Assessment of Performance Metrics for Use of WSNs in Buildings

Won-Suk Jang[1] and William M. Healy[2]

[1]Building and Fire Research Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8632; PH: (301) 975-5855; FAX: (301) 975-5433; e-mail: wonsuk.jang@nist.gov
[2]Building and Fire Research Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8632; PH: (301) 975-4922; FAX: (301) 975-5433; e-mail: william.healy@nist.gov

Abstract

This paper is part of an effort to develop measurement systems and methods to better predict the performance of wireless sensor and control networks in building applications. Because of the variability in application requirements, the development of measurement methods to assess the performance of wireless sensor networks in buildings is extremely challenging. This paper presents the key challenges in using wireless technology in practical building applications through the results of a literature survey and interactions with building industry professionals. It is anticipated that the findings will provide potential users of wireless technology a clear metric as to how the technology will perform in a particular, and to understand the barriers to adoption of wireless sensors in buildings when appropriate.

Introduction

Wireless technology facilitates easy deployment of sensors throughout various applications in building automation, construction, and structural health monitoring. However, many engineers and operators who may consider using those sensor systems do not have a clear metric to describe how wireless systems will work in particular applications. These measurement needs are stated in an assessment of the United States' measurement system as "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 [Swyt, 2007]." Furthermore, a recent DOE roadmap entitled "Advanced Sensors and Controls for Building Applications" 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.[Brambley et al., 2005]" Owing to 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. As the first part of the effort, this paper presents 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.

Background

To identify these needs, a research team at the National Institute of Standards and Technology (NIST) surveyed the literature and interviewed people involved in building operations and wireless products. Interviews were performed of people who represent 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 1) the challenges or concerns that they see in using wireless sensors and controls in buildings, and 2) the types of measurements that they could envision that would give users more confidence in the performance of a wireless system.

This paper addresses these obstacles to the use of wireless technology in buildings by developing measurement methods and testbeds that will enable users to predict the performance of a wireless system for a building application. While each 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.

Practical Challenges

This section highlights the most important, practical issues that can address a useful metric for designs and applications of wireless sensor in a building.

1) Cost

A major advantage in using wireless sensors and controls over wired systems is the decreased installation and maintenance cost. In wired systems in a large building, cost issues become prominent when the number of wires and complexity of the network increases. The installation cost for wired systems was reported as $7.21 and $2.20 per linear meter of wiring in existing construction and new construction, respectively [Kintner-Meyer and Brambley, 2002]. In addition, it has been reported that the typical wiring process accounts for 75% of the installation cost of sensor networks in a structural health monitoring system [Lynch, 2007]. While the installation cost depends upon the type of construction, the size of the building, and the need for radio repeaters, promised declines in the prices of the radio hardware will make wireless more competitive.

The number of nodes and repeaters is the key factor in assessing the cost of a wireless system. 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, it is obvious that an installer of a wireless system must see how much this system will cost over 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.

2) Reliability

Reliability of the wireless system is one of the major concerns of potential users of wireless technology in buildings. At its most basic level, the same level of reliability with a wireless system is expected as is seen with wired systems, while its reliability requirement may either be more or less severe in a broader range of applications.

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

Accuracy

Measurement accuracy is not specific to wireless sensor networks but is a concern with all sensor devices. Traditionally, internal or external noise imposes inherent limitations on the accuracy of sensors and equipment. The 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. In addition, data corruption or distortion caused by environmental impact will typically result in values that are noticeably in error.

One positive characteristic of wireless sensor networks with respect to accuracy is node redundancy. High node density may compensate for overall uncertainty caused by the noise and non-ideal conditions, and can increase the overall accuracy of the measurement in a particular areas. For instance, a cluster-based topology can be employed to collect sensory data at the same local area. While this topology presents the problem of knowing which sensor's data are closest to being correct, it does present the possibility of obtaining data when certain sensors become defective or in using statistical methods to determine the best estimate of the true value of a parameter. Thus, densely distributed wireless networks could help increase the overall accuracy by allowing redundant measurements.

Signal Coverage through Building Materials

Different construction types and the resultant coverage of the wireless signal are significant factors for the reliability of a wireless link. In most cases, the maximum allowable distance between the transmitter and the receiver is specified when there are no obstructions between the two radios (e.g., in an open field). However, the actual prediction of signal propagation is much more complicated because walls, floors, ceilings, and furnishings are often present in the indoor environment. Different construction materials also attenuate the signal to varying degrees, and even tend to stop propagation of radio-frequency (RF) waves. Further complicating matters is the fact that different frequencies and transmission power levels may respond in different manners in different buildings. Without clear understanding on the allowable ranging distance in real applications, users may both 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 reached.

