread spectrum technology, the power spectral density of the resultant signal is reduced in proportion to the amount of spreading and thus the signal becomes disguised by natural noise in the system. The receiver, exploiting knowledge of the precise spreading function used by the transmitter, can reject the noise and de-spread the signal to recover the original data. In addition to providing a waveform with low probability of detection and interception, spreading also gives the system anti-jam properties.

The implementation of the HIDL waveform provides significant flexibility in timeslot allocation with asymmetric allocations possible thus allowing different data rates in different directions. Relay capability can be naturally configured and the amount of spectrum used can be tailored to the mission's requirements.

Implementing various encryption mechanisms, the system provides INFOSEC (Information Security), TRANSEC (Transmission Security) and COMSEC (Communication Security) for mobile operations. The inherent low latency allows for rapid response to information and independence from GPS measurements, and thus, immunity to standard GPS jamming methods. The innovative HIDL waveform addresses the need for secure, reliable communications for battlefield command & control applications.

REFERENCES

[1] J. Moore, "Blazing trials, dropping bread crumbs", Defense Systems, 2007.

[2] J. Stott, "The effects of phase noise in COFDM", BBC Research and Development, EDU Technical Review, 1998.

[3] O. Edfors et al., "OFDM Channel Estimation by Singular Value Decomposition", IEEE Trans. Communications, 1998.

[4] H. Minn et al., "A robust timing and frequency synchronization for OFDM systems", IEEE Trans on Wireless Communications, 2003.

[5] M. Lawlor, "Network-Centric Operations Go on the Road", SIGNAL Magazine, 2005.

[6] "STANAG 4660 Interoperable Command and Control Data Link (IC2DL)", Naval UAS Newsletter, 2007.