Implementation and Testing of the Protected Tactical Waveform (PTW)

Brian J. Wolf, *Member, IEEE*, and Jacob C. Huang

***Abstract*—The 2010 Joint Space Communication Layer (JSCL) Initial Capabilities Document (ICD) forecasts a large demand increase for US MILSATCOM in contested environments during the 2020-2025 timeframe. In response, the US Air Force in 2012 commenced the MILSATCOM Design for Affordability Risk Reduction (DFARR) effort to develop prototypes for a new protected tactical communications system. MIT Lincoln Laboratory (MIT LL) was tasked with building a test bed for this effort that would enable demonstration of prototype user terminals and space segment designs provided by DFARR contractor teams. This paper describes the test bed implementation and its use throughout the DFARR, which culminated in system-level over-the-air demonstrations, and risk-reduction demonstrations for a terminal End Cryptographic Unit (ECU) prototype.**

***Index Terms*—Satellite communications, DVB-S2, frequency hopping, WGS**

I. Introduction

The Protected Tactical Service (PTS) is envisioned to provide wideband, protected communications to the tactical edge in anti-access and denied environments. A major component of the PTS is a new communications waveform, the Protected Tactical Waveform (PTW), which provides specifications for baseband framing, modulation and coding, dynamic link adaptation protocols, and security features for data protection and jamming resistance. During the Design for Affordability Risk Reduction (DFARR), concepts were developed for user terminals, space segment designs, information assurance, mission management, and ground segment design for reachback connectivity to the Department of Defense Information Networks (DODIN), Advanced Extremely High Frequency (AEHF) satellite constellation, and Service networks [1][2]. To achieve system affordability, concepts were advanced to enter initial system operation using existing satellites, and re-using existing terminal types with modem upgrades to support PTW. Another major focus of the DFARR was the development of prototype modems implementing features of the terminal and space segments. These prototypes were tested against a reference hardware set developed by MIT Lincoln Laboratory (MIT LL).

The diagram in Fig. 1 provides an overview of the demonstration and test activities through 2014. Initial test bed development efforts at MIT LL yielded an integrated system consisting of a terminal modem, a hub modem, forward/return link emulation, dual RF interfaces (at X-band and EHF/SHF), packet generation/analysis capabilities, and standard instruments for signal analysis. Following development of the baseline test bed, lab testing began with contractor teams from Boeing Space Systems, L-3 Communications Systems West, Northrop Grumman, Raytheon, and Space Systems/Loral. Lab testing focused on demonstrating compatibility between contractor-developed brassboard prototypes and the reference hardware developed by MIT LL: the contractors, using either a terminal or hub modem prototype, tested with the counterpart hardware (hub or terminal modem) in the test bed.

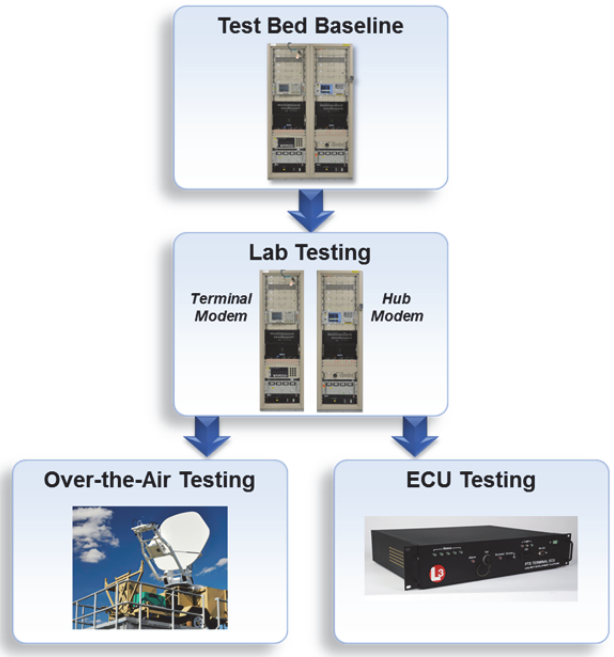

Fig. 1. Progression of test bed configurations during 2014 DFARR testing of PTW.

