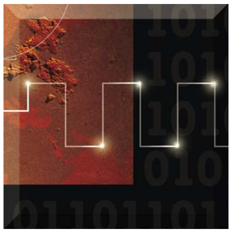


Wireless Local Area Network Flight Demonstration for High Doppler Conditions

William P. D'Amico and Mark H. Lauss

In the late 1990s, the U.S. Army's Yuma Proving Ground (YPG) adapted wireless local area network technologies to provide test data acquisition over a large portion of that test range. YPG implemented a ground-based infrastructure that supplies two-way wireless network connectivity and seamless data acquisition for multiple, simultaneous test activities and data sources. YPG and APL, under the Two-Way Robust Acquisition of Data program, partnered to provide the science behind "the how and why" of the YPG network and to investigate the use of a wireless node on a high-velocity munition, often described as the "fast mover" problem.

BACKGROUND

In the future, U.S. combatants will be structured as a network-centric force. The concept of a widespread force seamlessly gathering, distributing, and comparing information for a unified operational view of the battlefield is revolutionary. In practice, however, the network-centric concept is very difficult to implement in the military world. On the one hand, we are accustomed to reasonably efficient wired, Internet-supported network functions and activities, but a battlefield network requires the use of multiple and diverse wireless links that are not as reliable or as efficient as a wired physical layer. In addition, the test and evaluation (T&E) community faces a similar dilemma. The performance of platform-centric or stand-alone weapon systems and their munitions has typically been monitored using point-to-point radio links, commonly referred to as telemetry. One can then conclude that a wireless network would most logically support the T&E of a network-centric force. Furthermore, spectral limitations for point-to-point telemetry may drive the T&E community to a network approach, as test requirements generate higher and higher data rates. Serial point-to-point links typically reserve fixed frequencies and bandwidths for long periods of time, even though data are transmitted only for intermittent and short periods of time. These links do not dynamically share the spectrum as a function of time. Wireless networks, however, do share the spectrum in time, which is an attractive feature if it can work well in highly stressed military conditions. A number of internal memoranda and open literature publications have already documented the Two-Way Robust Acquisition of Data (2-RAD) program. Those sources are used as references and form the basis of this article.

2-RAD PROGRAM ORGANIZATION AND SPONSORSHIP

The U.S. Army's Yuma Proving Ground (YPG) wireless local area network (WLAN) is pictorially shown in Fig. 1 and is based on the IEEE 802.11b standard. This figure often produces skeptical statements such as "the network can't work reliably over those distances" or "the power levels at each node must be very large." In fact, the network has worked in a highly reliable fashion 24 hours a day, 7 days a week, for over 5 years. Furthermore, the typical maximum radiated power level at an infrastructural node is 1 W into an 11-dBi omnidirectional antenna. The IEEE 802.11b standard, which is based on indoor use, restricts power to 1 W into a 6-dBi omnidirectional antenna.

The basic operation of the YPG WLAN is given in Ref. 1, but a short review is provided here. The infrastructural sites are configured as wireless bridges, producing a topology that is normally referred to as a wireless mesh network (WMN). A WMN is a point-to-point-to-point, multihop topology with *ad hoc*–like behavior. The YPG WLAN has proven to be reliable, adaptable, and scalable for data transfer purposes. It operates without the aid of a real-time network manager while exhibiting self-organizing and self-healing traits. The WLAN operates in the unlicensed Instrumentation, Scientific, and Medical (ISM) band between 2.4 and 2.4835 GHz and uses only one of the three nonoverlapping channels in this band.

One of the wireless bridges is used in traditional bridge fashion in that wireless data packets are transferred to a network of another type. In this case, that other network is an optical fiber–based LAN. This fiber network hosts a "messaging computer" system architecture called the Integrated Test Management Facility (ITMF). The ITMF collects all of the data packets, sorts them according to meta-data tags, eliminates corrupted and duplicative packets, and reassembles the packets into logical files. These files can be archived or used as input to graphical displays in near–real time. A key feature of the ITMF is that it can then be the source for retransmission of these data files to nodes in the WMN, a fully two-way data architecture. For example, meteorological stations at several sites distributed across YPG periodically send data through the WMN on the latest conditions. The ITMF assembles a new "meteorological message" that is routed back to test directors in the field, thus providing them with the most recent and accurate meteorological conditions.

Figure 1 also shows a standard infrastructural site, which consists of a lightweight frame that can easily be placed in the back of a pickup truck (as shown). An infrastructural site consists of a wireless bridge, a solar panel, a voltage converter, an automotive battery, and a power amplifier/antenna. No attempt was made to miniaturize these components since the use of commercial off-the-shelf (COTS) devices will limit the bill of materials to approximately $4000. Infrastructural sites of this type have been in continuous outdoor operation at YPG for nearly 5 years with very little operational and maintainance cost.

