NIST Technical Note 1604

Practical Challenges in Wireless Sensor Network Use in Building Applications

William M. Healy
Won-Suk Jang

NIST National Institute of Standards and Technology • U.S. Department of Commerce

NIST Technical Note 1604

Practical Challenges in Wireless Sensor Network Use in Building Applications

William M. Healy
Won-Suk Jang
Building Environment Division
Building and Fire Research Laboratory

September 2008

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Technical Note 1604
Natl. Inst. Stand. Technol. Tech. Note 1604, 12 pages (September 2008)

Abstract

While wireless sensor network technology has advanced in recent years, potential users of these systems in buildings still have concerns about their application. This report summarizes results of a literature survey and interactions with building industry professionals that were designed to gain an understanding of the barriers to adoption of wireless sensors in buildings. Users have concerns with cost, reliability, power management, interoperability, ease of use, and security. This work is meant to set the stage for the development of measurement techniques that will provide better metrics for how wireless sensor systems perform in actual building applications.

Keywords

Wireless; sensor; building technology; building monitoring; building control

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. Introduction

Wireless communication technology opens up a wealth of opportunities for monitoring and controlling conditions within a building by easing the installation of sensors, actuators, and controllers. While building automation systems can currently operate heating, ventilating and air conditioning (HVAC) and lighting systems efficiently, the presence of more sensors and actuators throughout a building could further improve the comfort of occupants while reducing energy consumption. Additionally, extra sensors can augment the safety and security systems in a building. Wireless technology enables increased numbers of sensors, actuators, and controllers in a building by drastically reducing the cost and effort of installation. The elimination of signal wire also provides greater flexibility within spaces with adaptable configurations and permits sensing and control in historic buildings without damaging the structure.

The emergence of wireless technology in building applications is evidenced by the numerous articles that have documented the use of wireless in buildings [1-6]. The technology promises to play an even larger role in building operations with the recent efforts by the American Society of Heating, Refrigerating, and Air-Conditioning Engineers' (ASHRAE) Building Automation and Control Networks (BACnet) committee to develop methods to expand a BACnet network with ZigBee wireless mesh networks [7].

Despite the apparent ease with which people can deploy wireless sensors and actuators in a building, engineers and operators still have concerns and questions regarding the use of wireless technology in buildings. A measurement need identified in the Assessment of the United States Measurement System stated that "Potential end-users of wireless sensor networks have shown reluctance towards using them in a wider range of applications because of uncertainty in the reliability of the wireless links."[8] The uncertainty in reliability is but one aspect of wireless sensors that inhibit their use. This paper summarizes some of the most critical issues with wireless system performance that inhibits their adoption.

This work is part of an effort by NIST to develop measurement systems and methods to better predict the performance of wireless sensor and control networks in building applications. A recent Department of Energy (DOE) roadmap entitled "Advanced Sensors and Controls for Building Applications" [9] recommended the development of an Operational Test and Evaluation Program for sensor systems that would "provide systematic and comparable testing, employ and develop testing protocols that are standards based, and help to identify environmental vulnerabilities and operational limitations." It is anticipated that these measurements will provide potential users of wireless technology a clear metric as to how the technology will perform in a particular application and will provide vendors of wireless technology a design target. The first part of the effort is to identify the key challenges in using wireless technology in building applications to ensure that the work addresses the critical barriers to the use of wireless sensors and controls when they can provide a benefit to the building owners and occupants.

Because of the variability in both building types and application requirements, the development of measurement methods that can be used to assess the performance of wireless sensor networks in buildings is extremely challenging. The proposed measurement methods or testbeds should be broad enough to apply to a wide variety of use cases, yet they must be simple enough to provide a useful metric with minimal effort.

2. Background

To determine these needs, NIST surveyed the literature and interviewed people involved in building operations and wireless products. Those people interviewed included representatives of large building automation companies, wireless equipment manufacturers, engineering consulting and design-build firms, building maintenance departments, and research organizations. These people were typically asked about the challenges or concerns that they see in using wireless sensors and controls in buildings. Additionally, NIST asked those people about the types of measurements that they could envision that would give users more confidence in the performance of a wireless system. Responses were consistent, and the concerns expressed by the industry representatives are captured in the following section.