Following lab testing, two additional tests were conducted: over-the-air testing on WGS with L-3 Communications Systems West, and testing of a prototype terminal End Cryptographic Unit (ECU) developed by L-3 Communications Systems East. For over-the-air testing, L3W integrated their terminal modem with standard WGS terminal types. For ECU

Draft paper submitted 15 April 2015. This work was supported by the Department of the Air Force under Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the authors and are not necessarily endorsed by the United States Government.

The authors are affiliated with MIT Lincoln Laboratory, located at 244 Wood St., Lexington, MA 02420. E-mail {brian.wolf, jacob.huang}@ll.mit.edu.

978-1-5090-0073-9/15/$31.00 ©2015 IEEE

testing, L3E embedded their ECU prototype into the MIT LL terminal modem, and exercised a number of link scenarios using the MIT LL hub modem.

The remainder of the paper is organized as follows: in Section II we describe the objectives of each demonstration activity. In Section III we provide an overview of the test bed. Representative results of the demonstrations are described in Section IV, and Section V highlights conclusions and future work.

II. System Demonstration Objectives

The primary objective of laboratory tests was proving the waveform signaling interface between the PTS hub and user terminals. PTS uses a hub-and-spoke communications architecture: the user transmits data using a terminal modem to a hub modem via the PTW *return link* (RL). The hub modem processes the data and relays it to destination terminals via the PTW *forward link* (FL). User data may also be relayed directly to gateway/reachback portals, if present at the hub. Depending on system architecture variant, the hub modem may be located at a ground site, i.e., in transponded satcom architectures, or in the satellite itself.

The DFARR effort provided the first opportunity to develop PTS system designs and waveform implementations. As such, over-the-air demonstrations represented a major milestone in proving these initial modem designs could integrate into existing service terminals. Furthermore, ECU demonstrations showed maturity of a reference ECU-to-terminal interface specification.

A. Laboratory Testing

Laboratory testing was used to demonstrate consistent implementation of the waveform specification. Higher-level system features, such as link protection, link adaptation, and data protection, were also identified as major objectives.

All aspects of the waveform design, from modulation and coding to protection features such as frequency hopping and time permutation to randomize the time/frequency characteristics of the signal, were selected to eliminate advantages of partial-band jamming or other targeted interference sources [2]. In addition, PTW uses Suite B cryptographic algorithms for keystream generation so that the waveform remains operable by uncleared operators. The keystreams drive table-based algorithms for frequency hopping and time permutation. Employing table-based algorithms allows the system to flexibly alter operating bands or hopping/permutation patterns by changing the underlying tables on which these functions are based. Suite B algorithms are also used to drive a cover process which provides data protection during transmission over the air. PTW enables segregation of forward link data between different groups of users by employing different cover key streams to the traffic for each group.

To maintain high efficiency and utilization, the hub manages bandwidth and time allocations for all users on both the forward link and return link. Link adaptation features utilize a range of symbol rates, modulations, and code rates to provide a large operational range for links, from high-data rate links associated with larger terminals down to highly-robust link configurations when operating with small terminals or in environments where jamming or other sources of interference are present.

B. Over-the-air Operation

Integration of terminal modems into existing WGS terminal types and testing over a WGS satellite demonstrated that PTS can be fielded quickly and affordably by leveraging existing deployed hardware. A second objective of over-the-air testing was the demonstration of link acquisition and tracking protocols designed into the waveform specification. These protocols were necessary during over-the-air demonstrations to maintain terminal and hub modem timing across satellite links to account for range variations to the satellite and clock drift between the two modems. Another benefit of these demonstrations came from executing the mission planning process, which provided all parties with greater familiarity in how to prepare and support PTS missions on existing satellites.

