Wireless industrial sensor networks: Framework for QoS assessment and QoS management

Ivan Howitt,[a] Wayne W. Manges,[b] Phani Teja Kuruganti,[b] Glenn Allgood,[c] José A. Gutierrez,[d] James M. Conrad[a]

[a]*ECE Department, University of North Carolina at Charlotte, Charlotte, North Carolina 28223, USA*
[b]*Extreme Measurement Communications Center, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831, USA*
[c]*Computational Science and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831, USA*
[d]*Embedded Systems and Communications-Eaton Corporation, Milwaukee, Wisconsin 53216, USA*

(Received 10 May 2005; accepted 11 December 2005)

Abstract

This paper presents a framework that addresses Quality of Service (QoS) for industrial wireless sensor networks as a real-time measurable set of parameters within the context of feedback control, thereby facilitating QoS management. This framework is based on examining the interaction between the industrial control processes and the wireless network. Control theory is used to evaluate the impact of the control/communication interaction, providing a methodology for defining, measuring, and quantifying QoS requirements. An example is presented illustrating the wireless industrial sensor network (WISN) QoS management framework for providing dynamic QoS control within WISN. The example focuses on WISN operating in a time-varying RF interference environment in order to manage application-driven QoS latency constraints. © 2006 ISA—The Instrumentation, Systems, and Automation Society.

Keywords: Quality of service; Wireless; Industrial networks; Interference

1. Introduction

Global competition and dwindling natural resources are spurring industries' search for technology innovations to improve process efficiencies that can enhance quality and increase productivity. Innovations are sought to achieve higher levels of availability, reliability, and maintainability for production equipment and production processes. In addition, to facilitate these goals, plant supervisors and production managers require timely situation awareness and understanding concerning aggregate production measures down to variations in individual machine performance.

The recent technology boom in ad hoc wireless networking is opening new opportunities for the vision of self-configuring, self-healing, and robust industrial wireless networks. This new vision extends wireless technology's utility well beyond its frequent deployment as a point-to-point link within the industrial environment. The challenge in achieving this new vision is maintaining Quality of Service (QoS) requirements. Assessment and management of QoS needs to occur, allowing the network to adapt to changes in the RF, information, and operational environments. The capacity to adapt is paramount to maintaining the required operational performance. Proprietary solutions that attempt to address this issue often require elaborate installation planning and rigorous maintenance schedules. This expenditure of effort hinders the scalability that wireless communications provide.

Wireless communications is poised to support

0019-0578/2006/$ - see front matter © 2006 ISA—The Instrumentation, Systems, and Automation Society.

technical innovations in the industrial community, with widespread use of wireless sensors forecasted to improve manufacturing production and energy efficiency by 10% to 18% and reduce emissions by 25% [1]. With this incentive, the Department of Energy's (DOE) Industrial Technologies Program sponsored a workshop [1] to provide a forum for technology end users and suppliers to help the industries accelerate the adoption of wireless systems for process measurement and control, i.e., wireless industrial sensor networks (WISN). This meeting was also the kick-off meeting for the Wireless Industrial Networking Alliance (WINA) [2].

The use of wireless technology within the industry has been actively explored over the past ten years [3,4]. The challenge continues to be the fact that success occurs at the intersection of the four engineering and information technology disciplines defined in the name: Wireless, Industrial, Sensor, and Networks. Solutions require the combination of expertise from each of these areas:

- Industrial expertise providing application domain knowledge,
- Sensor expertise required to understand issues associated with calibration, drift, digitization, sampling, and transducer phenomena,
- Wireless device and radio frequency (RF) environment expertise addressing issues of technology suitability, electromagnetic compatibility, and electromagnetic interference (EMI) issues associated with industrial environments,
- Network expertise addressing the need for complex hierarchical network architectures involving thousands to tens of thousands of wireless sensor nodes, which support a multiplicity of industrial applications.

In line with the WINA charter, as illustrated in Table 1, the WINA technical committee has undertaken the development of a quality of service (QoS) design and assessment framework for WISN. The goal of this activity is to assist the wireless communication supplier and the end user community with achieving a successful solution. This paper details the WISN QoS framework. In Section 2, an overview of the framework is presented. In Section 3, the characteristics of an industrial RF environment are reviewed and in Section 4, a method for characterizing the QoS requirements in the context of industrial applications is presented. In Section 5, monitoring and maintaining QoS within the WISN is addressed, and conclusions are presented in Section 6.

Table 1
WINA charter [2].

Wireless technology and wireless networking systems hold great promise to help U.S. industry use energy and materials more efficiently, lower systems and infrastructure costs, lower production costs, and increase productivity. Although major advances in both price and performance have occurred in wireless networking, its acceptance in the industrial sectors has been slow. WINA focuses on four activities to accelerate the adoption of wireless technology in the industrial sector.

Activity 1:	Identify, characterize, recommend, and certify appropriate wireless technologies
Activity 2:	Promote effective standards, regulations, and practices
Activity 3:	Focus on customer requirements
Activity 4:	Quantify and communicate the benefits and potential impacts of wireless technologies.

2. Overview

The formulation of a WISN solution for a specific industrial application will need to address the wireless communication design in the context of the application as well as in the context of the application's environment, e.g., RF industrial environment. To address these challenges, a design framework for developing WISN is proposed as illustrated in Fig. 1. A measure of effectiveness (MOEs), in this case QoS, provides a means for evaluating the overall effectiveness (i.e., trade-off analysis) of a proposed wireless communication design. Correspondingly, measures of performances (MOPs)—throughput, latency, reliability, security, adaptability, and affordability—represent the aggregate properties that define QoS. The MOPs/MOEs are based on mapping functional needs onto operational requirements and defining measurable and quantifiable parameters. A construct for assessing QoS in terms of the notional relationship between controls and communications is presented in Section 4. A brief overview of issues associated with industrial RF environment is presented in Section 3. Details concerning QoS and its associated MOPs are as follows:

Throughput: Addresses the ability of the network to carry the offered traffic by the industrial