Interference

A low-power wireless device is potentially vulnerable to interference from other wireless technologies that have much higher power within the same industrial, scientific, and medical (ISM) band. Typically, many of the devices being constructed as part of wireless sensor networks operate in the 2.4 GHz band because of its worldwide usage. While the risk of interference is minimized by various techniques of signal communication, there still exists the potential for interference from other equipment considering the large number of devices emitting at similar frequencies. From interviews, end-users expressed concerns that the devices will not report healthy data at certain times because of the possibility of interference. A standard measurement technique of wireless system performance given a typical interference pattern could help users understand the effects of other devices on their wireless systems.

Latency

Acquiring data in real-time is considered an application-specific issue in wireless sensor network. Inherent features of WSNs, such as dynamic topology, lossy links, limited bandwidth, and channel variations, often limit the real-time performance. Different demands on end-to-end latency are required because most applications have different expectations that data acquired from a wireless sensor should be made available to a receiver within a reasonable period of time. While the end-to-end latency is most crucial for certain applications, e.g. emergency response, quality-of-service (QOS) is usually a higher priority for many applications. Thus, most solutions for the real-time issue involve trade-offs between power management and latency, and careful management of transmission control and topology should be provided.

Fault Tolerance

In randomly deployed wireless sensor nodes, the failure of individual components, such as a node, network, or sink, is unavoidable. In the design of sensor networks for building application, it is important to identify the failures that will affect the overall performance of the system and that will degrade the confidence level in the measurements. In building applications, a fault can be classified by three categories: 1) node faults, 2) network faults, and 3) sink faults. First, various sources of node faults can be identified under harsh environmental conditions. A variety of extreme conditions can cause antenna failures, circuit failures, and battery leakage, which will lead to poor performance of WSNs. Second, a network fault is another common fault in a WSN since the high density of deployed nodes will increase the chance of individual communication failures. Third, sinks, the points where data are collected, are subject to faults. Typically, the power supply and network infrastructure are the main components for sink faults that will cause the malfunction of the entire sensor network.

There are a number of metrics that one can use to assess or predict reliability:

Received Signal Strength Indication (RSSI)

Received Signal Strength Indication (RSSI) is a term used to describe a measurement of the power present in a received radio signal. RSSI is calculated at the radio chip on the receiver and provides useful implication of network link quality. The drawback of RSSI as an indicator of the reliability of wireless link is that it does not always correlate with the success rate of packets reception. RSSI simply measures the received power strength regardless of the surrounding noise. For instance, a low-strength signal in total absence of noise may have a better chance to get a higher link quality than a high-strength signal in a noisy environment.

Link Quality Indication (LQI)

The use of a Link Quality Indication (LQI) is specified by IEEE802.15.4 to assess the quality of the communication link between a receiver and transmitter [IEEE802.15.4-2006, 2006]. LQI is based on signal-to-noise ratio or energy density of the signal in the frequency band used by the standard and provides average correlation values for each incoming packet over at least 8 symbol periods. As with RSSI, LQI allows users to assess the communication link considering the environmental effects on a single transmitter/receiver pair. However, LQI 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.

Packet Error Rate

Packet error rate (PER) is defined as the ratio of the number of packets unsuccessfully received to the total number of packets transmitted over certain period of time. In a reliable system, it is simply expected that each data packet transmitted 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 compare the number of messages successfully received at the base station. The reliability can then be expressed as the percentage of dropped packets of data over the total number of transmissions, or as a packet error rate.

3) Power Management

In wireless sensor networks, the energy source is generally limited, often being comprised of small batteries. This limitation becomes critical when hundreds or thousands of nodes are placed in a network for long-term monitoring applications. In this circumstance, it is practically impossible to change or recharge the batteries in such a large number of nodes. From discussions with vendors and users of wireless sensors, the expected lifetime of the sensors emerged as a common concern. While there is no clear consensus on the acceptable time between battery replacement, a timeframe of 5 years appears to be a generally accepted rule-of-thumb. Many vendors claim that their sensor nodes are so efficient that no maintenance will be required for 10 years, effectively limiting the lifetime of the sensor node by the shelf life of the battery itself. Typical energy content of batteries is listed in Table 1, but self-discharge can limit the amount of energy available for useful purposes.

Table 1. Typical energy capacity of batteries [Halpern and Saleem, 2005]

Cell Size	Energy content [mA•h]
AAA	700
AA	1500-2000
C	5000
D	9000-12000
9V	550

To achieve long battery lives, minimal energy should be consumed by going to “sleep-mode” when not taking data, transmitting data packets for very short periods, and minimizing the amount of transmitted data. Different operation modes by a radio node are available for the management of typical power consumption, shown in Table 2. In general, signal transmission is a larger source of energy consumption than data acquisition and processing, so any efforts to minimize radio transmission will help prolong battery life. The specifics of the application, however, will have a large bearing on the time needed between battery replacements. In this sense, the lifetime of the system will be affected by the frequency of data acquisition and transmission, the power levels at which the radio transmitters are set, and the network design utilized. While a mesh network offers a potential to increase communication reliability, each node in that network serves as a repeater that must consume significantly more energy relaying messages than if it were only required to send its own data.

