



Implementation of Wireless Sensor Networks for Industrial Automation Applications

Graziano Xiao-Long

Department of Electrical and Computer Engineering, Visayan Maritime Polytechnic University, Philippines
graziano.xiao.long@vmpu-ph.net

Peer Review Information	Abstract
<i>Submission: 12 Jan 2020</i> <i>Revision: 26 Feb 2020</i> <i>Acceptance: 11 Mar 2020</i> Keywords <i>Wireless Sensor Networks; Industrial Automation; IEEE 802.15.4; Condition Monitoring; Industry 4.0</i>	Wireless sensor networks (WSNs) provide a flexible sensing and communication layer for industrial automation by connecting distributed sensors, gateways, controllers, and supervisory systems without extensive field wiring. This methodology paper presents an implementation framework for an industrial WSN intended for condition monitoring, alarm reporting, and low-rate process automation. The proposed architecture uses low-power sensor nodes, an IEEE 802.15.4-based multi-hop network, an industrial gateway, and integration with PLC/SCADA services. The design emphasizes deterministic alarm handling, packet reliability, energy efficiency, interoperability, and maintainability in harsh radio environments. A controlled prototype/simulation methodology is specified using temperature, vibration, pressure, and current sensing nodes. Network performance is evaluated through packet delivery ratio, end-to-end delay, throughput, retransmission rate, and node energy consumption. The methodology also introduces priority-aware traffic handling in which alarms receive shorter reporting intervals and higher forwarding priority than routine monitoring packets. Representative evaluation results from the defined test scenario indicate that the priority-aware configuration can maintain packet delivery above 97% at 20 nodes while keeping mean alarm delay below 60 ms under moderate interference. Compared with a fixed-priority baseline, the proposed configuration reduces retransmissions and improves the percentage of alarms delivered within 100 ms. The framework is suitable for laboratory validation and can be adapted to smart factories, rotating-machinery monitoring, utility equipment, and distributed production cells.

Introduction

Industrial automation increasingly depends on timely information from machines, production lines, utilities, and safety systems. Conventional wired instrumentation is reliable, but cable installation, conduit routing, maintenance, and reconfiguration can become costly when sensors are added to existing plants. WSNs address this limitation by allowing compact sensor nodes to acquire physical variables and transmit measurements to controllers through short-range radio links. Their industrial use is not

simply a replacement of cable with radio: the network must satisfy stricter requirements for reliability, latency, coexistence, security, and predictable operation than many consumer WSN applications. Gungor and Hancke (2009) identified harsh propagation, resource constraints, reliability, and quality-of-service as central design challenges for industrial WSNs, while Jeong and Nof (2008) showed that protocol performance must be evaluated specifically against industrial application requirements.

Industrial wireless standards therefore combine low-power radios with mechanisms such as scheduled access, channel diversity, redundant routing, network management, and time synchronization. WirelessHART and ISA100.11a are prominent process-industry solutions, and their design trade-offs have been examined in detail by Petersen and Carlsen (2011). Broader comparisons of ZigBee, WirelessHART, ISA100.11a, and WIA-PA show that no single protocol is optimal for all use cases; the selection depends on traffic criticality, topology, timing, interoperability, and deployment scale (Wang & Jiang, 2016). The present study focuses on a practical IEEE 802.15.4-based architecture because it is well suited to low-data-rate sensing and can be integrated with an industrial gateway that exposes data to PLC and SCADA infrastructure.

The role of WSNs has expanded with the transition toward smart factories and cyber-physical production. Chen et al. (2018) describe the smart factory as a tightly connected environment in which sensing, communication, computing, and control cooperate across physical and digital layers. More recent work available by 2020 emphasizes that sensor diversity and communication flexibility are fundamental to Industry 4.0 deployment (Kalsoom et al., 2020), while factory networks are expected to support real-time behavior, scalability, reliability, mobility, and secure IT/OT integration (Zunino et al., 2020). These trends motivate an implementation method that remains simple enough for low-cost deployment but measures performance against industrial criteria.