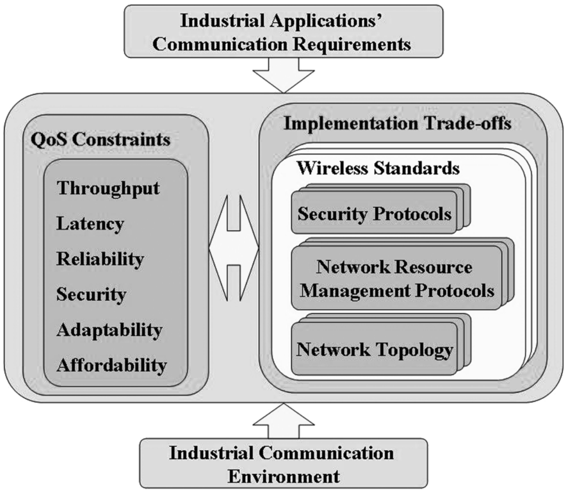

Industrial Applications' Communication Requirements
QoS Constraints
Throughput
Latency
Reliability
Security
Adaptability
Affordability
Implementation Trade-offs
Wireless Standards
Security Protocols
Network Resource Management Protocols
Network Topology
Industrial Communication Environment

Fig. 1. Design framework for developing WISN for industrial and manufacturing applications.

applications based on the WISN implementation and as impacted by the communication environment.

Latency: Addresses the timing considerations for the application information to be carried by the WISN implementation including the characterization of the time delay as well as the variation in the time delay, i.e., jitter. Latency requirements for certain communication traffic, such as a machine's servo control sensors, will have very strict requirements while a WISN to support supply chain management might have a more relaxed latency requirement. Factors influencing latency include sensor node density, interrogation rates, network topology, and number of simultaneous actions.

Reliability: Addresses the ability of the network to carry out its functional requirement of carrying industrial application information over the network over a broad range of operational conditions. Issues include the ability of the network to address communication disruptions, unanticipated variations in traffic, and variations in the operational environment using a predictable "fail-soft" mechanism. In addition, WISN are often energy constrained and therefore reliability includes the ability of the network to maintain operational integrity under energy constraints such as dirty power, battery operation, or energy scavenging.

Security: Addresses the operational impact and cost associated with the failure to prevent three typical categories of attacks on the communication network: (1) unauthorized interception of confidential information, (2) modification of information and network control messages, and (3) interruption of information and network control messages [5]. WISN deployed in an industrial environment can be subjected to both physical and logical security attacks. A deep concern to industrial companies is maintaining confidentiality of trade practices. Utilizing wireless technology can appear to be a potential compromise of this requirement, especially if the information carried on the wireless devices can be used to divulge information pertaining to an industrial process. Therefore, the industrial network's capability to prevent and detect unauthorized interception needs to be evaluated. In addition, industrial networks could be subject to malicious attacks that would compromise integrity of information, as well as the availability of sensor network functions. The capability to handle malicious attacks involving modification and interruption of data and network control messages needs to be addressed in designing the industrial network. The assessment process needs to balance the tradeoff between the security requirements of the industrial communication network with the communication administration overhead associated with security protocols, i.e., security implementation cost needs to be balanced against the other QoS cost performance constraints.

Adaptability: Central to WISN is its ability to adapt to new configurations and new tasks. Adaptations required by the industrial application include mobility in all or some of the sensor elements as well as scaling and/or reconfiguring the WISN to handle a new process or modification to an existing process as a result of a new task or goal. The WISN will also need to adapt to handle variations in the industrial environment over the time frame of seconds to years, e.g., RF propagation effects due to dynamic changes in stock supplies or retooling a plant's manufacturing line. Adaptability also includes the wireless network's capability of handling variations in the traffic flow due to changes in sensor location and machine or process utilization. The network will need to adapt to changes in the environment while maintaining the required levels of throughput, latency, reliability, and security. In addition, if the WISN are too complex to adapt and reconfigure to changing needs and a changing environment, then an inherent advantage to the WISN approach is compromised. To fully enable WISN, the adaptation of the wireless network should be transparent to the end user.

Within the industrial environment, adaptability is one true advantage of wireless over wired networks. Directly interconnecting all neighboring nodes with wiring is too complex and cost-prohibitive. WISN, however, provide low cost and redundant connectivity that can be exploited in the network layer to optimize routing for current conditions.

Affordability: Once functionality, operability, and utility are addressed, there will be a need to assess affordability. Affordability in this context includes cost of ownership (packaging requirements, modifications, maintainability, etc.), implementation costs, replacement and logistics costs, and training and servicing costs as well as the per-unit costs.

3. Wireless industrial environment

Advances in wireless communications over the past several decades can be attributed, in part, to incorporating the evolving comprehension of the RF channel characteristics into the communication system design. By understanding the RF environment within the industrial environment, the network design process and the ability to assess the design can be enhanced. In order to characterize the industrial network's RF environment, the radio signal propagation and RF interference sources need to be understood. In the industrial network, the interference sources are comprised of environmental noise sources such as certain machines or industrial processes as well as unintentional interference from other collocated wireless devices. In addition, intentionally interference sources may be introduced to create network vulnerability.

3.1. RF signal propagation

Extensive work is reported in the literature on characterizing the radio propagation in indoor environments including industrial sites [6,7]. Understanding the RF signal propagation is essential for designing the WISN to achieve and maintain the QoS constraints.

The reliability of the communication link between a transmitter (Tx) and receiver (Rx) is dependent on the environment as well as the wireless devices used. As an example, the IEEE 802.11b WLAN specifies a frame error rate of less than 8% for a received signal of −80 dBm (decibels referenced to a milliwatt). The reliability of a link will directly impact the latency and throughput QoS constraints. The RF signal propagation characteristics will also impact security and adaptability QoS constraints. As an example, from a security point of view, understanding the RF signal propagation provides insight into the locations at which WISN communication system can be compromised by either intercepted data or malicious attacks.

