SAND2015-4812C

A Comparison of Approaches to Short-Range Wireless Communications in Nuclear Facilities

Jay K. Brotz, Sandia National Laboratories, Albuquerque NM

Faranak Nekoogar, Lawrence Livermore National Laboratory, Livermore, CA

James R. Skorpik, Pacific Northwest National Laboratory, Richland, WA

As interest in unattended and automated monitoring increases in the fields of nuclear arms control, international nuclear safeguards, and nuclear materials management, technological concepts relying on wireless communications are discussed increasingly. In this paper we discuss the benefits of the potential applications of wireless communications along with the challenges in these environments. We then discuss five approaches to short-range wireless communications for use in nuclear facilities, including active radio frequency identification (RFID), passive RFID, low-frequency magnetic induction (RuBee), optical, and acoustic communications. Wireless monitoring devices could provide constant updates of inventory, active sealing, and sensing of area access without potentially challenging facility modifications to deliver power and networking infrastructure. Both active and passive radio frequency (RF) communications have been established in other fields, but are relatively new to use in nuclear facilities. Low-frequency magnetic induction communications is a fairly new technology that has been demonstrated in some applications and has some promise in being certified for use near explosives. Optical and acoustic communications are new concepts for short-range wireless communications that are currently being developed.

Introduction

Technological concepts for monitoring in nuclear facilities, for applications in international nuclear safeguards, nuclear materials management, or future arms control concepts, are becoming increasingly capable. One capability area that has emerged in these concepts over the past decades and that presents unique challenges is wireless communications [1]. There are several advantages to wireless communications for such monitoring equipment. Persistent communications allows transitory devices, such as active tags and seals that might be attached to containers that move about, to transmit information at more frequent intervals without manually obtaining a readout by physically connecting a reader to the device. Fixed devices, such as radiation monitors, can be installed more easily and inexpensively and with fewer facility modifications if network cabling is not required. Monitoring devices in high radiation areas can be queried without any personnel receiving a radiation dose, improving the safety of those involved. Despite the challenges with wireless devices (e.g., information security, explosive safety, and the necessity of being powered by batteries), there are significant benefits that will likely lead to increased adoption.

Several methods of wireless communications have been developed for use in devices related to international nuclear safeguards, nuclear materials management, and arms control. Five recently investigated methods are discussed in this paper: active radio frequency identification (RFID), passive RFID, RuBee, optical methods, and acoustic methods.

Active Radio Frequency Identification

Active RFID is also designated as “aRFID.” The “active” preface is to distinguish it from “passive” RFID. The term RFID alone is typically associated with the RF technology that replicates an optical bar code. These RFID technologies, like a barcode, require no integral power source such as a battery and are thus both “passive” technologies. The bar code utilizes the incoming optical signal to reflect back a unique identification (ID) pattern. The passive RFID utilizes an incoming RF interrogation signal to scavenge power to “backscatter” back a unique digital ID.

The aRFID devices use a small, smart RF electronic chip called a transceiver, which can both transmit and receive RF signals. These devices span a programmable frequency range typically from 400 MHz to 3 GHz. This allows the developer or user the ability to select a frequency for the application requirement. For example, lower frequencies have longer send and receive ranges and will penetrate and pass through objects better than higher frequencies; for example, a military application uses 433 MHz RF tags for logistic tracking of metal sea containers. However, high frequencies can accommodate higher data rates and are better suited for streaming data (e.g., Wi-Fi and Bluetooth at 2.4 GHz). The aRFID devices can support custom communication protocols or run on industry standards such as IEEE 802.15.4g [2], ZigBee, Wi-Fi, and Bluetooth. The majority of aRFIDs operate at low transmit power (<10 mw) in FCC-defined Industrial Scientific & Measurement (ISM) bands that are license-free. To date, there are over ten mainstream companies that sell RF transceivers at unit prices under $10. They are packaged as an integrated circuit (IC) commonly known as a mixed signal application-specific integrated circuit (ASIC) with a variety of modulation schemes and automatic error correction. Package size typically is 5 mm × 5 mm with a pin count of 32.