The Director of Operational Test and Evaluation is responsible for providing new technologies to the major range and test facility base community. Clearly, the YPG WLAN is a new technology that is working well, but in general the T&E community could not easily understand the "how and why" so that this capability could be migrated to other ranges and applications. In addition, YPG was interested in understanding the potential use and operation of the network under various extreme conditions. One such condition would be the "fast mover" case in which a munition would be configured as an airborne node passing through the vertical extent of the WMN ground-based infrastructure. The Director of Operational Test and Evaluation's Central Test and Evaluation Investment Program (CTEIP) sponsored the 2-RAD program from September 2000 to September 2003. YPG and APL were the primary partners. Engineers and technicians at the Army Research Laboratory (ARL) at Aberdeen Proving Ground, Maryland,

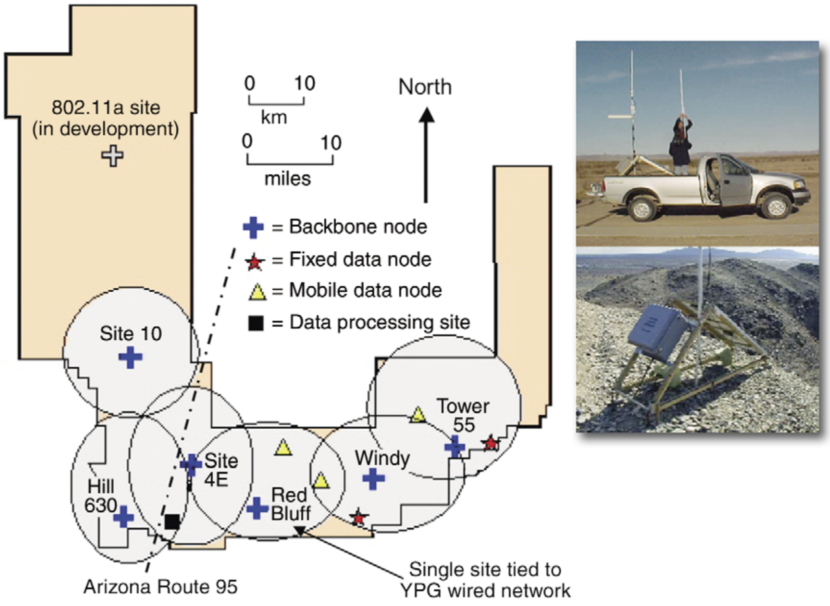


Figure 1. The Yuma Proving Ground 802.11b wireless local area network.

designed and built the flight hardware. Engineers at the Naval Air Systems Command (Point Mugu, California) designed and built a 2.4-GHz antenna for the rocket.

BASIC YPG WLAN PERFORMANCE

The initial 2-RAD task was to characterize and model the physical layer of the existing YPG WLAN. An APL team conducted a site survey to verify the hardware specifications and geographical locations of the physical layer equipment. YPG also provided a three-dimensional topological description of the range over which the WLAN operated. The results of this task are documented in Ref. 2. In summary, infrastructural sites have sufficient power to support the maximum 802.11b data rates when separated by a line-of-sight distance of 70 km. Three-dimensional models were also built to understand the vertical extent of the infrastructural coverage to include predictions of bit and packet error rates.

Since the quality of service (QoS) of 802.11b networks is notoriously poor for a large number of nodes, simple network models were also constructed. APL formulated models for average network throughput as a function of packet size and the number of nodes in the network. The number of active nodes in the YPG network is typically less than 20 (based on the six infrastructural sites and a nominal number of mobile and fixed data generation sites). The analysis in Fig. 2 verified actual experiences, showing that reasonable QoS was indeed available. A similar analysis in Ref. 3 showed that throughput has a highly nonlinear relationship to packet size. As is always the case, large packets work best within the carrier sense multiple access (collision avoidance) 802.11b architecture. Now that the basic operation and capability of the WLAN were modeled and understood, planning for the flight test demonstration began.

WLAN FLIGHT TEST

Objectives

The 2-RAD flight demonstration goal was to investigate the use of the YPG WLAN concept to support the test of airborne munitions using miniature COTS-based products. This would provide a unique testing capability that would be especially useful if multiple munitions were airborne simultaneously or for very, very long trajectories where multiple ground stations would be needed. Many issues must be addressed to provide a mature fast moving WLAN munitions data acquisition capability, especially for gun-launched munitions that are commonly tested at YPG. Several of these issues are Doppler and Doppler rate effects, association and handover under high-mobility conditions, omnidirectional miniature antennas to support two-way links, shock stability and miniaturization of components and connectors, and encryption and the impact on network throughput.