Due to underlying electromagnetic propagation mechanisms, RF signal propagation has a natural dichotomy for characterizing its behavior: large-scale propagation and multipath fading. Based on an extensive measurement campaign made in five factories conducted by Rappaport [7], large-scale propagation for WISN is well modeled by a log-normal shadowing model,

$$P_R(d) = \mathrm{EIRP} + G_R + 10n\log_{10}\left(\frac{\lambda}{4\pi d}\right) + X_\sigma\ (\mathrm{dBm}), \tag{1}$$

where $P_R(d)$ is the received power in dBm at a distance of d from the transmitter, EIRP is the transmitter's effective isotropic radiated power in dBm, G_R is the receiver's antenna gain (dB) in the direction of the signal propagation, n is the path loss exponent, λ is the wavelength of the carrier, and X_σ is a zero mean normal distributed random variable (RV) with standard deviation σ. Since X_σ is zero mean, the sum of the first three terms in Eq. (1) represents the expected value of $P_R(d)$ and the received power is inversely proportional to the log of the distance where n is the proportionality constant. The RV X_σ models the variations in the received signal strength due to the variations in the obstructions between the transmitter and receiver, i.e., walls, inventory storage racks, and machinery. In [7], based on a least-square error fit to the entire ensemble of data collected from the factories, $n=2.2$ and $\sigma=7.9$ dB. For individual measurement campaigns, typical values of n ranged from 1.8 to 2.8 and σ ranged from 4 to 10 dB. Fig. 2 illustrates the received signal power as a function of distance based on $n=2.2$ and $\sigma=7.9$ dB, and using typical values for IEEE 802.11b operating at 2.4 GHz (EIRP=20 dBm, G_R=0 dB). In the figure, the shaded region represents plus and minus one sigma about the mean. Since X_σ is normal

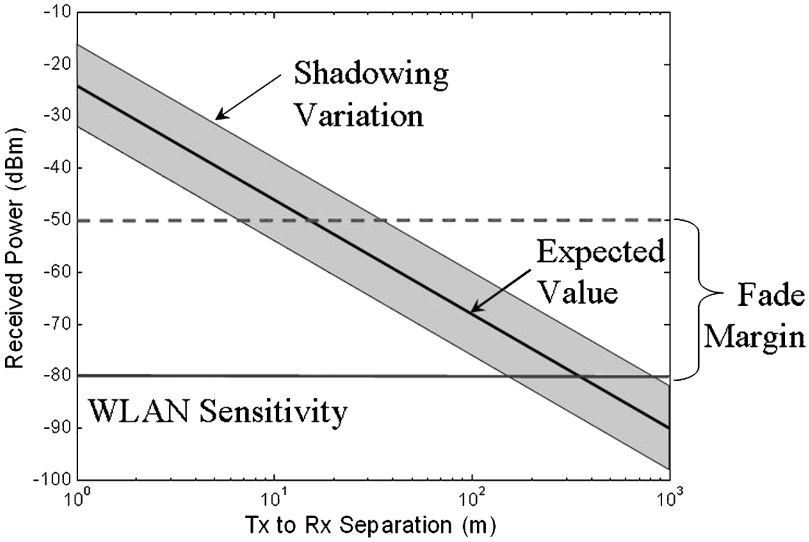


Fig. 2. Received signal power vs distance based on typical values for WLAN operating in a typical industrial environment.

distribution in dB, the likelihood of the received signal occurring within the shaded region for a given distance is 68%.

Multipath fading is another important consideration when characterizing the industrial environment's RF signal propagation. Multipath fading is caused by multiple reflections of the transmitted signal arriving at the receiver. These reflections represent different wave fronts that have traveled through different paths and therefore are time delayed and phase shifted versions of the original transmission. The received signal is the vector sum of these signals. Different methods can be employed to counter the effects of multipath fading. One of the most straightforward methods is to use a received signal fade margin when determining the coverage range for a transmitted signal. The required fade margin can be on the order of 30 dB in an obstructed environment. This would imply using −50 dBm as the receiver sensitivity for the WLAN. The impact of the industrial environment on the reliable coverage range is substantial, as illustrated in Fig. 2.

3.2. RF interference

RF interference occurs when the detection of the desired signal is corrupted by another signal at the intended receiver [8]. Based on current unlicensed (UL) band wireless protocols, data are transmitted based on packet transmissions. A corrupted packet is detected at the receiver and a retransmission is often initiated. The impact of a corrupted signal will be dependent on the data stream affected and the underlying application. In order for the desired signal to be corrupted, the interference signal must occur at the same time, frequency, and with sufficient power. There are two potential unintentional interference sources within the WISN: (1) wireless communication networks operating in the same frequency band whose operations are uncoordinated, (2) industrial equipment which produces RF harmonics within the communications network's frequency band.

Since the wireless technologies being considered for the WISN operate in the UL bands, the potential for interference exists between various wireless networks operating adjacent to each other or between the various hierarchical communication layers that are implemented using different wireless technologies. Methods for evaluating and designing networks that decrease the likelihood of interference between UL band wireless technologies are presented in [8].

Certain machine tools are potential sources of interference unique to the industrial environment. These interference sources include arc welders, power electronics, and induction motors. Anecdotal evidence indicates these sources of interference may be of concern, even though limited empirical data from the literature would suggest otherwise. In [7], interference from industrial noise sources is indicated to be insignificant for

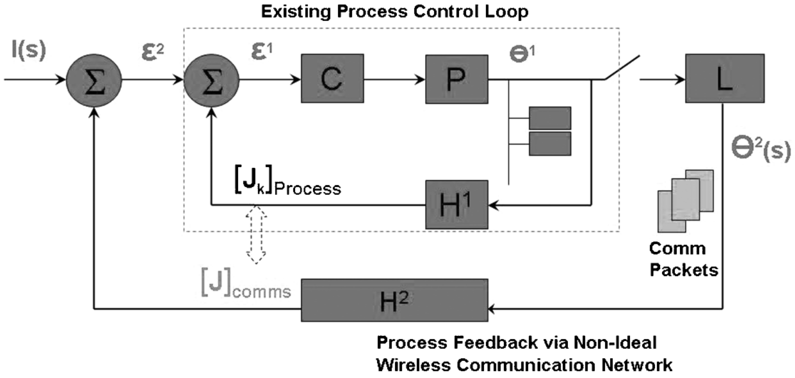

Existing Process Control Loop
I(s)
Σ
ε2
Σ
ε1
C
P
Θ1
L
Θ2(s)
[Jk]Process
H1
Comm Packets
[J]comms
H2
Process Feedback via Non-Ideal Wireless Communication Network

Fig. 3. A typical block diagram illustrating interrelationship between process control and wireless communication network in a feedback loop.

communication systems operating above 1 or 1.6 GHz when measurements were made at distances in excess of four meters from the noise sources. In order to ensure the reliability of the network operation, more details are required on the characteristics of these interference sources and their impact on QoS. This is especially true for WISN, where wireless devices may operate within a meter or less of interference sources.