As a precursor to this discussion, Table 1 presents a list of concerns that inhibit the use of wireless sensor networks for a variety of industries as documented by a recent market report [10]. These concerns are listed in order from most commonly cited to least cited. Many of the issues pointed out in this study, such as reliability, interference, ease of installation, and cost are consistent with the findings presented here that are specifically related to the building industry.

Table 1 Concerns expressed regarding the use of wireless sensor networks [10].

Ranking	Concern
1	Lack of installation ease/ease of use
2	Lack of/concerns about reliability or robustness
3	Concerns about interference
4	Lack of standards/interoperability
5	Power consumption still too high/battery life too short
6	Overall costs too high
7	Lacking encryption and other means of security
8	Bit rate too low/high
9	Applications not understood/clearly defined
10	Size of node/endpoints too big

NIST plans to address these obstacles to the use of wireless technology in buildings by developing measurement data, methods, or testbeds that will enable users to predict the performance of a wireless system for a building application. While each building and application is different, it is anticipated that a consistent set of metrics will provide useful information in designing the layout of the wireless network for a desired level of service.

3. Practical Challenges

Cost

A major advantage in using wireless sensors and controls over wired ones is the decreased installation cost. This decreased installation cost, however, is countered by a higher first cost of the equipment. Wireless sensors must possess radios to transmit the data, software to process the data into radio signals, and software to coordinate the transmittal of data through the wireless network. These hardware and software features increase the initial cost of the sensor and control products. Additionally, the sensors may require added maintenance cost, most notably to change any batteries that are used to power them. Users need a clear way to compare the cost of a wired sensor and control network to its wireless equivalent. The comparison requires data on the cost of the hardware, the cost to install the system, and the cost to maintain the system.

Wiring costs can be difficult to quantify. Kintner-Meyer and Brambley [1] report values of $7.21 and $2.20 per linear meter for wiring in existing construction and new construction, respectively. Another study reports that 75 % of the cost to install a sensor network for structural health monitoring was related to the wiring [11].

Kintner-Meyer and Brambley presented the plot shown in Figure 1 to provide a gauge of the cost effectiveness of a wireless monitoring system over a wired one based on first costs of the sensor systems. A ratio above 1 indicates that a wired system is more cost effective. The cost ratio depends upon the type of construction, the size of the building, and the need for radio repeaters. This chart was developed based on the cost of wireless equipment in 2001. Promised declines in the prices of the radio hardware should make wireless more competitive.

The key factor in assessing the cost of a wireless system is the number of nodes and repeaters that are needed. The number of nodes will be based on the desired resolution in a particular application, while the building construction, size, and wireless transmission scheme will dictate the need for repeaters. Designers may need to make tradeoffs to achieve a desired price point for a particular installation.

Overall, an installer of a wireless system must see that this system will cost less than a wired system that performs the same function. A clear metric on assessing the costs of a wired system versus a wireless system would greatly help users see financial benefits or drawbacks of a wireless system.