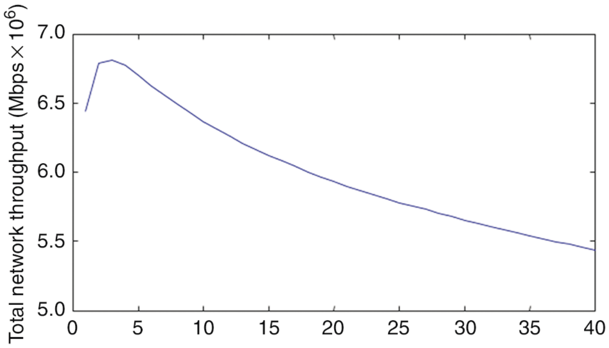


Figure 2. Network average throughput as a function of the number of nodes.

As discussed in the previous section, some aspects of the WLAN operation were addressed analytically, but it soon became clear that many of the issues could be further examined by the use of a hardware test bed where actual 802.11b devices were subjected to a synthetic environment. This test bed represents an intermediate step between analysis and flight test. As such, a hardware test bed, the Adaptable Channel Test Bed for the Investigation of On-the-move wireless Nodes (ACTION),[4] was assembled to provide risk reduction. ACTION can inject frequency and amplitude errors to simulate in-flight conditions where *ad hoc* behavior, Doppler, and handover issues can be studied extensively.

The fast mover problem could generate Doppler and Doppler rate–induced frequency shifts at a stationary receiver that would disrupt network operation. The Doppler shift is a function of velocity of the node, while the Doppler rate shift is a function of distance and velocity between the transmitting and receiving nodes. The 802.11b specification limits the frequency variation of manufactured products to nominally ±60 kHz, but there is no unique specification for Doppler effects. For a Mach 5 fast mover node at standard temperature and pressure, the Doppler shift is only about 13 kHz. A trajectory was assumed for the planned flight test, and it was used to compute the associated Doppler effects with respect to a fixed ground station.[5] The computed Doppler effects were well within the limits of the overall allowable frequency variation for an 802.11b device.

The second critical network issue noted previously is handover. In simple terms, can a fast mover outrun the network before the handover process is completed, especially if the network channel is busy because of other message traffic? This is shown pictorially in Fig. 3 as a fast mover leaves the influence of one access point (AP) and attempts to join another network controlled by another AP. The 802.11 association process is relatively well defined and was addressed analytically by developing two equations for the channel busy time.[6] The time needed for a mobile station to associate with a new infrastructural site is shown in Fig. 4. Initially, two simplifying

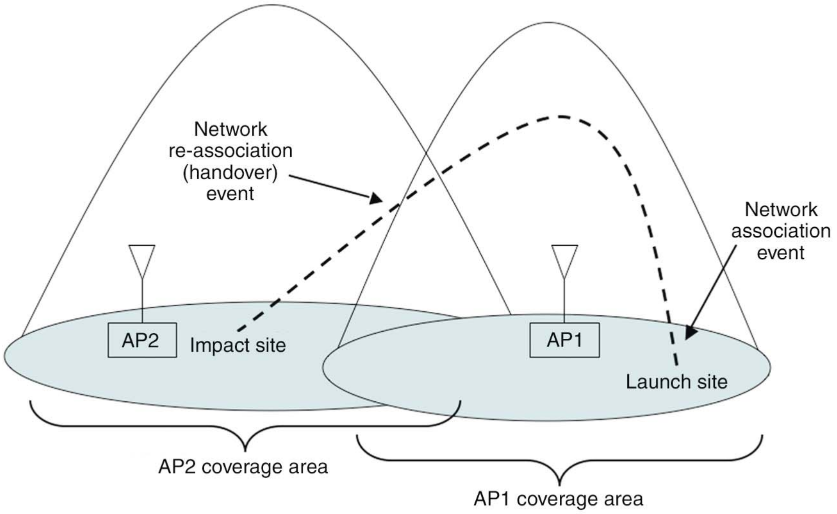
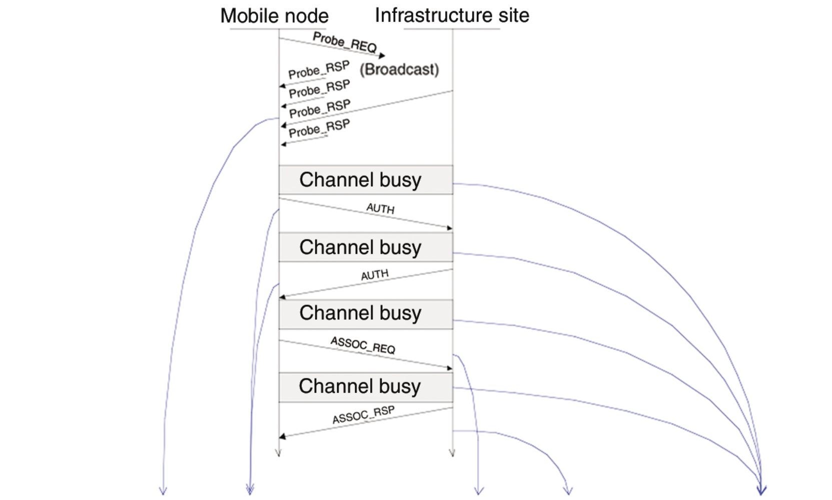