RF interference can also be from intentional interference sources, which can take on different levels of sophistication, from denial of service attacks to intentional spoofing. A general discussion concerning intentional interference and cyber attacks goes beyond the scope of this paper.

4. Assessing QoS requirements: Interaction between controls and communications

Determining the QoS constraints for the WISN can be a daunting task. The application domain experts often do not understand the terminology and concerns of the wireless communications & networking experts and vice versa. In addition, the degree of reliability required by the communication network based on the industrial application is often not well understood or characterized. Both of these issues can be addressed by evaluating the WISN QoS requirements within the context of an industrial controls problem and examining the interaction principles between the two. The approach can be applied to a wide array of industrial applications and is directly applicable to industrial control processes in which the WISN is used to support sensing and/or actuator components within the processes. It is also applicable for WISNs used to support supply chain management that can also be viewed as a control process.

4.1. Interrelationship between process control & communications

The performance of communication links can have a major impact on process control systems. The relationship between the control and communications is illustrated in Fig. 3. The dotted line encompasses a notional model of a process control loop. The outer loop denotes the role of a communication network in ordering system stability. The loops contain the typical elements of a feedback control system where L is the target load, P & C denote the process and respective control, and H^1 is the feedback transfer function. In this notional construct H^2 represents the transfer function of the wireless communication network used for process and information feedback. The purpose of the control system is to effectively manage and control the system variables (i.e., line frequency) in the presence of a highly variable and nondeterministic load. To achieve this, the response behavior of each system block should be accurately known or predictable. The existence of the wireless communication network introduces new terms in the stability equation. The behavior of the communication network and its impact on a stable system's operation needs to be understood and quantified to generate the bounded limits for the system's stable state operation.

The transfer function of the inner control loop, i.e., the existing process control loop, can be derived as

$$\frac{\theta^1(s)}{\varepsilon^2(s)} = \frac{C(s)P(s)}{1 + H^1(s)C(s)P(s)}, \tag{2}$$

where $\theta^1(s)$ and $\varepsilon^2(s)$ are the output and input of the process control loop, respectively. The transfer function of the entire system is

$$\frac{\theta^2(s)}{I(s)} = \frac{L(s)C(s)P(s)}{1 + H^1(s)C(s)P(s) + H^2(s)L(s)C(s)P(s)}. \tag{3}$$

The communications network introduces a new term in the stability equation: H^2LCP. This term represents the cross-coupling between the process control inner loop and the communication network and indicates the complexity of the interdependence between the process control and communication.

Clearly the communications infrastructure must support the real-time transactions occurring at all levels in the control architecture. The consequences of communication problems like unpredictable latencies, excessive drops in throughput at critical times, and link flooding due to intentional and unintentional intervention from "outsiders" coupled with load uncertainties will affect the overall system stability and must be evaluated against the "ideal" performance. The scale and the criticality of the network demands for *a priori* error estimates between the intrinsic or quoted QoS and the actual perceived QoS need to be studied and understood. Since the communication infrastructure overlaid is a measurement and control network, end-to-end performance guarantees to directly affect the control system stability.

4.2. Example problem: Variability in wireless network latency

A first-order feedback control system is used to demonstrate the effect of latency in the feedback loop. Fig. 4(a) shows the transfer function of the feedback control loop described in Fig. 3. The outer loop (WISN) is the wireless industrial communication network. A transport delay of 0.01 s is introduced in the inner feedback loop. The variable parameter is the communication latency in the outer loop. Figs. 4(b)–4(d) show the output behavior for zero latency, fixed latency, and randomly variable latency, respectively. This shows the effect on system stability as the communication network model progresses from being predictable to highly variable.

5. Wireless industrial network QoS: A controls paradigm

5.1. Overview

As presented in the previous sections, if an industrial site incorporates a wireless network for industrial processing, the application requirements will define the network's QoS constraints. QoS has often been perceived as a quoted parameter of a particular network, but not as a real-time measurable or quantifiable parameter. Work has been conducted on defining the QoS for individual architectural layers, but less attention has been spent on a framework for ensuring that the application's required QoS constraints are being satisfied. If the network is responsive, intelligent enough to understand the QoS requirements of the application, and able to adaptively adjust accordingly, then the user can be assured a certain QoS performance level is maintained within the bounds of operational performance requirements. This can be done by developing methodologies to measure and quantify the parameters affecting the QoS and provide them as feedback to the application using the network. This is vital in developing next-generation networks for industrial control and monitoring applications.

The approach presented is similar in scope to the approach presented by Li and Nahrstedt for application-aware QoS adaptation [9]. Fig. 5 presents a block diagram representing a general framework for assessing and dynamically managing, i.e., controlling, the WISN in order to drive the observable QoS performance to the application defined target QoS. The figure illustrates both the major functional components and the information flow to accomplish the QoS management framework. The major functional blocks described are:

- WISN with QoS Self Test,
- RF Environment Sensing Network, and
- WISN QoS Management.