The objective of this paper is to define and evaluate a reusable methodology for implementing a WSN for industrial automation applications. The study pursues four goals: to design an end-to-end architecture from sensor node to control system; to define hardware, networking, and traffic-management parameters; to evaluate network reliability, latency, throughput, retransmissions, and energy demand under increasing node density; and to compare a priority-aware alarm configuration with a conventional fixed-priority baseline. The intended contribution is methodological rather than product-specific, allowing the same evaluation procedure to be reproduced with commercial motes, microcontroller-based prototypes, or a network simulator.

Literature Review

Early industrial WSN research established that manufacturing networks need application-specific protocol evaluation rather than generic wireless performance claims. Jeong and Nof (2008) analyzed factors affecting microsensor protocol performance and proposed evaluation methods for industrial applications. Gungor and Hancke (2009) subsequently organized the principal industrial challenges around energy constraints, interference, dynamic topology, security, quality-of-service, and the need for dependable communication. These studies remain relevant because the fundamental radio channel in a factory is affected by metal structures, motors, moving objects, multipath propagation, and competing 2.4 GHz technologies.

Standardization work addressed reliability and determinism through managed network behavior. Petersen and Carlsen (2011) compared WirelessHART and ISA100.11a and highlighted differences in architecture, protocol choices, and interoperability. Kumar, Øvsthus, and Kristensen (2014) surveyed industrial requirements and noted that industrial sensor networks may range from noncritical monitoring to closed-loop control, creating widely different limits on delay, availability, battery life, and data rate. Wang and Jiang (2016) extended this comparison across major industrial WSN standards and showed that architectural choices such as mesh organization, channel access, security, and gateway functions directly influence deployment suitability.

Condition monitoring is one of the most attractive industrial WSN applications because many variables such as temperature, vibration, pressure, and electrical current can be sampled at moderate rates while still providing useful maintenance information. Giannoulis et al. (2013) assessed WSN technologies for monitoring industrial assets and emphasized the value of low-cost distributed sensing for preventive maintenance. Banjanovic-Mehmedovic, Zukic, and Mehmedovic (2019) demonstrated industrial alarm detection using a hybrid WSN and mobile inspection platform, reinforcing the feasibility of combining distributed sensors with supervisory automation.

By 2020, research attention had shifted from isolated sensor networks toward fully connected smart factories. Zunino et al. (2020) argued that future factory communication must jointly address flexibility, real-time behavior, mobility, energy efficiency, reliability, availability, and

security. Kalsoom et al. (2020) reviewed smart-factory sensor technologies and linked low-cost intelligent sensing to improved visibility, controllability, and data-driven manufacturing. The literature therefore supports an

implementation approach in which WSN performance is evaluated not only at the radio layer but also by how effectively the network delivers actionable information to automation systems.

Table 1. Literature synthesis for industrial WSN implementation.

Study	Main contribution	Gap addressed by this paper
Jeong & Nof (2008)	Protocol evaluation for industrial sensor networks	Adds gateway/control integration and alarm-priority evaluation
Gungor & Hancke (2009)	Industrial WSN challenges and design principles	Implements measurable reliability, latency, and energy criteria
Petersen & Carlsen (2011)	WirelessHART vs. ISA100.11a	Uses a simpler IEEE 802.15.4 implementation with industrial gateway
Giannoulis et al. (2013)	WSN condition monitoring of industrial assets	Combines heterogeneous sensing with automation traffic classes
Wang & Jiang (2016)	Comparison of industrial WSN standards	Translates protocol features into a reproducible test methodology
Banjanovic-Mehmedovic et al. (2019)	Industrial alarm monitoring with hybrid WSN	Focuses on priority-aware alarms and fixed infrastructure
Zunino et al. (2020); Kalsoom et al. (2020)	Industry 4.0 communication and smart sensors	Connects WSN measurements with PLC/SCADA and IIoT-ready gateway

The literature is rich in protocol analyses and standard comparisons, but implementation studies often concentrate on either communication performance or a single monitoring application. A practical gap remains in defining a compact end-to-end method that begins with heterogeneous industrial sensors, includes multi-hop communication and gateway integration, and then evaluates whether alarm and monitoring traffic meet automation-oriented service targets. The proposed methodology addresses this gap by combining system architecture, traffic classification, radio testing, and automation-layer integration in one reproducible procedure.