Figure 3. Description of handover for an airborne node (AP = access point).



$$t_{\text{associate}} = t_{\text{probe\_delay}} + (2 \bullet t_{\text{AUTH}}) + t_{\text{ASSOC\_REQ}} + t_{\text{ASSOC\_RSP}} + (4 \bullet t_{\text{channel\_busy}}).$$

Figure 4. Association time of a mobile node to an infrastructure site.

assumptions—zero processing time for authentication messages and perfect packet reception—proved to be highly restrictive. Subsequent to the submission of Ref. 6, laboratory measurements were made to empirically establish realistic values for those two assumptions for the case of five nodes. A second equation was then developed for the channel busy time:

$$t_{\text{channel\_busy}} = \underbrace{\frac{n}{P_{\text{tr}}P_{\text{s}}}}_{\substack{\text{Expected number}\\ \text{of slots for which}\\ \text{channel is busy}}} \cdot \underbrace{[(1-P_{\text{tr}}P_{\text{s}})\sigma + P_{\text{tr}}P_{\text{s}}T_{\text{s}} + P_{\text{tr}}(1-P_{\text{s}})T_{\text{c}}]}_{\text{Expected slot size}}$$

where

n = number of stations or nodes,

P_{tr} = probability of at least one station transmitting,

P_{s} = probability of a transmision being successful,

T_{s} = length of time containing a successful transmission,

T_{c} = length of time containing a collision, and

σ = length of an idle time interval.

Note that the three terms on the right-hand side of the equation simply represent three time durations—the time for nothing to happen (no station is trying to transmit), the time for something good to happen (a successful transmission), and the time for something bad to happen (a collision). Once the IEEE 802.11b specifications and measured manufacturer optional delays are incorporated for a specific packet error rate, a comparison between theory and laboratory data can be made. One would expect that the channel busy time would be related to the number of nodes in a complex fashion as a result of the nonlinear nature of networks. The comparison, however, showed essentially linear behavior except for the addition of the fifth node. Additional analysis for a larger number of nodes and comparisons with actual flight data should be made. The slope of this nearly linear result is related to the channel busy time and the time that the overall handover process consumes. This model can act as a guide to flight test and network experiments for understanding this aspect of the fast mover problem.

The third critical issue is subtle and involves antenna design. Typically one-way, point-to-point, air-to-ground telemetry systems use relatively low-gain, dipole-like antennas on the munitions and high-gain, ground-based directional antennas. In a wireless network, antennas need to provide sufficient coverage for two-way communication with a reasonably large sphere of influence (as illustrated in Fig. 3). In fact, the natural two-way behavior of wireless networks can use multiple nodes to mitigate the 1/*r*-squared effect by using lower power levels at individual nodes in a multihop WMN. Since the ISM band is just above the traditional aeronautical band used for telemetry on government ranges, a modified S-band antenna was designed for the rocket provided by Point Mugu. It was planned that this antenna would provide a gain of approximately 2–3 dBi, but preflight measurements at YPG indicated that a gain of slightly over 5 dBi was achieved. This excellent antenna performance would be a key factor in the successful flight tests.

The fourth issue involves miniaturization and high-*g* survival. This issue was not directly addressed since COTS 802.11b products are based on custom packages of existing chip sets. Obviously, there are more components to a WLAN than a standard telemetry system, but miniaturization and shock hardening can be achieved by following the practices and experiences of the CTEIP-sponsored Hardened Subminiature Telemetry and Sensor System (HSTSS) program.[7] This program demonstrated that many standard commercial practices could guide component selection and assembly techniques to withstand very high shock levels. The key is to use these practices and to avoid large/bulky connectors. An 802.11b chip set could be packaged by following HSTSS chip-on-board procedures.[2]

The final issue was to consider the impact of encryption on WLAN operation. Harris Corporation has released the SecNet11 product that implements NSA Level 1 standards using a COTS chip set. Hardware and keys were only recently obtained by YPG (resources were not from the 2-RAD program). YPG and APL personnel have conducted simple tests using multiple laptops and SecNet11 cards in an attempt to reproduce throughput data similar to the type shown in Fig. 2. Because tests have not been completed, they are not reported here.

Plan and Results

A flight test plan was established using the 2.75-in. Hydra rocket system as a fast mover. This rocket was selected since it can accommodate physically and aerodynamically modified warheads. The rocket motor produces an 80-*g* launch acceleration, and the motor/warhead assembly reaches a velocity of over 600 m/s when the motor burn is completed. A typical Hydra rocket and a nominal velocity profile are shown in Fig. 5. The supersonic portion of the flight would last for only the first few seconds, but that was considered to be sufficient to validate operation as a fast mover.