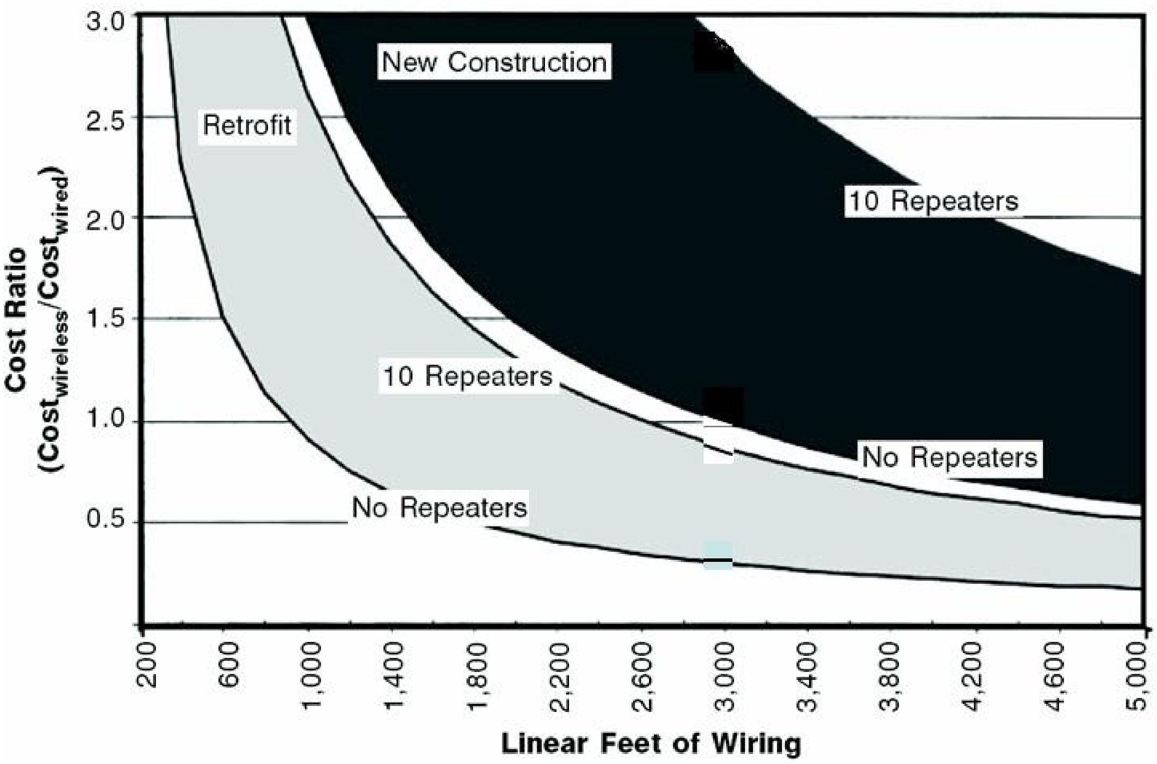


Figure 1 Plot of First Cost Ratio vs. linear foot of wiring (From [1])

Reliability

One of the major concerns of potential users of wireless technology in buildings is the reliability of the wireless system. At its most basic level, a customer of a building automation system expects the same level of reliability with a wireless system as is seen with wired systems. For a broader range of applications, that reliability requirement may either be more or less severe. In a qualitative sense, reliability means that the desired data are sent to the receiver at the desired times, with little delay, and with minimal measurement error.

Defining reliability is itself a difficult endeavor. The following discussion will describe different aspects of reliability and factors that affect reliability.

Accuracy

As used here, accuracy refers to the sensor itself as opposed to the data transmission over the airwaves. Accuracy problems, therefore, are not specific to wireless sensor networks but are a concern with all sensor networks. Wireless sensor networks may help ameliorate some of the effects of inherent sensor error by more easily allowing redundant measurements. Such architecture could help increase the overall accuracy of the data coming from the sensor network.

Noise may affect sensor readings by modifying the analog signal generated by the transducer. Typically, sensor readings will be converted from analog to digital format at the sensor node before being transmitted wirelessly. Because the data are transmitted digitally, the change in accuracy of the measured value because of noise interfering with the data transmission is less of a concern. Typically, corruption of the data stream will result in values that are noticeably in error.

Signal coverage through building materials

A large factor in the reliability of a wireless link is the propagation of the signal through different construction types and the resultant coverage of the wireless signal. The maximum allowable distance between the transmitter and the receiver is often reported only for situations in which there are no obstructions between the two radios (e.g., in an open field). The presence of walls, floors, ceilings, and furnishings greatly complicates the prediction of propagation. Metal walls tend to stop propagation of radio-frequency (RF) waves, while other materials attenuate the signal to varying degrees. The configuration of walls and partitions, however, may occasionally provide tunnels through which the radio waves can propagate. An added concern among users involves the effect of changing configurations of spaces, such as the movement of bookshelves, on propagation. An assessment of the robustness of the installation to such changes is vital. Complicating matters is the fact that different frequencies and transmission power levels may respond in different manners in different buildings. Without clear guidance on the transmission distance in real applications, users of wireless sensors may either be forced to place more repeaters than necessary (and, hence, increase the cost of their system) or run the risk of locating sensors in places where their data will not be accessible.