An RF transceiver alone does not make up an aRFID. There is always a smart controller that handles the setup and the command and control of the RF device. Usually the controller is a microcontroller with the popular choices being the MSP430 family from Texas Instruments and similar devices from Microchip. Microcontrollers from both of these manufacturers are extremely low power for applications requiring battery-operated mobile aRFID. The microcontroller when combined with sensors performs data acquisition, data analysis, data storage, and off-board connectivity with the RF link. When queried by an enabled RF host (known as a reader or integrator) such as a tablet, the aRFID device can upload data back on the RF link. Other options are for data to be RF transmitted either from a “sensor alarm” event or on an internal repetitive time-based trigger signal. A periodic RF send can also serve as a "heartbeat" or "state-of-health." The majority of sensors now have digital interfaces such as Inter-Integrated Circuit (I^2C) or Serial Peripheral Interface (SPI) that interface directly into the microcontroller. Of those sensors that have analog outputs, the microcontrollers have internal high-speed analog-to-digital converters (ADC). The controllers also have a suite of internal features such as real-time clock, cyclic redundancy check (CRC), counters, and AES-256 encryption.

The items shown in Figure 1 represent a custom aRFID unit from Pacific Northwest National Laboratory (PNNL). The round 1-inch board is the RFID itself with the main microcontroller, data storage, near field communications (NFC) short-range wireless setup link, acoustic sensor, and coin cell battery. The square board is the RF board and, when mated to the RFID board, it becomes the aRFID. When packaging the device into a case, it can play the role of a "pod" or "mote," which can become a component in a distributed sensor network—also called a mesh network. With an appropriate embedded protocol, the sensors can communicate with each other to share data processing and to also extend the overall RF range. Mesh networks find applications in instrumented buildings for monitoring energy usage by using simple, low-cost temperature and humidity sensors.

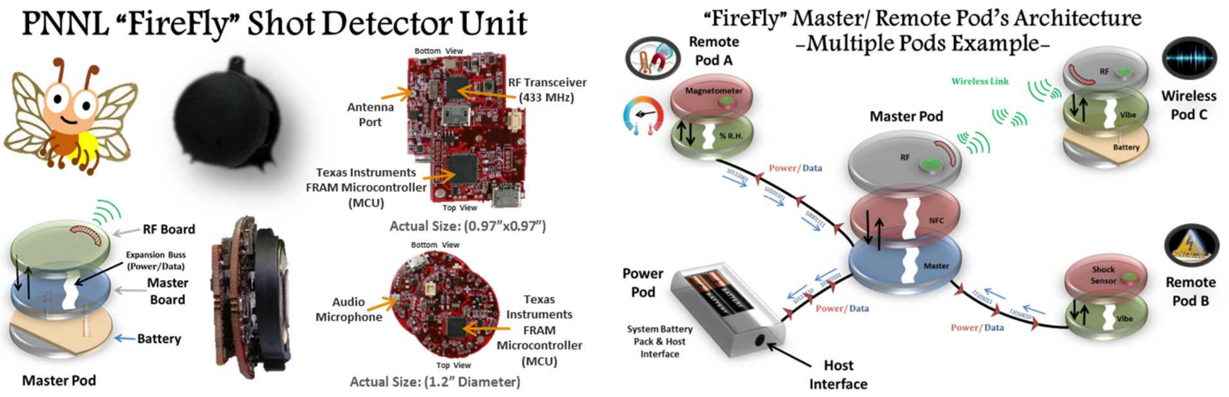

Figure 1: PNNL Active RFID Tag

A PNNL past military requirement was for a next-generation aRFID tag and reader design using an open source ISO18000-7 RF protocol [3]. The U.S. Army has been using logistic tags placed on sea containers to track logistics worldwide. The aRFID tags contain the manifest of all the items that are located within a tagged shipping container. Active RFID readers are located at key choke points such as warehouses, loading docks, post entrance gates, and on train railways. PNNL produced and validated the items in Figure 2, which became a reference design for vendors to use for developing the product.