The demonstration of a WLAN with a Hydra rocket raised another issue: What data would be collected? The Hydra rocket is a well-known, unclassified rocket whose performance and aerodynamic behavior have been extensively documented. It would, however, be interesting to select a sensor for use on the rocket that is "plug-and-play" to demonstrate the "computer nature" of the WLAN architecture. In general, one of the more challenging sensors for telemetry applications is a video imager. Video data, if uncompressed, can approach data rates of 10 Mbps. Typically, the imager is assumed to be "on" at all times such that a major portion of the spectrum is consumed for the entire test sequence. On the other hand, a single-board computer (SBC) with a universal serial bus (USB) host port could control camera functions (shutter speed, intensity, and data rate). Hence, it was decided to augment the 2-RAD Hydra rockets with an inexpensive, USB-compatible imager.

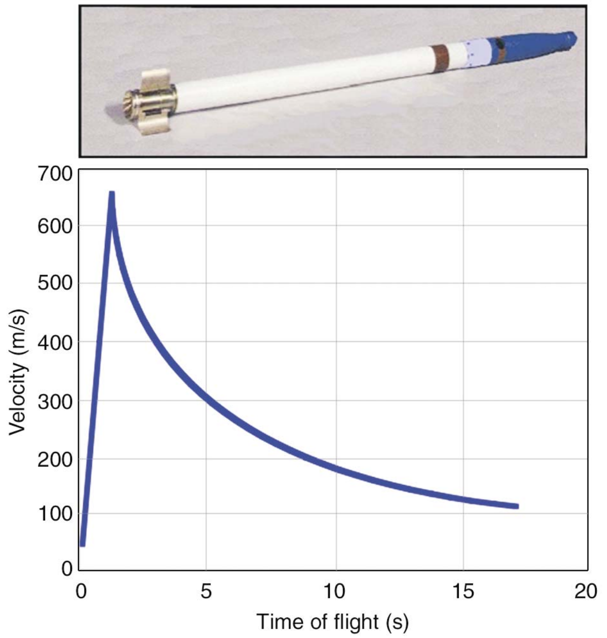


Figure 5. Typical Hydra rocket with an inert warhead (top) and a nominal velocity history (bottom).

We recognized that image quality would be poor and that blurring would occur because of the rocket spin, the limited ability to control shutter speed and intensity, and the variable ambient light conditions related to sky/ground differences. The camera was used to flood the network with packets and to demonstrate the plug-and-play philosophy. The decision to use a USB camera and an SBC with a USB host port required the use of WLAN devices that were beyond the YPG experience. A CompuLab 586CORE (133 MHz AMD ElanSC520 X-86 processor, 64 MB SDRAM, 64 MB Flash, 100/10BaseT Ethernet, and USB host port) was compatible with a Linksys WAP11 wireless AP/client board. Initially, the intent was to use a Cisco 350 PCMCIA client card, but no SBCs were identified that met the width requirement and provided both a PCMCIA slot and a USB host port. A Logitech QuickCam for the Notebooks Pro camera was used. A 0.5-W two-way power amplifier was also included to ensure sufficient transmit and receive power levels. The hardware assembly is shown in Fig. 6.

The Linksys card in the rocket and a Cisco Aironet 340 series wireless bridge (the infrastructural hardware used at YPG) were used at ARL for final assembly and

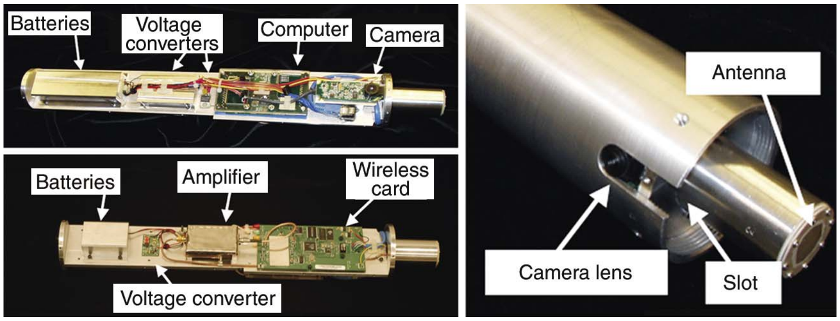


Figure 6. Hydra warhead modified with WLAN components.

system checks at short ranges before shipping. At YPG during initial setup, however, the Linksys card and YPG infrastructure would not associate at the distances required to cover the complete rocket trajectory. Many 802.11b products are known not to work well beyond 1000 ft. This situation produced a complete change in how the test equipment would be arranged and used. Several more Linksys cards were shipped overnight to YPG, and a Linksys network was configured (independent of the YPG WLAN) to support the flight tests. All ground stations were configured as clients, with the Hydra rocket configured as an AP. Hence, all ground stations could "listen" simultaneously to data broadcast from the rocket. A single channel (channel 1 at 2.412 GHz) was used. This setup emulates one that could be used to support a very long-range munition, where several unattended ground stations would be used. Figure 7 shows the network infrastructure that was used at YPG. Since the fast mover portion of the Hydra rocket trajectory is only during rocket motor burn, a series of ground stations (GSs) were located at the launcher and underneath the rocket trajectory directly in front of the launch site.