Interference

Even if a structure does not change its physical configuration, changes in the presence of devices that emit RF radiation may interfere with the propagation of signals from wireless sensors and control nodes. Buildings possess many devices that emit RF pulses, whether they are engineered to emit those pulses or are simply byproducts of other operations. Many of the devices being constructed as part of wireless sensor networks operate in the 2.4 GHz Industrial, Scientific, and Medical (ISM) Band. Several other bands are available in the spectrum for unlicensed use throughout the world. For example, ISM bands exist at 900 MHz and 5.8 GHz. The advantage of the 2.4 GHz band, however, is that it is valid worldwide, whereas other bands differ slightly from region to region. Because of this fact, many wireless devices in buildings operate in the 2.4 GHz band. While the risk of interference is minimized by various methods of signal generation, the potential for interference from these devices still exists considering the large number of devices emitting at similar frequencies. End-users expressed concerns that the devices will fail to report data at certain times because of the possibility of interference. Interference will likely result in the transmitted signal being dropped completely, but the possibility exists that a signal is transmitted with a corrupted data stream. Such a situation can usually be checked through application software, but the interference will still result in unusable data. A standard technique of measuring wireless system performance given a representative interference pattern could help users understand the implications of other devices on their wireless systems.

Latency

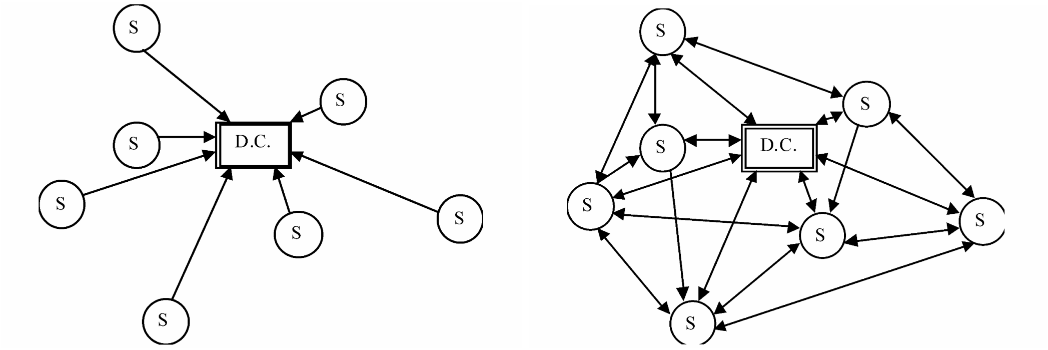
There is an expectation that data acquired from a wireless sensor should be made available to a receiver within a reasonable period of time. While wireless signals travel at the speed of light, certain system designs may add undue delay to the transmission of the signal and increase this latency. Multihop transmissions require multiple nodes to process a received signal and re-transmit that signal, adding to the total time needed for a data packet to make its way through the communications network. Efforts to increase battery life may also increase latency. For example, one technique for conserving battery life could involve transmitting sets of data collected at different times in a single message. This technique would have a significant impact on latency, as data sit in memory for a period of time before being transmitted to the central receiving station. For building automation systems, vendors and users expressed the general opinion that alarms from sensors should be transmitted to a central receiving station within approximately 10 seconds of the onset of the alarm condition. The wireless sensor network must be designed to achieve signal transmission from the most distant sensor node within the desired timeframe.

Fault Tolerance

When considering the performance of an entire sensor network, one expects that the failure of one sensor node or transmission path would not cause problems throughout the network. In this sense, a reliable network is one that can tolerate such faults while providing accurate data from the majority of sensor nodes.