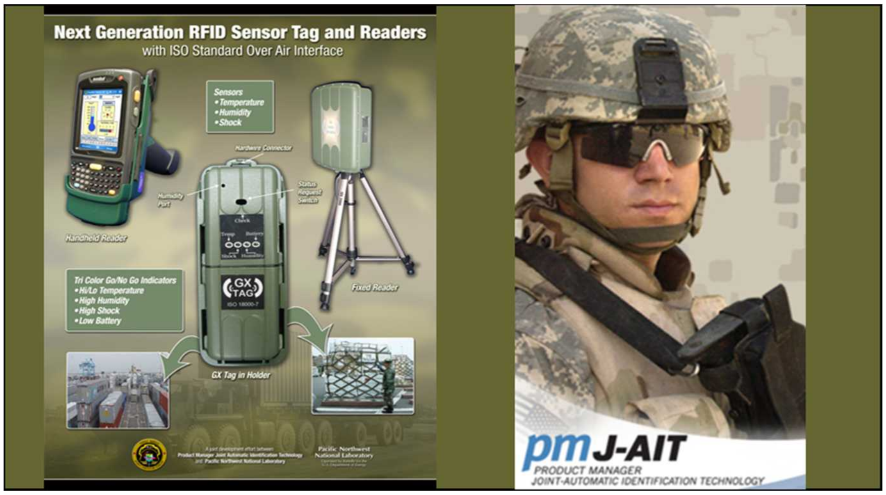
Next Generation RFID Sensor Tag and Readers
with ISO Standard Over Air Interface
Sensors
• Temperature
• Humidity
• Shock
Hardware Connector
Humidity Port
Status Request Switch
Handheld Reader
Check
Temp
Battery
Shock
Humidity
Tri Color Go/No Go Indicators
• Hi/Lo Temperature
• High Humidity
• High Shock
• Low Battery
GX TAG
ISO 18000-7
Fixed Reader
GX Tag in Holder
A joint development effort between
Product Manager Joint Automatic Identification Technology
and Pacific Northwest National Laboratory
Pacific Northwest National Laboratory
pmJ-AIT
PRODUCT MANAGER
JOINT-AUTOMATIC IDENTIFICATION TECHNOLOGY

Figure 2: PNNL RFID Sensor Tag and Reader

Passive Radio Frequency Identification

In this section we report on a new advanced secure passive (battery-free) RFID tag integrated with a fiber optic seal and a variety of sensors that allows real-time monitoring of items through secure wireless communications that employs AES encryption and dynamic authentication. The passive RF Tag-and-Seal-and-Sensor (TSS) introduced in this paper is a unique system developed specifically for international safeguards by Lawrence Livermore National Laboratory (LLNL) and its industrial collaborator, Dirac Solutions Inc. (DSI). The TSS allows remote monitoring of a fiber optics seal status, data from a variety of sensors (including temperature, accelerometer, and gamma radiation levels), as well as unique ID using a secure AES encrypted and dynamically authenticated wireless channel without the need for a battery. In addition, the TSS has an optional physical security feature, which is called "self destruction upon removal." This unique tamper resistant feature allows the RFID chip to break irreversibly with any attempt to remove the tag from the container. Figure 3 shows the concept of operation for continuous monitoring and on-demand monitoring using TSS.

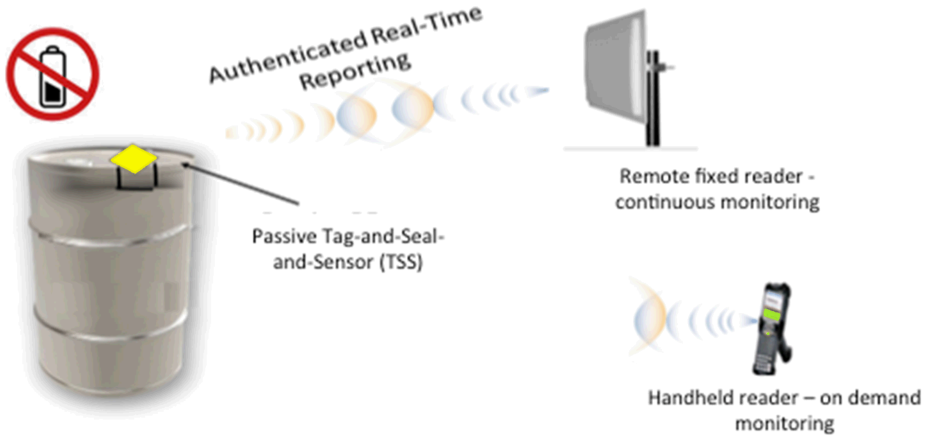
Authenticated Real-Time Reporting
Remote fixed reader - continuous monitoring
Passive Tag-and-Seal-and-Sensor (TSS)
Handheld reader – on demand monitoring