WISN with QoS Self-Test: The WISN are implemented to perform a set of applications which may change over time and which have defined QoS constraints. The WISN are comprised of hardware/software that enables specific capa-

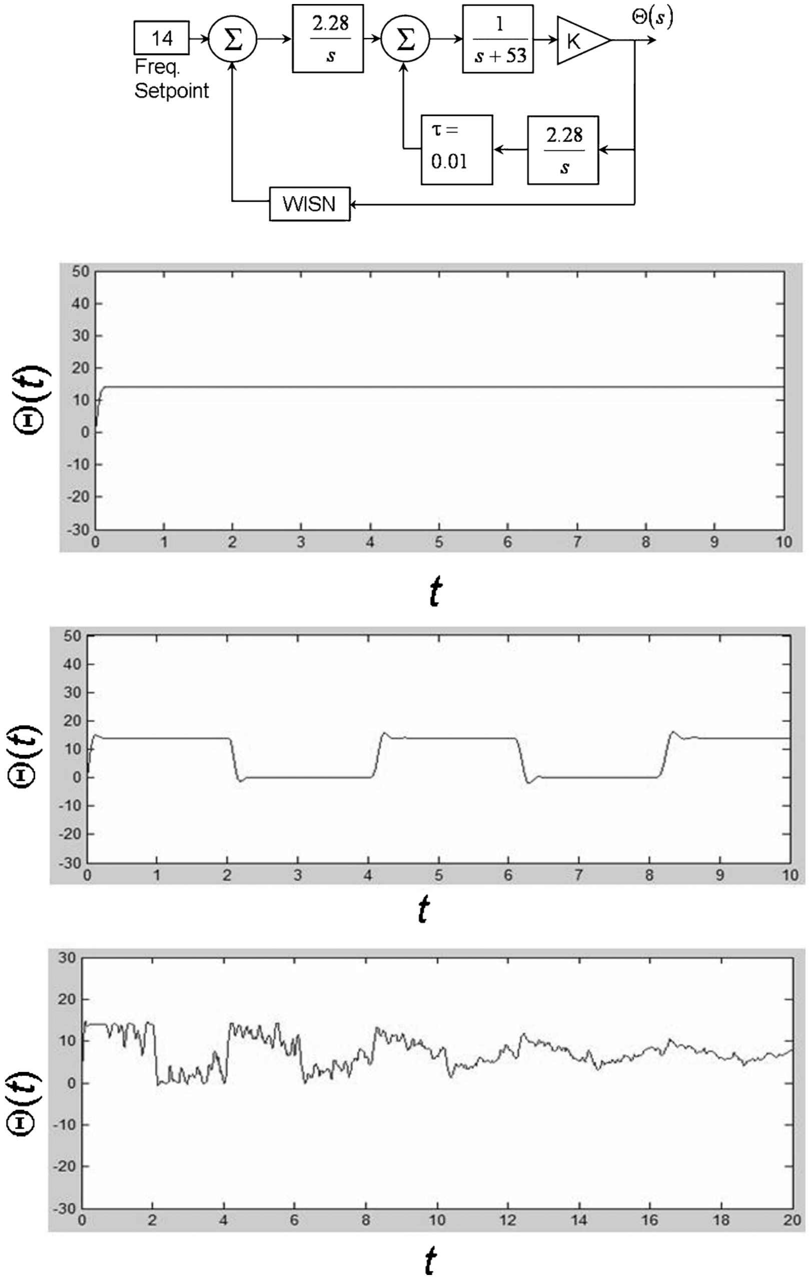


Fig. 4. Example illustrating the effect of variability in wireless communication network latency on the overall process control: (a) Block diagram of control process with wireless sensor network in feedback loop; (b) WISN is modeled as ideal, no latency; (c) WISN is modeled with fixed latency; (d) WISN is modeled with variable latency where variability is based on a uniform distribution.

bilities, i.e., operational frequency bands, frequency agility, power control, routing algorithms (for multihop networks), and scheduling algorithms. In addition, the WISN operate within a dynamic RF environment comprising time varying co-channel interference sources and time varying RF propagation characteristic such as multipath. Even if the WISN nodes are at fixed locations, dynamics in the environment will significantly impact the RF propagation characteristics. By incorporating a QoS self-test within the WISN, the WISN management functional block can readily test the observable QoS parameters and assess the networks performance. Depending on the outcome

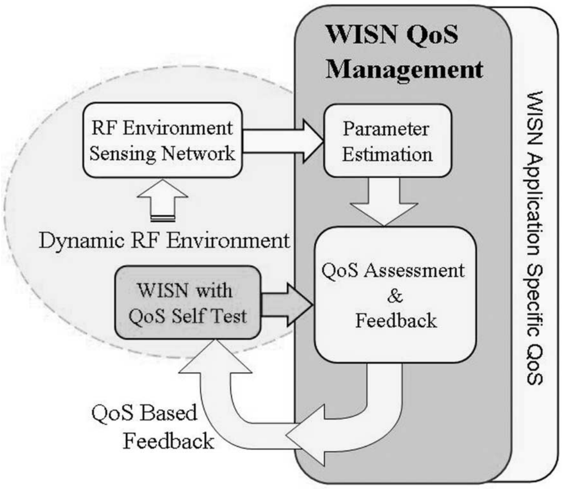


Fig. 5. Block diagram illustrating process for managing WISN QoS based on feedback control process.

of the assessment, the network's operational characteristic could be modified to achieve the target QoS constraints.

RF Environment Sensing Network: The purpose of this functional block is to provide spectrum usage patterns within the operational environment of the WISN. Mangold *et al.* discuss the concept of radio resource measurement for opportunistic spectrum utilization in the context of a homogenous IEEE 802.11 scenario [10]. Their paper was motivated, in part, by standards activities in the IEEE 802.11k task group. The IEEE 802.11k task group is developing a radio resource measurements extension to the IEEE 802.11 WLAN standard. The RF environment-sensing network, as proposed in Fig. 5, will be used to enhance site-specific propagation estimates within the operational environment and capture time varying patterns in the propagation characteristics. The RF environment characteristics can then be used by the WISN QoS Management block to predict the WISN performance and adapt the operational characteristics of the WISN to meet the application specific QoS set point.