The GS1 antenna was an omnidirectional 2.2-dBi antenna, while the GS2 and GS3 sites used 11-dBi omnidirectional antennas. GS4 used a 23-dBi directional parabolic antenna. Each ground station consisted of a laptop, a Linksys WAP11 configured as a client, and an antenna (as specified above).

Commercial software (WildPackets AiroPeek Wireless Protocol Analyzer) was used to capture and analyze packets. These "sniffers" were located at sites 3 and 4, which were approximately 2 km offset from the trajectory and roughly located at trajectory midpoint and impact downrange distances. They consisted of a laptop with a Cisco 350 PCMCIA client card connected to their respective antennas. Sniffed data provided signal level, data rate, source and destination medium access control (MAC) addresses, packet type, and other information for both control and data packets.

During preflight checks, electromagnetic interference was generated when the Linksys cards were totally enclosed within the metal rocket payload. Because of the higher than expected gain from the rocket antenna, the two-way amplifier was disconnected and not used. Signal problems related to the Linksys radios (both rocket and GS radios) were suspected to be thermal in nature**.** Daytime ambient temperatures exceeding 105°F were common. The Linksys cards at GS1–3 were placed in coolers with ice packs to mitigate these unexplained disassociations. In addition, the rockets were kept out of direct sunlight until the final firing sequence.

Association of all nodes was attempted after a rocket was placed in the launcher and prior to launch.[8] Two rockets were launched with essentially identical results (Fig. 8). GS1 was associated before launch and maintained a two-way link for at least 3 s after launch, i.e., throughout the high-velocity regime of flight. The sniffer at GS4 captured packets for 33 s after each launch. GS2 and GS3 were not associated prior to launch and did not achieve association during the flight of either rocket. The data were examined only to confirm that the network was working with the rocket fully associated to GS1 and was sending video packets at the maximum rates dictated by the modeling of Fig. 2.

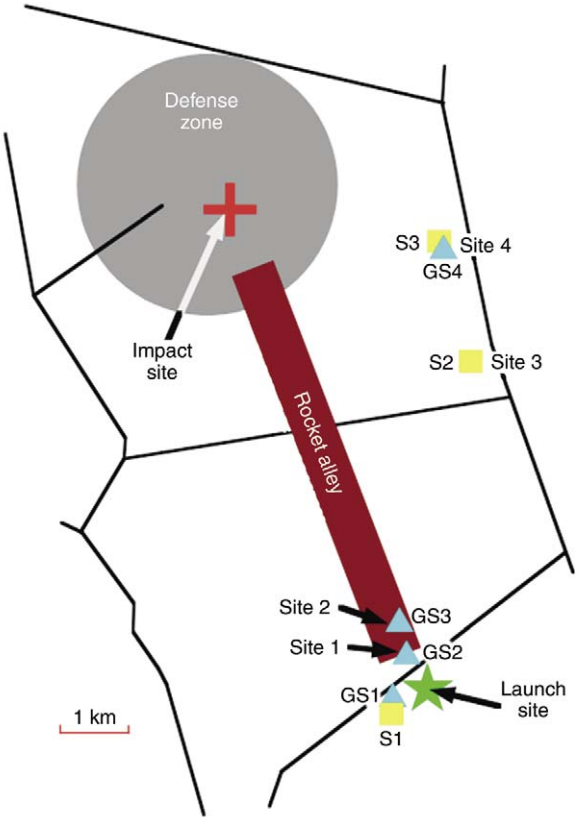


Figure 7. Test setup at Yuma Proving Ground, Rocket Alley Launch Site (GS = ground station and S = sniffer).

Figure 8. Photo frame from a high-speed camera of a Hydra rocket fired from a ground launcher.