Figure 3: Concept of Operations for Long-Range Passive (Battery-Free) Tag-and-Seal-and-Sensor with Data and Physical Security

As shown above, similar to active seals, TSS allows real-time monitoring without the need for batteries, hence eliminating the concerns with limited and unpredictable lifetime of the battery-operated tags. As the long-term storage of special nuclear material (SNM) might last for several years, the TSS extends the lifetime of the physical seals, tags, and sensors indefinitely in the monitoring areas. Furthermore, the data and physical security features of TSS are countermeasures against the two typical RFID threats: (1) man-in-the-middle threat, and (2) cloning threat. Therefore, the TSS system is transformational in addressing a critical need in safeguards and warhead monitoring areas for long-term real-time and on-demand monitoring.

It is important to note that TSS units do not actively transmit any signals and their communications with a reader are based on "backscattered technology." This means that one reader actively transmits signals and any number of TSS units only reflect or modulate the transmitted signal (like a mirror). So the level of active signal transmission is much less in TSS systems, a feature that can benefit nuclear facilities with respect to safety and security issues and increase the noise floor caused by active RF transmission of hundreds or thousands of tags.

The TSS system consists of a TSS sensor unit and an RFID reader, where one reader is capable of reading thousands of TSS units. The data collected by the reader from TSS units will be displayed on a monitor screen in a command and control station, or a mobile unit, such as a tablet, for an inspector's convenience.

TSS units harvest power from the incident RF signal from their remote reader antenna. In areas outside the view of the reader antenna, the TSS is equipped with an optional external battery data logging unit to record the tamper event and report to the reader antenna as soon as it enters the reader remote powering zone. The external optional battery is only for recording data outside the reader antenna powering zone (i.e., transportation activities). This optional, external battery when used, does not convert the tag to an active tag, as there is no active transmission from the battery and this optional battery is only for the purpose of data logging. Unauthorized removal of the battery case will be recoded as tamper in the tag memory.

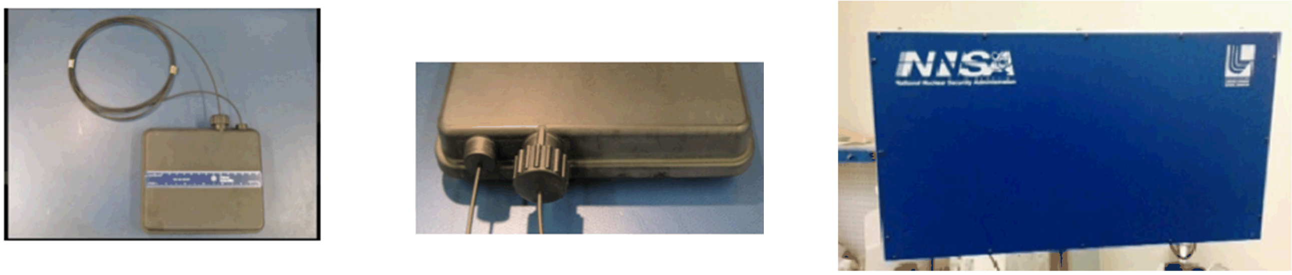

Figure 4: (Left) The Passive TSS and detail of Weatherproof, Field-Serviceable Fiber Ingress/Egress, (Right) TSS Reader

The standalone reader unit includes a customized secure RFID reader capable of encrypted and dynamically authenticated communications, specialized dual polarity antenna for seamless detection of TSS units regardless of their orientation, and a single-board computing platform that allows for high level signal processing for improved signal-to-noise ratio. This reader is easily deployable in various facilities, and includes a backup emergency battery for continuous operation when there is an interruption of power in the facility. It is capable of networking through Ethernet for reporting to centralized data collection and analysis centers. Multiple readers can be networked for large facility monitoring. DSI is also pursuing development of TSS units with internal Application Specific Integrated Circuit (ASIC) that can improve the range and reduce the size of the system.