C. End Cryptographic Unit (ECU) Integration

In a deployed system, the PTS terminal modem design partitions all critical security functionality into an NSA-certified ECU. A prototype terminal modem ECU was developed for testing during the DFARR effort to serve as risk reduction for future terminal development. Incorporating the PTS-specific ECU into the terminal modem introduces new interfaces for user data, control, and timing references. Using these interfaces, the ECU tests demonstrated ECU initialization, operation with a representative subset of waveform modes, and operation of link adaptation protocols between the terminal and hub with the ECU in the processing loop. While the reference interface specification used for testing provided a proof-of-concept, it is not intended to serve as a formal interface specification for future efforts.

III. System Prototyping

The PTS Advanced Test Set (PATS) is the MIT LL-developed test bed designed to support the planned demonstration activities. Consisting initially of a prototype terminal modem and hub modem, the design and operational characteristics were tailored to each demonstration event.

A. PATS Baseline and Lab Testing Configurations

The test bed terminal and hub modems utilize identical hardware and software components; the set of functionality desired is selected at system start-up. A generalized view of the PATS terminal/hub modem architecture is shown in Fig. 2. At the user level, a web-based GUI provides user control over configuration, status reporting, and logging. Processing of data and signals is performed in firmware implemented across five VIRTEX-7 based FPGA boards. Special memory registers (not shown) located between each processing stage in the FPGAs provide the capability to observe data flow for debugging and functional verification. Analog components

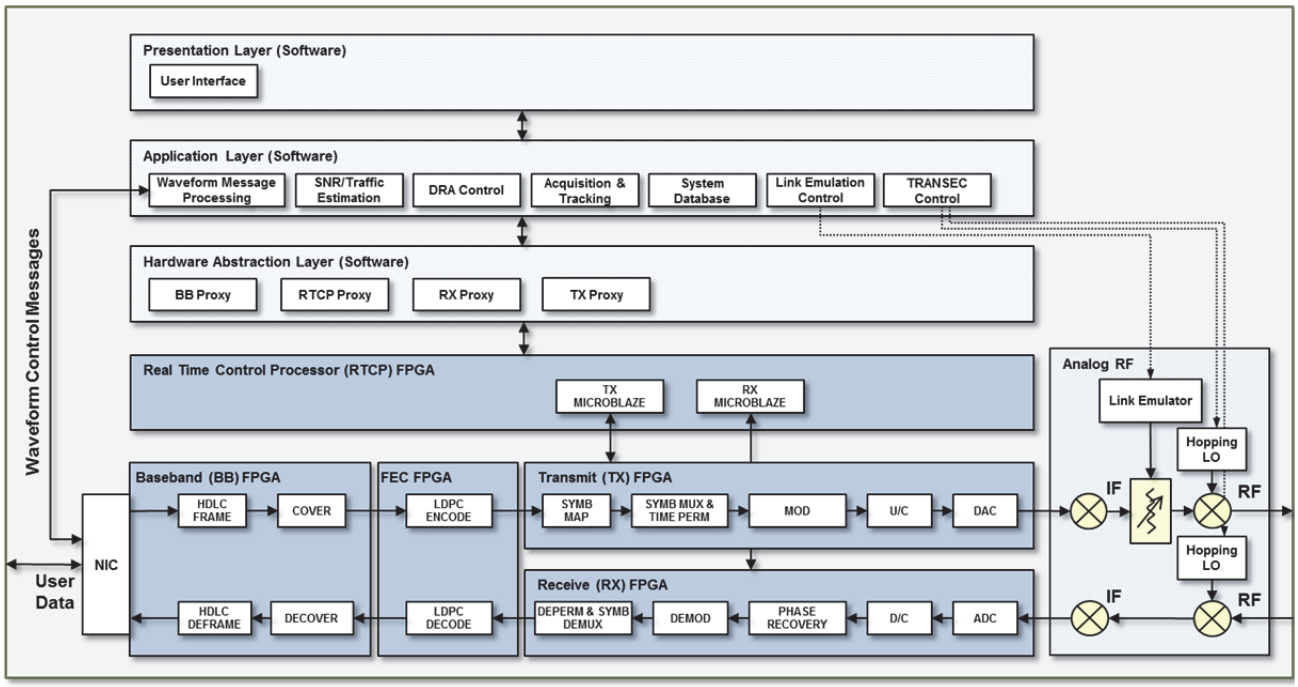

Fig. 2. Generalized view of functional components in the prototype PTW modem, showing software components, real-time controller firmware, data processing firmware, and analog RF components in terminal and hub prototypes.

perform frequency translation, link emulation, and frequency hopping.