Hardware, Software, and Network Design

To overcome these obstacles to reliability, designers can consider the design of the hardware, software, or network. For example, frequency hopping in the allowable frequency band could help eliminate interference problems. To increase reliability, many system designers are moving towards mesh networks in place of star networks. Figure 2 depicts the topologies of both types of networks. Star networks are comprised of a collection of sensor nodes that each communicate directly with a central receiving station. Each node must therefore be in communication range with the base station, and obstacles placed in the transmission path will eliminate the ability for that sensor's data to be captured. In mesh networks, each sensor node can communicate with neighboring nodes, and each node can relay messages from other nodes. Software is typically written so that the nodes in the network configure themselves in an ad-hoc manner to route messages from the sensor node through the network to the base station. This setup allows for routing of messages around obstacles and permits easy expansion of the sensor network even if the outermost nodes are out-of-range of the base station. The ad-hoc manner of these networks and the ability to change transmission paths makes these network designs more reliable. The drawbacks with mesh networks arise from their multihop nature. Battery life for each node can be shortened because of its increased transmission load, and latency can increase because a signal must be received, processed, and re-transmitted at each intermediate node.



(a) Star

(b) Mesh

Figure 2 (a) Star and (b) mesh network topologies.

Another challenging aspect of reliability arises in defining metrics to assess reliability. Some options for reliability metrics are provided below.

Signal-to-Noise Ratio

This common measure compares the strength of the received signal to the ambient noise received by the radio. It is a metric that yields the relative strength of the signal.

Received Signal Strength Indication (RSSI)

Received signal strength indication (RSSI) is a term used to describe the strength of a wireless signal. The value of RSSI often lacks units, and different vendors can arbitrarily set the range of the indication. For example, one manufacturer may set the range to be from 0 to 100, with 0 being no signal and 100 being the strongest signal while another may set the range as 1 to 60. Circuits to determine RSSI are often placed on radio hardware, providing the ability to automatically determine RSSI in a variety of devices with wireless receivers. The algorithm used to determine RSSI may vary on different devices, so it is a measure that is most useful in assessing the effect of environmental factors on a particular radio. The drawback that has been observed with the use of RSSI as an indicator of the reliability of the wireless link is that it does not always correlate with the rate of reception of wireless packets. RSSI simply measures the strength of the signal regardless of the surrounding noise. A low-strength signal in a noiseless environment gets a low RSSI despite the fact that it has a better chance of transmitting data successfully than a high-strength signal in a noisy environment (which would receive a high RSSI).

Link Quality Indication (LQI)

The Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard [12], the predominant standard for the physical aspects of low data-rate radio communications as used in the building industry, specifies the use of a link quality indication (LQI) to assess the quality of the communication link between a receiver and transmitter. This calculation is based on signal-to-noise ratio or energy density of the signal in the frequency band used by the standard and is typically computed over at least eight transmission cycles to estimate the link strength for a typical transmission. This value is also without units, and comparison of the numbers between different technologies is difficult. As with RSSI, this measure can be used to assess the environmental effects on a single transmitter/receiver pair. It provides a more thorough estimate of the quality of an IEEE 802.15.4 link than RSSI since it assesses all possible frequencies in the physical layer of the transmission. LQI is a valuable measure of reliability owing to the fact that much of the radio hardware used to implement wireless sensor networks automatically computes the value for the user.

Packet Error Rate

At its simplest level, a reliable system is one in which each packet of data transmitted by the sensor is received correctly by the receiver. One way to measure reliability in this manner is to keep track of the number of messages sent by the transmitter and monitor the number of messages successfully received at the base station. The reliability can then be expressed as the percentage of the total number of transmissions that are either dropped or received erroneously, or as a packet error rate.

Power Management

In discussions with vendors and users of wireless sensors, the expected lifetime of the sensors emerged as a common concern. Most often, these sensors are powered by batteries. If those batteries require frequent replacement, significant maintenance costs will be incurred. While there is no clear consensus on the acceptable time between battery replacements, a timeframe of five years appears to be a generally accepted ruleof-thumb. Many vendors claim that their sensor nodes are so efficient that no maintenance will be required for ten years, effectively limiting the lifetime of the sensor node by the shelf life of the battery itself. Typical energy content of batteries used for wireless nodes is listed in Table 2, but self-discharge can limit the amount of energy available for useful purposes.