RuBee

RuBee is a two-way, active protocol for communications using long wave (LW) magnetic signals with a 131 kHz carrier [4]. It is described in the open standard IEEE 1902.1 [5]. While the data rate is small compared to RF protocols (approximately 1200 bits per second) it has the advantages that it has been demonstrated to be intrinsically safe around explosives [6] and has a relatively small range (the magnetic signal drops off with the cube of the distance, as opposed to the square of the distance with the electrical signal) giving it improved information security over an RF tag. In addition, RuBee signals can travel through metal, even using large metal objects to extend the range of a signal in a monitored area. This is due to the fact that magnetic signals are not attenuated by metal like electrical signals are. In fact, RuBee signals are not affected by anything in their environment, including walls and other building features, equipment, or people.

Though the antennas needed to communicate to RuBee tags from a base station grow fairly large in order to reach even modest ranges, the antenna design is a wire loop, which lends itself well to many facility configurations. Large loops can be placed on the floors, walls, or ceilings of facilities in an unobtrusive way that leads to very high tag read success rates. Sandia National Laboratories carried out a preliminary investigation using RuBee tags on mock nuclear weapons containers in a test bunker facility using large floor loops for the antennas as shown in FIGURE. The team found that the tags communicated with high reliability with the base station despite being directly on the metal surface of the container. In addition, multiple floor loops were used to identify the location of specific items of interest within the bunker, and a loop near the door was used to aid in inventory management by alerting the system that something new has come into the bunker or something existing has exited.

The best example of use of RuBee in a nuclear facility to date is a five-year assessment carried out at the Pantex Plant in Amarillo, TX, to identify technologies that can automatically identify tagged tooling and other items. RuBee tags provided by Visible Assets, Inc., were chosen as the preferred mechanism and fully evaluated. They were found to be intrinsically safe for use near nuclear weapons, in addition to having no security risks and 100% read rates in harsh environments (such as near water or steel) [7].

Further work is necessary to take full advantage of the RuBee communication method as a general, two-way system that is flexible for any safeguards, nuclear materials management, or arms control use.

Optical and Acoustic

There are concerns about the use of RF transmissions in certain environments, especially concerning explosive safety and information security. Sandia National Laboratories sought to provide technical options for short-range, wireless communications without using RF and developed systems using both optical and acoustic methods. Both methods are more directional in nature than previously used RF approaches and as such come with modifications to their uses and communication node configurations. Whereas omnidirectional communications may be made with a single coordinator (fixed base station) anywhere in a room and many nodes (transitory devices) in any location and orientation, directional communications need line-of-sight channels through which to communicate. For our development of optical and acoustic short-range networks, this has meant several coordinators mounted directly above the places in a room where the nodes are expected to be, and nodes placed on top of items under containment with their transmitters pointed directly up, as shown in a top-down view of a room with multiple monitored items in Figure 5. This has the benefit that position within a room can be identified, if each coordinator is polled separately.