Baseband data processing is achieved by HDLC framing [3] incoming Ethernet frames consisting of user data and waveform control messages. HDLC framing provides a constant line rate over the satellite link by inserting flag bytes (0x7E values) when there is no data to transmit. HDLC protocol fields are omitted to reduce overhead. The overall waveform overhead incurred by HDLC framing is approximately 1.1% for Ethernet MTUs, and approximately 10% for minimum length frames.

Data protection is achieved by using a bit-cover process before frames are grouped into information blocks for encoding. The DVB-S2 short block code [4] is used as the primary forward-error-correction (FEC) mechanism. This provides a fixed 16,200 bit encoded block length based on a combination of LDPC and BCH techniques with resulting rates ranging from 0.19 to 0.88 and supporting approximately 10 dB of link SNR fluctuation for a given symbol rate and modulation.

Codeword data is grouped into symbols and multiplexed across many hops, where a hop is the duration of time a transmission stays at one frequency before "hopping" away to another frequency. The hops are then permuted in time. Together, these features provide increased resistance to transient jamming or interference. Hop data is modulated using standard approaches as outlined in [4]. At the digital-to-analog converter (DAC) output, the signal is mixed to a 3.1 GHz intermediate frequency (IF) which is common to all operating bands. This allows reuse of link emulator hardware across the various frequency bands supported by PATS. The link emulator controls attenuation for signal level, noise level, and the sum of signal and noise, each having 62.5dB dynamic range. PIN diodes provide attenuation control on a hop-by-hop basis across 250 MHz of signal bandwidth centered on the signal. A final mixing stage provides translation of signal plus noise to the desired operating band using a frequency-hopped oscillator.

In the receiver, the signal is de-hopped to a common IF and downconverted to baseband. Phase coherence from hop to hop is not maintained through the de-hopping process, thus each hop must be phase-corrected prior to demodulation. This is performed using an approach based on [5]. Following this step, the signal is demodulated and decoded, and successful CRC check by the HDLC deframer indicates whether a valid HDLC frame was received.

B. PATS OTA configuration

For over-the-air demonstrations, the PATS RF chain was modified to interface with the MIT LL Over-the-air Ka Test Terminal (OTAKaTT), an existing 2.4m dish antenna with an L-band IF interface. Although PTW does not require an external time reference for operation, to expedite demonstrations a GPS receiver was added to the test bed to provide a coarse timing reference between the terminal modem and hub modem. GPS time was provided to the hub modem using the IRIGB serial time code format [6]. Fiber optic cable connected signal interfaces of the hub modem in the laboratory to the OTAKaTT on the roof of the laboratory.

C. PATS ECU testing configuration

For ECU testing, the baseband FPGA in the PATS test bed was replaced by a prototype ECU developed by L-3 East. In addition to performing baseband framing and cover functions, the ECU also generated frequency hopping and time permutation data, performed periodic key updates, and

processed return link assignments to control data flow into the encoder located in the terminal modem. The ECU provided three Ethernet ports as interfaces during testing: one for user traffic ingress/egress, one ingress/egress to the FEC FPGA, and one service port for loading configuration Transmission Security (TRANSEC) data and reporting status.

IV. System Demonstration

A. Dynamic Resource Allocation (DRA)

During lab testing, DRA tests focused on performance of DRA protocols under 5 scenarios, as summarized in Table 1. In the first two scenarios, return link and forward link noise was introduced at a specified rate and the link adapted to use increasingly robust modes of operation without loss of data. In scenario 3, an extended link outage was simulated; after the outage, the links were brought back up at degraded SNR so that the original link modes were no longer operable. This required the use of robust control broadcasts on the forward link to reestablish return link and forward link data flow.