It is important to note that the RF environment-sensing does not include measuring instantaneous small-scale multipath characteristics which are too time-sensitive for remote measurement. Instead, measurements would be targeted at capturing large-scale changes or patterns in the shadowing characteristics such as building structural changes, population density, and variations in inventory. Therefore, the RF Environment Sensing Network needs to measure the factors that influence the QoS management. These factors are in general time-variant, as introduced in [11]. The network coherence time T_{Ncoh} represents a statistical measure capturing the time interval over which the communication links within the WISN can be approximated as time-invariant. The concept of network coherence time is analogous to channel coherence time used as a statistical measure of the channel's stationarity when impacted by Doppler shift. The sampling rate of the sensing network will need to be proportional to T_{Ncoh} in order to ensure reliable parameter estimations based on the RF environment sensing data.

As depicted in Fig. 5, the RF environment-sensing network is separate from the WISN and is not an integrated part of the WISN, as it could be, as suggested by the IEEE 802.11k task group. The motivation for using an external sensing network is twofold: energy conservation and multiple usages. Measuring changes in the environment and passing this information to the WISN QoS Management block will need to be done on a regular basis, i.e., proportional to T_{Ncoh}. Based on the WISN application, the WISN node's on-off duty cycle may not allow them to accurately measure the dynamics of the operational environment. Requiring the nodes to turn on solely to measure the environment could be counterproductive in preserving the sensor node's energy. Also, it is conceivable that in future industrial, commercial, and public areas, an RF environment sensing network will be needed to service multiple requirements. These requirements might include RF measurements for multiple WISN, WLANs, and other wireless networks as well as addressing common network security requirements.

WISN QoS Management: The general concept for this functional block is to optimize the performance of WISN based on the measured operational characteristics of the WISN and the measured RF environment characteristics. The WISN QoS self-test is used to determine if the current operational performance falls within the specified QoS tolerance. If not, corrective measurements are taken to adapt the network's performance. In addition, RF environment-sensing data are used to estimate RF environment characteristics that could impact the performance of the network, such as location and power levels of interference sources.

This characterization can then be used to predict performance impact on the WISN, and the WISN can apply corrective measures to prevent the QoS from falling below the desired tolerance levels.

As depicted in Fig. 5, optimization could be conducted at a central location and the operational changes are downloaded to the network. An important constraint for this functional block is that updating the WISN needs to be cost-effective, e.g., if the sensor nodes in the WISN are energy-constrained, then the energy cost required for updating the network needs to be less than the energy savings obtained by the performance improvement achieved by the update. Even though the WISN QoS Management is depicted as a centralized process, a distributed version of the process is not precluded and could provide a more efficient approach for certain WISN implementations.

5.2. Example WISN QoS management in an interference environment

The following example illustrates the WISN QoS Management strategy for providing dynamic QoS control within WISN. The example focuses on WISN operating in a time varying RF interference environment. The goal of the example is to illustrate the interaction between wireless technologies, RF environment, application based QoS requirement, and the QoS management.

For the example, the wireless industrial sensor network is based on Bluetooth technology operating in the presence of IEEE 802.11b interference. The scenario is illustrative of hierarchical network architecture where a sensor network is deployed using a wireless personal area network (WPAN) technology and IEEE 802.11b is used as a wireless backbone on a plant floor. The network topology for the analysis is given in Fig. 6(a). Bluetooth nodes are located on a fixed grid at 3-m intervals and are depicted as circles, each labeled H_i, in Fig. 6(a). For clarity, not all of the nodes are labeled in the figure. This topology is similar to a mesh network deployed as a sensor network within a manufacturing plant.

For the analysis presented, an exponential decaying path loss model is used for determining the received power [Eq. (1), but without the shadowing term]. Given path loss exponent, $n=3$, and Bluetooth transmit power of EIRP=0 dBm, Bluetooth nodes can reliably transmit 10 m. The neighborhoods for the source node, H_0, and destination node, H_{39}, are depicted in the figure by two semicircles (dashed lines). The minimum number of hops required to transmit a packet from H_0 to H_{39} is 3. Due to the relatively high degree of connectivity, there are 33 routes requiring 3 hops (two are illustrated in the figure, $R_1=[H_0H_{19}H_{20}H_{39}]$ and $R_2=[H_0H_{12}H_{27}H_{39}]$) and there are 1122 routes requiring 4 hops ($R_3=[H_0H_6H_{15}H_{33}H_{39}]$ illustrates a 4-hop route). IEEE 802.11b interference sources are located at the triangles in Fig. 6(a): I_1 at location {10,0} and I_2 at location {6,5}.

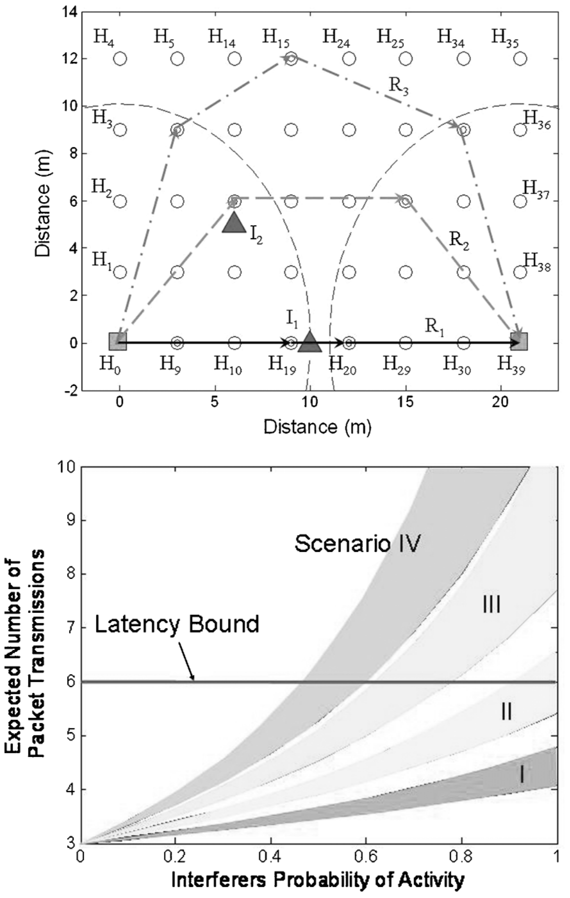


Fig. 6. (a) Network topology for Bluetooth WISN with IEEE 802.11b interference scenario; (b) expected number of transmissions vs the level of interference activity level for each scenario.