Table 2 Typical energy capacity of batteries [13]

Cell Size	Energy content [mA•h]
AAA	700
AA	1500 to 2000

To achieve such long battery lives, wireless vendors carefully program the nodes to minimize energy consumption by going to "sleep-mode" when not taking data, transmitting very short packets of data, and minimizing the amount of data to be taken. Table 3 gives typical power consumption by a radio node for different operational modes. In general, wireless transmissions consume significantly more energy than data acquisition and processing, so any efforts to minimize radio communications will extend battery life. One example that demonstrates this approach is data processing at the sensor node with transmission of information only when alarm levels are reached. The specifics of the application, however, will have a large bearing on the time needed between battery replacements. The frequency of data acquisition and transmission, the power levels at which the radio transmitters are set, and the network design utilized will affect the lifetime of the system. While a mesh network promises to increase reliability, each node in that network serves as a repeater and, hence, must consume significantly more energy relaying messages than if it were only required to transmit its own data.

Table 3 Typical power consumption for a radio node [14]

Radio mode	Power consumption (mW)
Transmit	15
Receive	13
Idle	12
Sleep	0.016

One advantage when considering power management in buildings is the fact that there is often line power available where many sensors will be installed. Sensors can therefore transmit data wirelessly yet get their power from a wire. Likewise, line-powered repeaters can be installed in buildings to help extend the reach of a wireless network without resorting to multi-hop transmissions between a sensor node and the eventual destination of the data. In any building installation, however, there will be some places where line power is not available and the node will be forced to get energy from batteries or alternative means.

Regarding alternative means of powering sensors, significant work is underway to scavenge power from vibrations, light, or temperature gradients [15]. Such systems may provide the ability to eliminate chemical batteries from the sensor nodes, but some type of electrical storage will likely be needed to provide sufficient power to the sensors.

With both battery and energy scavenging options, there is a need for a clear metric on the energy consumption of these sensor nodes in different applications. Battery powered nodes will require an estimate of overall energy consumption over a period of time to gauge the time between battery changes. Nodes utilizing energy scavenging techniques will require power measurements to determine the amount of energy that must be collected to permit the data acquisition and radio transmissions that are needed.

Interoperability

The public's familiarity with IEEE 802.11 and Wi-Fi for wireless Internet and networking access in homes and offices has provided confidence in wireless technologies and can be credited with the relatively rapid adoption of wireless sensing technology in buildings. Much of the allure of Wi-Fi is the interoperability that has been enabled through standards. Users can install wireless networking cards from a range of vendors and have confidence that their systems will communicate reliably with other computers. The ZigBee Alliance hopes to bring that same level of interoperability to the wireless sensor and actuator community [16]. It has adopted the IEEE 802.15.4 standard for the physical layer of wireless communications and has added standards that will aid interoperability in the networking protocol. This interoperability will allow end users of the technology to use sensors appropriate for their particular application with the confidence that they can be easily integrated into the complete monitoring and control system. Users are hesitant to embrace a wireless sensor network system unless they can be sure that it can be easily modified using standard components. This interoperability applies to the physical radio interoperability as well as standard data models for exchange of data from sensors.

Ease of Use and Maintenance

Potential end users seek sensors that are easy to deploy and require minimal maintenance. Those who install the sensors or design systems using the sensors will rarely have expertise in the computer science, electrical engineering, and physics that are vital to the operation of wireless sensor networks. The sensors must, therefore, be easily integrated into existing networks, require minimal programming to achieve desired measurements, have intuitive user interfaces, and transmit data in a form that can be easily read by applications. Additionally, these sensors must be robust enough that they can be deployed for long periods of time with little maintenance efforts. As mentioned previously when discussing power options with sensors, any time needed for maintenance of the sensors in a network will increase the life cycle cost of the system.