For the final two tests, on-off jamming was simulated with the goal of showing that the DRA algorithm could be designed to operate through nuisance jamming by employing randomized backoff, hysteresis, or other algorithmic features. Error-free performance was not expected, as the 6 dB noise increase at the onset was sufficient to overcome the link margin employed by the DRA algorithm. However, the DRA algorithms maintained efficient link operation by remaining in a robust return link mode during rapid SNR changes, or by tracking the SNR and opportunistically using more bandwidth-efficient modes during slower SNR changes.

TABLE I
DRA Scenarios

Scenario Number	Description	Objective
1	8 dB noise increase at 0.5 dB/s on the return link	Demonstrate error-free adaptation through multiple return link changes
2	10 dB noise increase at rate 0.5 dB/s on the forward link	Demonstrate error-free adaptation through multiple forward link changes
3	100 s link outage (signal attenuated) on both return and forward links	Demonstrate link recovery using robust control broadcasts on the forward link
4	6 dB link fluctuation at 2s cycle on the return link	Demonstrate hysteresis and/or jamming detection mode of DRA
5	6 dB link fluctuation at 20s cycle on the return link	Demonstrate tracking of link SNR fluctuations

To further illustrate DRA operation, results from another self-test (not listed in Table 1) using the PATS hub and terminal modems are provided in Fig. 3 and Fig. 4. In Fig. 3, representative data for return link operation through a link emulator profile is shown. The link emulator was configured to reduce the return link P_r/N_0 by 20 dB; this was achieved by increasing noise power while maintaining constant signal power level. In the top graph, the return link P_r/N_0 estimate computed by the hub modem is plotted against time intervals (epochs) of 0.64s, and is shown to track the P_r/N_0 setpoint. As the measured value drops below a threshold for the current burst mode, modulation and coding (BMC) configuration, the hub modem sends new return link assignments instructing the terminal to switch to a more robust BMC. At the end of the test, the P_r/N_0 recovers to the original level. In the middle graph, the requested data rate of 256 Kbps is shown as a flat line. The actual data rate allocated is a function of BMC and fraction of time assigned to the terminal. Due to granularity of assignment size, the most spectrally efficient BMCs provide more than 256 Kbps using the minimum time assignment. As the link adapts to use lower order modulation and lower code rates, finer assignment granularity allows the assigned data rate to settle at the requested value. In the bottom graph, the total number of frames received versus time is plotted. The generation rate for this scenario is 100 frames per second, and the measured value oscillates around the average rate. The DRA algorithm is configured with a link margin of 3dB. Around epoch 19030, there are a few frame errors; this is because the measured P_r/N_0 is slightly higher than the actual P_r/N_0, and this delays the changeover to a more robust BMC while the actual P_r/N_0 continues decreasing. In the current system, P_r/N_0 estimates are based on statistics from relatively infrequent time tracking hops; a more accurate P_r/N_0 calculation method based on the M_2M_4 estimator described in [8] is planned for future work.