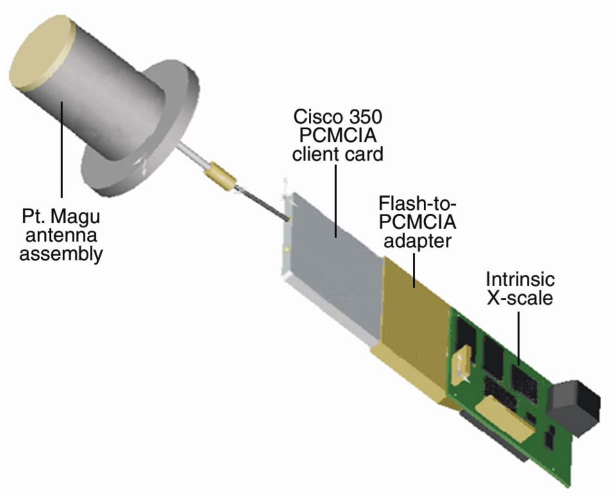


Figure 9. Suggested second-generation hardware configuration.

Hindsight, always being 20/20, suggests that the Linksys cards were the source of many, if not all, of the problems: nonassociation at long distances, incompatibility with the YPG infrastructure, electromagnetic interference internal to the rocket warhead, temperature effects, etc. Shortly after the hardware build, a new, small-width SBC was announced with integral PCMCIA and host USB ports. In addition, a faster processor and new drivers are now available. This second configuration (Fig. 9; camera not shown) should be used in any future flight efforts with munitions.

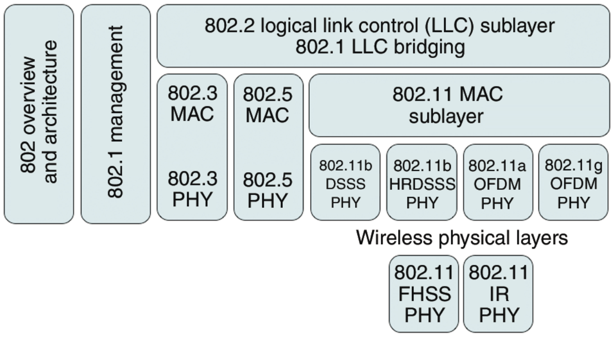


Figure 10. The 802.11 Technology Specification Family.

IMPLICATIONS AND CONCLUSIONS

The 2-RAD experiment has demonstrated that COTS 802.11b technologies can be used under the unusual Doppler conditions common to a high-velocity munition. This raises the issue of using 802.11-based technologies for military applications where volume and power are limited. Networking frameworks are typically organized using the Open System Interconnection (OSI) model that contains implementation protocols for seven layers. The 802.11 Technology Specification Family is shown in Fig. 10. This is a well-known and mature framework that follows the OSI model. It has been supported by the commercial sector and researched by the academic community. Customization of this standard in critical areas could provide products that are affordable and flexible for near-term military applications. Furthermore, since military-unique solutions are very expensive, the extension of a commercial standard for military use may provide an interesting option.

As shown in Fig. 10, the existing MAC sublayer can support six different physical (PHY) layers, including four very common spread-spectrum methods implemented in the unlicensed instrumentation, scientific, and medical band (2.4–2.462 GHz) or the unlicensed national information (5.125–5.825 GHz) band. DSSS (direct sequence spread spectrum) and HRDSSS (high-rate DSSS) are implemented in the 802.11b products, while OFDM (orthogonal frequency division multiplexing) supports the 802.11a and g products. There are two other PHY layers (FHSS, frequency hop spread spectrum; and IR) that are not normally used. The 802 MAC sublayer dictates data access and transmission permission to the PHY layer. The COTS 802.11 MAC could be customized to support a variety of highly robust military PHY layers in addition to the existing COTS PHY layers. The MAC also can be tuned to improve QoS when very high rate PHY layers are implemented.

APL researchers have embarked on a path to embed an 802.11-like MAC into a field programmable gate array (FPGA). With the MAC broken down into coded blocks on the FPGA, it can be customized to interface and perform well with new and unique PHY layers. Families of military-like PHY solutions can then be implemented. One such example is under development by the Department of Energy/National Nuclear Security Administration Kansas City Plant. This layer has already been shown to be highly flexible by using various modulation schemes for spectral efficiency. It can also be frequency-tuned from 900 MHz to 2.5 GHz with a variable output power amplifier (up to 10 W) in an over-the-air controlled mode. As FPGA and similar programmable logic technologies rapidly expand, they will provide sufficient memory and computation engines such that many of the baseband functions can be co-located with the MAC, thus providing a high degree of integration and relatively straightforward miniaturization.

These solutions should provide less than the planned size and mass goals set for the Joint Tactical Radio System (JTRS) Cluster 2 and 5 options. In addition, JTRS does not specifically have a plan to provide weapon data link network capabilities. An 802.11-like product using an FPGA-based MAC could point the way to a solution. Such a system could be used to network small, unmanned systems (air, ground, or sea surface). It would also be well suited for use as a weapon data link network where small, precision-guided munitions are networked to the shooter and to a ground–air coordinator. The 2-RAD program started within the test community to provide a unique capability for monitoring airborne munitions, but it has since initiated a concept to provide tactically acceptable, high-data-rate, miniature, and affordable network devices for military applications where only small volumes are available.