As motivated in Section 4, variations in time latency are a critical QoS parameter for WISN. Other QoS constraints, Fig. 1, are inherently interconnected and will need to be considered to fully evaluate and maintain the WISN QoS requirements. For the purpose of the example, only time latency will be considered where the latency is based on the time required to multihop the control message from H_0 to H_{39}. Due to the time varying characteristics of the interference sources, different routes through the network will provide improved end-to-end QoS performance, i.e., reduced latency and reduced variability in the latency. To illustrate, four scenarios are considered where each scenario examines a different number of interference sources. The scenarios are defined as follows:

- Scenario I: One IEEE 802.11b interference source at I_1,
- Scenario II: Two IEEE 802.11b interference sources—one at I_1 and one at I_2,
- Scenario III: Three IEEE 802.11b interference sources—two at I_1 and one at I_2,
- Scenario IV: Four IEEE 802.11b interference sources—three at I_1 and one at I_2.

For Scenarios II through IV, the interference source at I_1 is representative of an IEEE 802.11b access point with multiple transceivers operating in different frequency bands and utilizing a common antenna. Independence is assumed between the multiple interference sources.

The latency in transmitting the control message is directly related to the expected number of retransmissions required for the message to be successfully transmitted over a given route, $\bar{N}_{Tx}(R_i)$. As an example for R_1,

$$\bar{N}_{Tx}(R_1) = \bar{N}_{Tx}(H_0,H_{19}) + \bar{N}_{Tx}(H_{19},H_{20}) + \bar{N}_{Tx}(H_{20},H_{39}), \tag{4}$$

where $\bar{N}_{Tx}(H_i,H_j)$ is the expected number of transmissions to successfully transmit a message from node H_i to node H_j. Due to interference, each hop is susceptible to requiring one or more retransmissions. The likelihood of retransmission is based on the collision probability, i.e., the probability the Bluetooth packet will need to be retransmitted due to IEEE 802.11b interference [12]. For the purposes of this discussion, a key parameter in determining the collision probability is the likelihood an interference source is active, $\Pr[A_k]$. The probability of activity for the interference sources would be monitored by the rf environment-sensing network and used to establish a QoS management policy to be used by the WISN. The details concerning how the QoS management policy would be implemented are beyond the scope of the current discussion.

The impact on the WISN transmission latency was evaluated to illustrate the utility of QoS management. For each scenario, $\bar{N}_{Tx}(R_i)$ was evaluated for all possible routes R_i of hop length three and four. For each scenario, the probability of activity was varied in order to examine the effect of interference on the number of transmissions. In order to simplify the display of the results, all interference sources are at the same level of activity, $\Pr[A]=\Pr[A_k]\,\forall\, k$. Results are depicted in Fig. 6(b), where the graphs represent the spread in the expected number of packet transmissions required to multihop a single packet from the source to the sink. For the majority of the scenarios and interference levels, route R_1 is the worst 3-hop route, the one requiring the maximum number of expected retransmissions and therefore the greatest latency. The reason for this is the interference sources located at I_1 cause Bluetooth transmissions from H_0 to H_{19} to be susceptible to collisions and, therefore, a higher retransmission rate. In addition, the Bluetooth transmissions from H_{19} to H_{20} are also susceptible to collisions, but at a lower rate. For Scenario I, the lowest latency route is R_2, and for Scenario II, the lowest latency route changes from R_2 to $[H_0H_9H_{20}H_{39}]$. This is due to the introduction of the interference source at I_2. As the number of interference sources increases at location I_1, the lowest latency route changes from a 3-hop to a 4-hop route, i.e., R_3.

For the purpose of the example, the expected number of packet transmissions should be less than six, shown in Fig. 6(b). The latency bound is obtained by considering the impact of the variation of the communication latency in conjunction with the effect on the process control governed by the industrial application, presented in Section 4. Therefore, given that the RF environment-sensing network detects activity from a single interferer located at I_1, the WISN should operate within the QoS tolerance without intervention from the WISN QoS Management. This prediction is substantiated by running a QoS self-test within the WISN to verify the self-test results are consistent with the predicted time latency results estimated by the WISN QoS Management. At the other extreme, if Scenario IV is detected then, based on the estimated interference activity levels, certain routes within the WISN should be eliminated from consideration in order to ensure the required QoS. Given Scenario IV with activity levels in access of 60% would require additional intervention. This could be handled by establishing an activity usage policy within the IEEE 802.11b network or, if this is not feasible, additional measures would need to be taken within the WISN network to improve the latency.

6. Conclusions

Wireless communications is poised to support technical innovations in the industrial community with the widespread use of wireless sensors providing economic benefits to industrial end users. In addition to this, societal benefits will evolve through reduced emissions and energy consumption. In order to facilitate the wireless communication supplier and end user community in achieving a successful WISN solution, an integrated framework is presented for designing the WISN. As detailed above, the framework can be summarized by three essential components:

QoS Definition: QoS is the central measure of effectiveness in both the design evaluation in developing the WISN solution and the maintenance of the implemented WISN. A broad definition is applied in defining the MOPs used in characterizing the QoS requirements: throughput, latency, reliability, security, adaptability, and affordability. These MOPs can then be used to define measurable and quantifiable parameters based on mapping functional needs onto operational requirements.

QoS Assessment: A framework for defining measurable and quantifiable parameters for the QoS provides both a context for application domain and communication experts to address the QoS requirements as well as a method for estimating these requirements. As presented in this article, control theory can provide such a framework in which the interdependence between the industrial control process and communication network can be evaluated and bounds on the communication requirements can be established.

QoS Management: The time varying and harsh characteristics of the industrial RF environment in conjunction with the need to maintain the QoS requirements established for the industrial application dictates the need for a control's paradigm for QoS management. As presented in this article, the paradigm involves a feedback loop based on the WISN QoS self-test to actively manage the QoS. Due to the nature of the industrial RF environment and the network coherence time, the WISN self-test data are augmented with an external RF environment-sensing network. The RF environment characteristics can then be used by the WISN QoS Management block to predict the WISN performance and adapt the operational characteristics of the WISN to meet the application specific QoS set point.