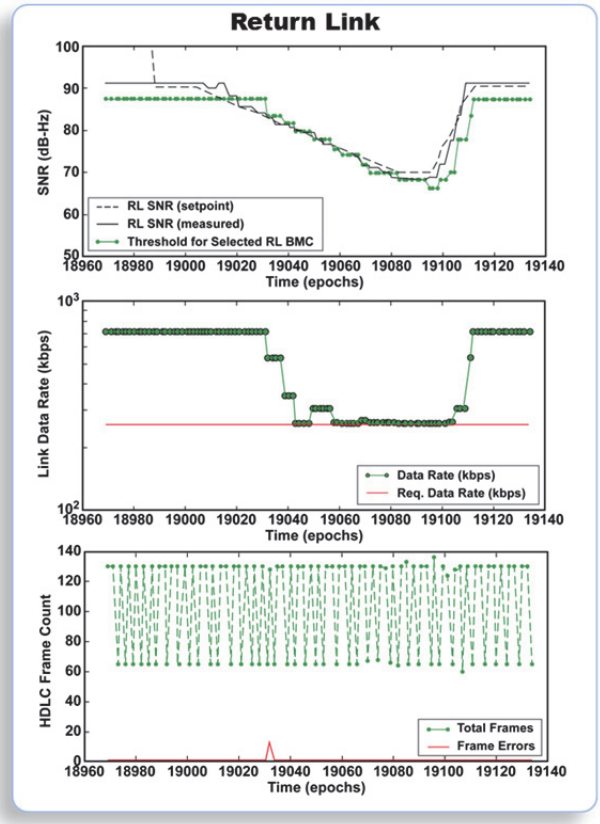

Fig. 3. Plot of return link emulated SNR setpoints, hub modem SNR measurements, and Pr/No thresholds for link mode selected by the DRA algorithm during a PATS self-test. Also shown are estimates of valid received data and bit errors throughout the link profile.

In Fig. 4, results from a similar test are shown for the forward link. In this case, the P_r/N_0 drops by 15dB very quickly, causing a burst of frame errors around epoch 10990. The P_r/N_0 continues to decrease as the link adapts to a more robust BMCs and data flow resumes. At around epoch 11010, the link P_r/N_0 decreases below the level required for the most robust BMC. Another burst of frame errors occurs due to the link outage. The terminal reports the P_r/N_0 below the minimum required threshold for the forward link, and the hub decreases the forward link resources to a minimal level (less than 100 Kbps). Remaining forward link frame errors are a result of this minimal assignment and forward link control assignments, which are also below the link P_r/N_0 threshold. As the link P_r/N_0 recovers, frame errors cease. One final note is that the forward link assignments have finer granularity, consequently assigned data rate closely matches allocated data rate for all periods excluding the link outage.

B. *Protection Features*

To test forward link data cover and data separation capabilities, three scenarios were exercised as outlined in Table II. In the initial configuration, the hub and terminal modems share the same data cover key, denoted A, and error-free link operation was confirmed. In the next stage, the Hub modem was provided with an additional cover key, denoted B, representing a separate group of users. Equal traffic was transmitted on the forward link using each key, and reception of 50% of the data at the terminal demonstrates data segregation between user groups. In the final stage, the terminal was provided with the "B" key and error-free datatransmission was verified. This demonstrates the capability of a terminal to process data streams covered according to different levels of privilege or data separation policies.

The combination of frequency hopping and random permutation of hops in time provides protection from partial-band or time-based jamming. During testing, supported frequency hopping bandwidth varied according to the band of operation, ranging from 500 MHz at X-band to 2 GHz at EHF, as shown in Table III. L-band and Ka-band operation was a product of test bed modifications for OTA testing. Testing of these features was accomplished by demonstrating error-free data transmission between the hub/terminal modem under test and the reference PATS hub/terminal modem.

TABLE II
COVER TEST SCENARIOS

Terminal Key Information	Forward Link Traffic Generation	Result (Recvd/Transmit)
A	A	648811/648811
A	A (50%), B (50%)	309337/618674
A, B	A (50%), B (50%)	617430/617430