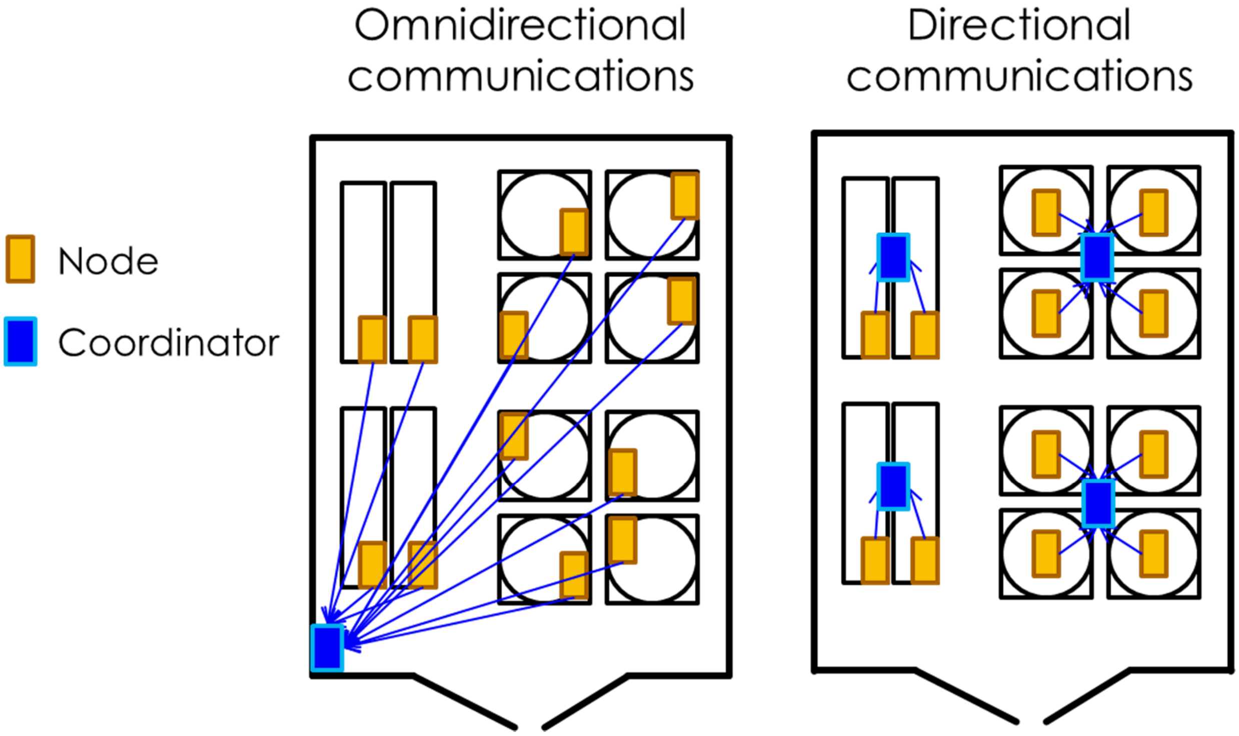

Figure 5: Configuration Differences between Omnidirectional and Directional Communications

The optical transceiver is designed with the infrared (IR) transmitters and receivers that were designed for data transmission for remote controls. The directionality of the IR transmit ter and IR receiver are shown in Figure 6 and Figure 7, respectively. The range seen is about 23 feet with a clear channel straight on and 15 feet with fluorescent lights on, though the placement, type, and intensity of lights will likely affect the achievable range differently. The maximum data rate achievable with these transmitters and receivers is 4800 bits per second. The data is modulated with on-off keying (OOK) in which eight light pulses represents a "1" and no light represents a "0".

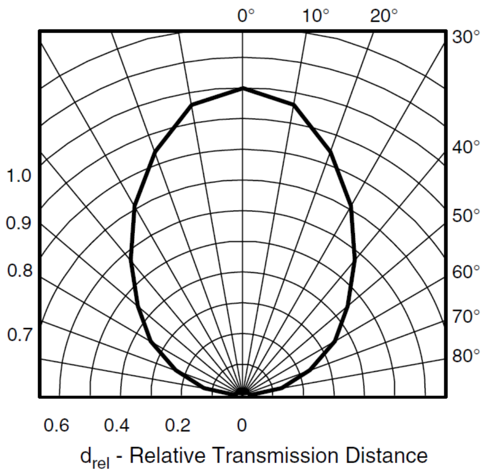

Figure 6: Infrared Receiver Directionality

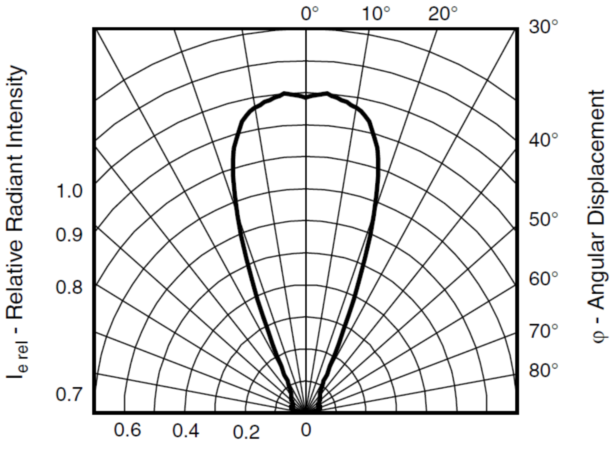

Figure 7: Infrared Transmitter Directionality

The acoustic transceiver is designed with ultrasonic transducers that are more commonly used for proximity sensing and ranging. While underwater ultrasonic communications are common [8], very little research has been done in ultrasonic air communications [9]. Our approach is outlined in the block diagram in Figure 8. The choice of differential quadrature phase-shift keying (DQPSK) was driven by robustness to noise and Doppler frequency shifts (hence phase-shift keying rather than amplitude- or frequency-shift keying) and higher data rates (hence quadrature rather than binary). Some designs use digital-to-analog converters (DACs) on the transmitter and analog-to-digital converters (on the receiver), though we have had success with audio codecs sampled at least twice as fast as our signal.