References

[1] Industrial Wireless Technology for the 21st Century. U.S. DOE Office of Energy Efficiency and Renewable Energy, http://www.oit.doe.gov/sens_cont/pdfs/wireless_technology.pdf, December 2002.

[2] Wireless Industrial Networking Alliance (WINA). http://www.wina.org.

[3] Weaver, A. C., Survey of industrial information technology. Proceedings of IECON'01, 2001, pp. 2056–2061.

[4] Wiberg, P.-A. and Bilstrup, U., Wireless technology in industry—Applications and user scenarios. Proc. of ETFA, 2001, pp. 123–131.

[5] Perrig, A., Stankovic, J., and Wagner, D., Security in wireless sensor networks. Commun. ACM **47**(6), 53–57 (2004).

[6] Kjesbu, S. and Brunsvik, T., Radio wave propagation in industrial environments. Proc. of IECON, 2000, 4, pp. 2425–2430.

[7] Rappaport, T., Characterization of UHF multipath radio channels in factory buildings. IEEE Trans. Antennas Propag. **37**, 1058–1069 (1989).

[8] Howitt, I., WLAN and WPAN Coexistence in UL Band. IEEE Trans. Veh. Technol. **50**, 1114–1124 (2001).

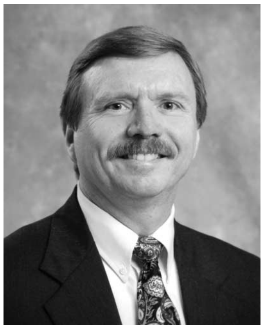
[9] Li, B. and Nahrstedt, K., A control-based middleware framework for quality of service adaptations. IEEE J. Sel. Areas Commun. **17**(9), 1632–1650 (1999).

[10] Mangold, S., Zhong, Z., Challapali, K., and Chou, C. T., Spectrum agile radio: Radio resource measurements for opportunistic spectrum usage. Proc. of GlobComm 04, pp. 3467–3471.

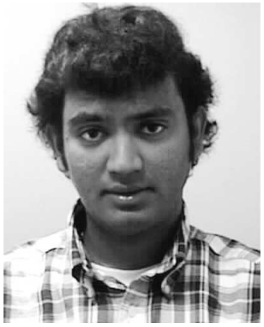
[11] Landry, R., Grace, K., and Saidi, A., On the design and management of heterogeneous networks: A predictability-based perspective. IEEE Commun. Mag. **42**(11), 80–87 (2004).

[12] Howitt, I., Bluetooth performance in the presence of 802.11b WLAN. IEEE Trans. Veh. Technol. **51**, 1640–1651 (2002).

Ivan Howitt Dr. Howitt received the BEE and MSEE from Georgia Institute of Technology in 1982 and 1990, respectively, and the Ph.D. degree in electrical engineering from University of California, Davis in 1995. He has worked as a Research Engineer with Georgia Tech Research Institute, a Visiting Assistant Professor at Virginia Tech, and an Assistant Professor at the University of Wisconsin, Milwaukee. In 2002, he joined the Department of Electrical & Computer Engineering, University of North Carolina at Charlotte as an Associate Professor. His research interests include interoperability issues facing UL band wireless services, methods for mitigating interference, and approaches for optimizing wireless network performance.



Wayne W. Manges Mr. Manges currently directs the U.S. Department of Energy's Industrial Wireless Program at ORNL focusing on the needs of the hard industries from DOE's Industrial Technologies Program. With 28 years at Oak Ridge National Lab, Wayne works extensively with steel, paper, and other industries to bring robust, wireless technology to their markets. He has been declared a visionary for his early views on wireless applications and has published and presented papers around the world and continues as a contributing editor for Sensors Magazine. He holds degrees from California University of Pennsylvania, University of Pittsburgh, Rensselaer Polytechnic Institute, and University of Tennessee.



Phani Teja Kuruganti Mr. Kuruganti received his MS degree in Electrical Engineering from the University of Tennessee, Knoxville in 2003, and a BE in Electronics and Communication Engineering from Osmania University, Hyderabad in 2001. He is now a research engineer at Oak Ridge National Laboratory, Oak Ridge, TN. His current research interests are industrial wireless communications, collaborative signal and information processing in sensor networks, and large scale hi-fidelity modeling and simulation.

Glenn O. Allgood Dr. Allgood is a Distinguished Researcher at Oak Ridge National Laboratory and is a member of the Modeling and Simulation Group in the Computational Science and Engineering Division. He has over 35 years experience in technology application and R&D that covers private industry, the military, academia, and the U.S. Government. He has over 125 articles, papers, and publication in areas such as finite element modeling, human factors, advance control, wireless systems, and cognition and complex systems, and has over 10 patents and invention disclosures. His current research interests are R&D economics and the study of complex systems and their emergent behaviors.

José A. Gutierrez Dr. Gutierrez is the Technology Manager of the Embedded Systems and Communications Department of the Innovation Center at Eaton Corp. His scientific focus is in the field of embedded systems and wireless networking design for commercial and industrial applications. He is the chief technical editor of the IEEE 802.15.4 standard and former Program Manager of the Zigbee Alliance. In addition, he is a member of the board of directors and technical chairman of the Wireless Industrial Network Alliance. Dr. Gutierrez has over 20 publications related to embedded wireless networking, artificial intelligence, automatic control, and robotic vision, including a book on low-rate wireless personal area networks.

James M. Conrad Dr. Conrad received his bachelor's degree in computer science from the University of Illinois, Urbana, and his master's and doctorate degrees in computer engineering from North Carolina State University. He is currently an associate professor at the University of North Carolina at Charlotte. He has served as an assistant professor at the University of Arkansas and as an instructor at North Carolina State University. He has also worked at IBM and Ericsson/Sony Ericsson. He is the author of numerous books, book chapters, journal articles, and conference papers in the areas of robotics, embedded systems, and wireless communications.