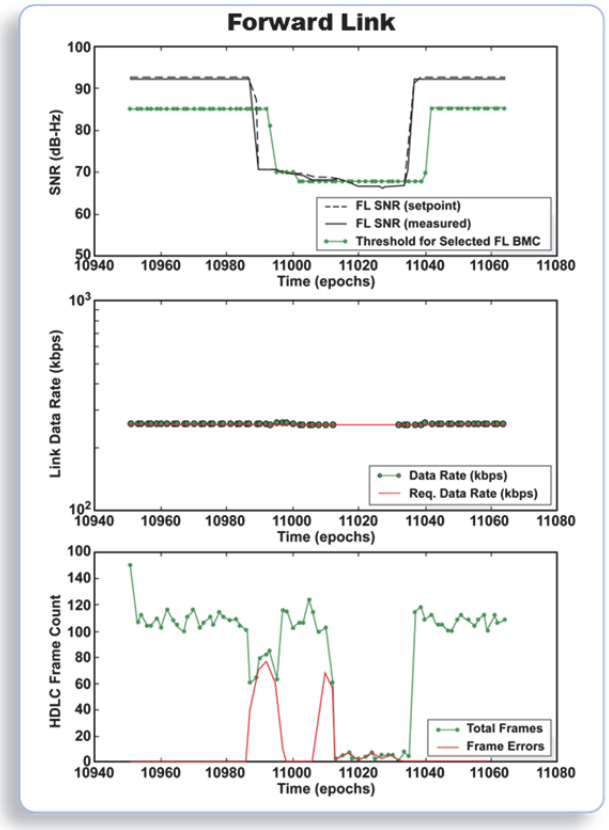

Fig. 4. Plot of forward link emulated SNR setpoints, hub modem SNR measurements, and Pr/No thresholds for link mode selected by the DRA algorithm during a PATS self-test. Also shown are estimates of valid received data and bit errors throughout the link profile.

TABLE III
PATS FREQUENCY HOPPING SUPPORT

Frequency	Return Link	Forward Link
[b]L-band	1.0 – 2.0 GHz	1.0 – 2.0 GHz
[b]X-band	7.9 – 8.4 GHz	7.25 – 7.75 GHz
[a]MIL-Ka	30 – 31 GHz uplink 20.2 – 21.2 GHz downlink	30 – 31 GHz uplink 20.2 – 21.2 GHz downlink
[b]EHF/SHF	43.5 – 45.5 GHz	20.2 – 21.2 GHz

[a]OTA testing, [b]Lab testing

C. *Over-the-air Operation*

Over-the-air testing demonstrated successful integration of terminal modems into standard WGS terminal types. Terminal antenna sizes ranged from a 0.396m to 2.4m. The hub modem integrated into the 2.4m OTAKaTT antenna. Link acquisition and tracking functionality was implemented in the terminal and hub modems to support OTA testing. On the forward link, the waveform specification defines synchronization hops for forward link time acquisition; the terminal uses these in an open-loop process to acquire timing. On the return link a closed-loop process is used to align terminal timing: probe hops transmitted by the terminal are measured by the hub modem, which then returns early/late information to the terminal using the forward link.

Tests executed over-the-air were similar to laboratory tests, so detailed results are omitted. However, the operating environment was much different, as reflected in measurements

of the WGS beacon taken prior to over-the-air testing. In Fig. 5, beacon power measurements in clear weather show a spread of approximately 1 dB between the 10th and 90th percentile, and 2 dB between the 1st and 99th percentiles. In Fig. 6, a plot of measurements taken during a storm shows a 10 dB range between the 10th and 90th percentile. There are several areas of extremely high attenuation (>10 dB) as heavy rain bands moved through the area. During actual testing, no sustained periods of heavy weather as significant as this occurred, but instances of degraded link conditions due to weather did have intermittent effects on the ability of smaller terminals to close higher-rate modes of operation.

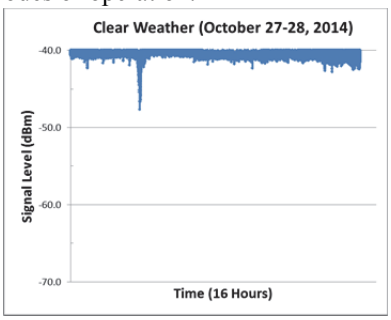

Fig. 5. Plot of WGS beacon measurements during clear weather.

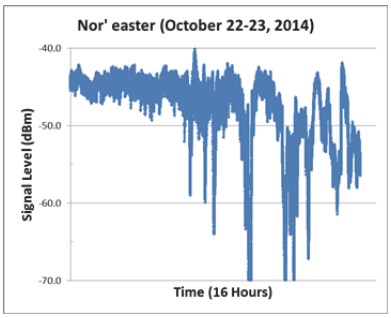

Fig. 6. Plot of WGS beacon measurements during storm conditions.