One advantage of sensor use in buildings is that line power is often available, and therefore, sensors can transmit data wirelessly yet get their power from a wire. Likewise, line-powered repeaters can help extend the accessibility of a wireless network without the need for multi-hop transmissions between a sensor node and a base station node. Regarding alternative means of powering sensors, significant work is underway to scavenge power from vibrations, light, or temperature gradients [Roth and Brodrick, 2008]. Such systems may eliminate chemical batteries from the sensor nodes, but some type of electrical storage will likely be needed to provide sufficient power to the sensors.

Table 2. Typical power consumption for a radio node [Zhao et al., 2002]

Radio mode	Power consumption (mW)
Transmit	15
Receive	12.5
Idle	12.4
Sleep	0.016

With power management in sensor networks, 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 for various activities performed by sensor nodes. Energy scavenging techniques will also require thorough studies on energy conversion mechanisms to determine the amount of energy that must be collected to permit the data acquisition and radio transmissions that are needed.

4) Interoperability

Familiarity with IEEE 802.11 and WiFi for wireless networking access in homes and offices has provided confidence for the relatively rapid adoption of wireless sensing technology in buildings. Interoperability has made WiFi attractive. Users can install wireless networking cards from a range of vendors with great confidence that reliable communication with other computers can be set up. One goal of the ZigBee alliance is to bring that same level of interoperability to the wireless sensor network community [ZigBee Alliance, 2008]. By adopting the IEEE 802.15.4 standard for the physical layer of wireless communications, ZigBee has added standards that will increase interoperability in both the networking protocol and data exchange. Thus, end users can use sensors appropriate for their particular application, and can easily integrate them with confidence into monitoring and control systems. Unless users can be sure that a wireless sensor network system can be easily modified and customized using standard components, they may be hesitant to embrace the technology in their applications.

5) Ease of Use and Maintenance

Easy deployment and minimal maintenance are also key factors that potential end users seek. Most civil and building engineers who use the wireless sensors will have little expertise in the electrical engineering and radio physics that are critical to the operation of wireless sensor networks. The wireless sensor platforms must, therefore, provide easy integration into existing networks, require minimal programming effort, possess intuitive user interfaces, and relay data in a standard format that can be easily read by applications. Additionally, these sensors must be robust enough for long-term deployment with little maintenance.

6) Security

With wireless data transmission, there is recurring concern that hackers will tweak the measured data or access building automation systems to use the wireless sensor network as a tunnel into other critical information infrastructure. Evidence of this concern is found in military facilities where the use of wireless is forbidden. Other facility managers claim that their IT security offices would raise great concerns if wireless infrastructure were installed; they have chosen not to fight that battle.

Conclusions

This paper presented key areas of concern that inhibit the use of wireless sensors in a building: 1) cost, 2) reliability, 3) power management, 4) interoperability, 5) easy of use and maintenance, and 6) security. It is proposed that measurement methods be developed to help give users a clear gauge of a system's performance in these areas. Each of the concerns may require its own set of test methods to easily assess the performance of wireless sensor networks in a particular building. A research team at 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. The results from the development of test methods will provide useful guidance on the effective utilization of wireless sensor networks in a wide variety of use-cases.

References

[1] Swyt, D.A. (2007). "An Assessment of the United States Measurement System: Addressing Measurement Barriers to Accelerate Innovation," NIST Special Publication 1048, National Institute of Standards and Technology, Gaithersburg, MD.

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

[3] Kintner-Meyer, M. and Brambley, M. (2002). "Pros & Cons of Wireless," ASHRAE Journal, 44(11), 54-61.

[4] Lynch, J.P. (2007). "An Overview of Wireless Structural Health Monitoring for Civil Structures," Philosophical Transactions Series A: Mathematical, Physical, and Engineering Sciences, 365(1851), 345-372.

[5] IEEE 802.15.4-2006 (2006). "Wireless MAC and PHY Specifications for Low Rate Wireless Personal Area Networks (WPANs)", IEEE Computer Society, New York, NY.

[6] Halpern, M. and Saleem, K. (2005). "Battery Power Issues for WSN's," Proceedings of NICTA Formal Methods Workshop, National ICT Australia, November 7-9, Sydney, Australia.

[7] Zhao, L., Zhang, W.-H., Xu, C.-N., Xu, Y.-J. and Li, X.-W. (2002). "Energy-Aware System Design for Wireless Sensor Network," Acta Automatica Sinica, Elsevier, 32(6), 892-899.

[8] Roth, K. and Brodrick, J. (2008). "Energy Harvesting for Wireless Sensors," ASHRAE Journal, 50(5), 84-90.

[9] ZigBee Alliance (2008). <http://www.zigbee.org> (November 19, 2008).