Security

A recurring concern of users is security. With data being transmitted wirelessly, there is concern that hackers will be able to access building automation systems and use the wireless sensor network as a tunnel into other critical information infrastructure. The concerns are evidenced by situations in military facilities where the use of wireless is forbidden. Other facility managers report that their information technology (IT) security offices would raise great concerns if wireless were installed; they have chosen not to fight that battle.

4. Next Steps

To help assuage these concerns, clear metrics and test methods are needed to assess each of these issues. NIST is currently working to develop such test methods to help users obtain a clear picture of how a wireless sensor system will work in their applications with a minimal set of measurements. Currently, such simple measurements are not available to help users make decisions on the use of wireless systems. The resulting rating can provide guidance on the optimal locations and density of wireless sensor nodes that will result in a reliable system with low maintenance and initial costs. Each of the concerns may require its own set of tests or a method to easily assess how a sensor system would perform in a particular building. Regardless, clear measures of wireless sensor system performance in buildings will help promote their appropriate use by giving users more confidence before completely committing to their installation.

5. References

[1] Kintner-Meyer, M. and Brambley, M.R., “Pros & Cons of Wireless,” *ASHRAE Journal,* Vol. 44, No. 11, November 2002, pp. 54-61.

[2] Kintner-Meyer, M, Brambley, M.R., Carlon, T.A., Bauman, N.N. “Wireless Sensors: Technology and Cost-Savings for Commercial Buildings,” in *Teaming for Efficiency: Proceedings of the 2002 ACEEE Summer Study on Energy Efficiency in Buildings*, Vol. 7, 2002, pp. 7.121-7.134.

[3] Wills, J., “Will HVAC Control Go Wireless?,” *ASHRAE Journal*, Vol. 46, No. 7, July 2004, pp. 46-52.

[4] Healy, W.M., “Lessons Learned in Wireless Monitoring,” *ASHRAE Journal* Vol. 47, No. 10, October 2005, pp. 54-58.

[5] Raimo, Jeff “Wireless Mesh Controller Networks,” *ASHRAE Journal*, Vol. 48, No. 10, October 2006, pp. 34-38.

[6] Ruiz, John, “Going Wireless,” *ASHRAE Journal,* Vol. 49, No. 6, June 2007, pp. 33-43.

[7] Martocci, Jerald P., “BACnet Unplugged: ZigBee and BACnet Connect” *ASHRAE Journal*, Vol. 50, No. 6, June 2008, pp. 42-46.

[8] Swyt, Dennis A., “An Assessment of the United States Measurement System: Addressing Measurement Barriers to Accelerate Innovation,” NIST Special Publication 1048, February 2007.

[9] Brambley, M.R., Haves, P., McDonald, S.C., Torcellini, P., Hansen, D., Homberg, D., and Roth, K.W., “Advanced Sensors and Controls for Building Applications: Market Assessment and Potential R&D Pathways,” Pacific Northwest National Laboratory Report PNNL-15149, April 2005.

[10] OnWorld, “Wireless Sensor Networks: Growing Markets, Accelerating Demand,” OnWorld Report, July 25, 2005.

[11] J.P. Lynch, “An overview of wireless structural health monitoring for civil structures,” Phil. Trans. R. Soc. A 365 (2007), 345-372.

[12] IEEE 802.15.4 “Wireless MAC and PHY Specifications for Low Rate Wireless Personal Area Networks (WPANs)”, IEEE, 2006.

[13] Halpern, Mark and Saleem, Khusro, “Battery Power Issues for WSN’s,” *NICTA Formal Methods Workshop*, National ICT Australia, November 7-9 2005, Sydney, Australia.

[14] Zhao, Lei, Zhang, Wei-Hong, Xu, Chao-Nong, Xu, Yong-Jun and Li, Xiao-Wei, “Energy-Aware System Design for Wireless Sensor Network,” *Acta Automatica Sinica*, Elsevier, Vol. 32, No. 6, 2002, pp. 892-899.

[15] Roth, Kurt and Brodrick, James, “Energy Harvesting for Wireless Sensors,” *ASHRAE Journal*, Vol. 50, No. 5, May 2008, pp. 84-90.

[16] ZigBee Alliance, www.zigbee.org.