D. Prototype ECU Integration

ECU integration testing was accomplished by operating the terminal modem with the embedded ECU prototype connected to the hub modem using the verified test bed ECU functions. Prior to ECU testing, the MIT LL team implemented a functional representation of the ECU interfaces using a Xilinx FPGA-based ECU emulator implemented in a MicroBlaze soft processor. This allowed the MIT LL team to fully validate the interface specification and automate ECU testing procedures prior to the actual testing. As a result, the actual test event was completed in less than half the time originally allotted.

One observation during ECU interface testing was the need to carefully implement flow control mechanisms between the network traffic interface, the ECU itself, and the modem. At the network traffic and ECU boundary, it was demonstrated that Ethernet pause frames could effectively control ingress traffic rates to avoid buffer overflow in the ECU itself. At the boundary between the ECU and the modem, however, codeword inputs to the FEC encoder must be provided at a pace to meet timing requirements for downstream return link processing. The ECU achieves this by maintaining knowledge of current assignments and using these to determine the data volume required for each time frame.

V. Conclusions

During the DFARR effort, three test bed variants were used to support laboratory waveform testing, over-the-air testing, and terminal ECU testing. In addition to terminal and hub modem prototypes, the test bed provided instrumentation and advanced debugging features, network traffic generation and analysis, and link emulation. Results from these activities show that the data processing functions, waveform protection features and signaling interfaces outlined in the waveform definition are sufficiently mature to support modem prototype development. In particular, demonstrations using different frequency bands and hopping bandwidths proved design flexibility, showing options exist for how the system may be deployed and operated. Over-the-air demonstrations showed that PTW modems could be integrated into a range of standard WGS terminal types quickly and at low cost. Demonstrations of a prototype terminal ECU provided a proof-of-concept interface specification.

Future work to plan and execute PTS field demonstrations is underway. Industry teams will develop terminal modem line-replaceable units (TM LRUs), and demonstrations will feature the TM LRUs integrating into existing terminal types and communicating with a fully integrated ground hub test bed. A team of Government partners will create the ground test hub bed, composed of the hub modem, a multi-band RF antenna, a mission-management system (MMS), and a key management system (KMS). Test events will utilize a Systems Integration Laboratory (SIL) dedicated to interoperability testing of TM LRUs, and PTS on-orbit system testing.

References

[1] J. Sullivan, M. Glaser, C. Walsh, W. Dallas, J. Blackman, J. VanderVennet, C. Sunshine, and J.C. Chuang, "Protected Tactical MILSATCOM Design for Affordability Risk Reduction (DFARR) Results," in *IEEE Military Communications Conference (MILCOM 2014)*.

[2] M. Glaser, K. Greiner, B. Hilburn, J. Justus, C. Walsh, J. Vanderporrten, J.C. Chuang, and C. Sunshine, "Protected MILSATCOM Design for Affordability Risk Reducation (DFARR)," in *IEEE Military Communications Conference (MILCOM 2013)*, San Diego, CA, 18-20 Nov. 2013, pp.998-1001.

[3] H. Yao, J.C. Huang, and G.W. Wornell, "Achieving High Bandwidth Efficiency under Partial-Band Noise Jamming," in *IEEE Military Communications Conference (MILCOM 2013)*, San Diego, CA, 18-20 Nov. 2013, pp.1133-1138.

[4] IETF RFC 1662: PPP in HDLC-like Framing. W.Simpson, Editor. July 1994.

[5] ETSI EN 302 307 v1.2.1 (2009-08): Digital Video Broadcasting (DVB), Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2).

[6] J.S. Stadler, "A Performance Analysis of Coherently Demodulated PSK Using a Digital Phase Estimate in Frequency Hopped Systems," in *IEEE Military Communications Conference (MILCOM 1995)*, 5-8 Nov., pp.107-112.

[7] *IRIG Serial Time Code Formats*, IRIG Standard 200-04, U.S. Army White Sands Missile Range, New Mexico.

[8] D. R. Pauluzzi and N. C. Beaulieu, "A Comparison of SNR Estimation Techniques for the AWGN Channel," *IEEE Trans. on Comm.* pp. 1681-1691, Oct. 2000.