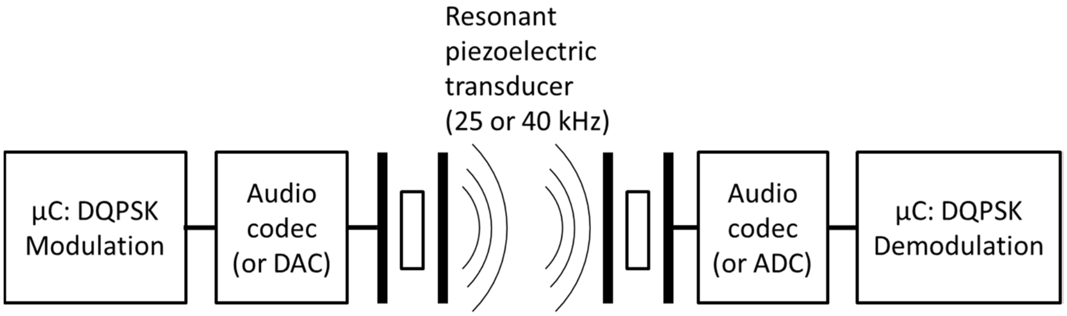

Figure 8: Block Diagram of Ultrasonic Transmitter and Receiver

We have designed transceivers with common, inexpensive 25 kHz and 40 kHz piezoelectric transducers being driven at voltages low enough that no amplification is necessary. Using audio codecs (sampled at 92 kHz) to drive and receive the transducers, at a maximum drive voltage of 1 V, we have observed successful communications at straight-line distances of up to 150 feet. However, we have observed that with increasing distance (moving the signal closer to the noise) the data rate must be reduced to result in communications without bit errors. At 150 feet, a data rate of about 50 bits per second is achievable, while at distances of about 20 feet, data rates up to 1500 bits per second have been observed without bit errors.

The biggest challenge with the ultrasonic transceiver is multi-path interference. This is mitigated with careful placement of the coordinator with respect to the expected locations of the nodes. If the channels are clear with few nearby flat surfaces that are parallel to the direction of communications, multi-path interference is not a significant issue.

The development of relatively simple optical and acoustic approaches to short-range, wireless communications shows promise for small networks where RF is not appropriate. While these technologies have been developed and tested in an arms control context, further testing is necessary to understand how robust these approaches are.

References

[1] N. C. Rowe, J. R. Younkin, C. A. Pickett and M. Whitaker, "Radio-frequency (RF) devices for safeguards: where we are and where we need need to go," in *INMM Annual Meeting Proceedings*, Oak Ridge, TN, 2011.

[2] IEEE, *IEEE 802.15.4: Standard for local and metropolitan area networks -- Part 15.4: Low-rate wireless personal area networks (LR-WPANs),* 2011.

[3] *ISO/IEC 18000-7:2014 Information technology -- Radio frequency identification for item management -- Part 7: Parameters for active air interface communications at 433 MHz,* 2014.

[4] D. C. Wyld, "RuBee: applying low-frequency technology for retail and medical uses," *Management Research News,* vol. 31, no. 7, pp. 549-554, 2008.

[5] *IEEE 1902.1: IEEE Standard for Long Wavelength Wireless Network Protocol,* 2009.

[6] Visible Assets, Inc., "U.S. Department of Defense determines RuBee (IEEE 1902.1) wireless has a HERO, zero safe separation distance (SSD) from fused ordnance," Stratham, NH, 2012.

[7] L. L. Duckworth, "Advanced inventory and materials management at Pantex," B&W Pantex, LLC, Amarillo, TX, 2011.

[8] L. E. Kinsler, Fundamentals of Acoustics, 4th ed., Hoboken, NJ: John Wiley & Sons, 1999.

[9] C. Li, D. A. Hutchins and R. J. Green, "Short-range ultrasonic communications in air using quadrature modulation," *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control,* vol. 56, no. 10, pp. 2060-2072, 2009.