REFERENCES

[1] Kasch, W., Burbank, J., Andrusenko, J., and Lauss, M., "Physical Layer Performance of the IEEE 802.11b WLAN Standard in Outdoor Applications: A Case Study in Yuma, AZ," in *Proc. 12th Virginia Tech/MPRG Symp. on Wireless Personal Commun.*, pp. 7–19 (5–7 June 2002).

[2] D'Amico, W., Stadter, P., and Lauss, M., "Practical Experiences with 802.11b WLANs," in *Proc. 2002 Int. Telemetering Conf.*, pp. 293–301 (Oct 2002).

[3] D'Amico, W., Burbank, J., Kasch, W., Andrusenko, J., and Barrett, G., "A WLAN Concept for Data Acquisition from Multiple Target Vehicles," in *Proc. 2003 Int. Telemetering Conf.*, pp. 356–363 (Oct 2003).

[4] Kasch, W., Burbank, J., and Andrusenko, J., "Performance of the IEEE 802.11b WLAN Standards for Fast-Moving Platforms," in *Proc. 2003 Int. Telemetering Conf.*, pp. 345–355 (Oct 2003).

[5] Bamberger, R., Barrett, G., Burbank, J., Nichols, R., and Lauss, M., "Wireless Local Area Network for Data Telemetry from Fast Moving Nodes," in *Proc. 2002 Int. Telemetering Conf.*, pp. 275–284 (Oct 2002).

[6] Barrett, G., Bamberger, R., D'Amico, W., and Lauss, M., "Analytical Model for Handoff of Fast Moving Nodes in High Performance Wireless LANs for Data Telemetry," in *Proc. 2003 Int. Telemetering Conf.*, pp. 374–381 (Oct 2003).

[7] Schneider, D., and Colangelo, R., "Instrumentation – Make It Common," in *Proc. 2001 Int. Telemetering Conf.*, pp. 366–372 (Oct 2001).

[8] Bamberger, R., Barrett, G., D'Amico, W., and Lauss, M., "Experiment Demonstrating the Use of a WLAN for Data Telemetry from Small, Fast Moving Nodes," in *Proc. 2003 Int. Telemetering Conf.*, pp. 382–391 (Oct 2003).

ACKNOWLEDGMENTS: This article is based on the work of a large team that supported a 3-year effort. Jack Burbank, William Kasch, and Julia Andrusenko (APL) conducted a site survey of the Yuma Proving Ground wireless network (locations, equipment, and topology) leading to link analyses that explained and verified the long-distance physical layer performance of the network. They were also responsible for a hardware test bed that was used to mitigate risk prior to a critical flight test. George Barrett (APL) was instrumental in simulations at the network layer. This article reviews concepts from one of his analyses for handover of a "fast moving" node. Robert Bamberger and Cash Costello (APL) were responsible for the selection and integration of most of the flight hardware components, including the wireless network card, the single-board computer, and the software to accommodate the onboard miniature camera. Marshall Childers led a team of engineers and technicians from the U.S. Army Research Laboratory (Weapons and Materials Research Directorate, Aberdeen Proving Ground, Maryland). They were responsible for the flight hardware design and the integration of the major subsystems into the rocket hardware. Marvin Ryken and Richard Davis (Naval Air Systems Command, Point Mugu, California) designed and built the antenna for the flight hardware, which was a key element in the success of the flight test. Finally, Charles Ramsdale (test director at YPG) and the YPG crew provided excellent support for a unique sequence of test operations and firings. The labors of these team members are documented in the publications referenced in this article. As usual, these documents do not do justice to the dedication and contributions of the group. The authors are indebted to all those cited.

THE AUTHORS

William P. D'Amico led the Two-Way Robust Acquisition of Data Team. Dr. D'Amico is a member of APL's Principal Professional Staff and is a Program Area Manager in the Research and Technology Development Center. He has an extensive background in the research and development of unique weapon technologies, especially in the areas of microelectromechanical systems, sensors, and telemetry. Dr. D'Amico and **Mark H. Lauss** of the Army's Yuma Proving Ground proposed the 2-RAD concept as an extension to existing wireless local area network (WLAN) applications. Jointly, they organized the program plan, assembled a multi-organizational team, and successfully executed the program. Mr. Lauss is the architect for a unique implementation of an 802.11b-based WLAN for real-time, long-distance, *ad hoc* data acquisition at YPG, where he is a member of the Instrumentation Development Branch. He has served in the development of data acquisition, reduction, and analysis systems for DoD weapon systems. He has held faculty positions at Arizona Western College and the University of the Virgin Islands in information technology and data communications. The team can be reached through Dr. D'Amico. His e-mail address is bill.damico@jhuapl.edu.

William P. D'Amico

Mark H. Lauss