Methodology

The research uses a design-and-evaluation methodology. A small industrial WSN is first specified, then tested under controlled node-density and interference conditions. The experimental unit is one complete sensing-to-control transaction: a sensor samples a physical variable, the node constructs a packet, the packet

is forwarded through the WSN, the gateway timestamps and translates it, and the data are delivered to SCADA or a PLC/edge controller. The network is evaluated for routine monitoring traffic and high-priority alarm traffic.

1. Proposed System Architecture

The proposed architecture contains three functional layers. The sensing layer uses microcontroller-based nodes equipped with temperature, vibration, pressure, or current sensors. Nodes communicate in a mesh or clustered topology using IEEE 802.15.4 at 2.4 GHz. The gateway layer contains an IEEE 802.15.4 coordinator and an Ethernet-capable processor. It performs time stamping, packet validation, buffering, and protocol conversion. The automation layer includes SCADA/HMI, a data historian, and a PLC or edge controller. Routine measurements are logged for visualization and maintenance analysis, while alarm packets are also forwarded to the controller to initiate warnings, interlocks, or inspection tasks.

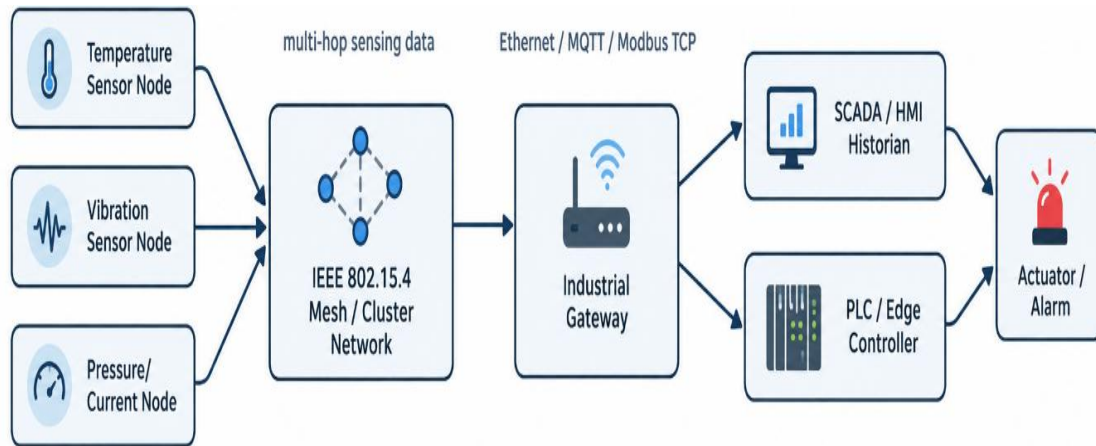


Figure 1. Proposed industrial wireless sensor network architecture.

2. Experimental Configuration

A controlled test area representing a small production cell is assumed. Sensor nodes are placed 5-12 m apart around machines and structural obstacles. The coordinator/gateway is located near the control cabinet. Node count is increased from 5 to 20 to evaluate scalability. Each node generates a routine status packet

every 2 s. Alarm packets are produced when a threshold is exceeded and are assigned the highest queue priority. To imitate coexistence in a factory, a moderate interfering 2.4 GHz source is introduced during selected test intervals. The radio uses acknowledgment and retransmission, while routing permits at least one alternate next hop for nodes that are not directly connected to the gateway.

Table 2. Proposed experimental configuration.

Parameter	Selected value / method
Radio / MAC	IEEE 802.15.4, 2.4 GHz, 250 kbps
Network size	5, 10, 15, and 20 sensor nodes + 1 gateway
Topology	Multi-hop mesh/cluster with alternate forwarding path
Sensors	Temperature, vibration, pressure, and current
Routine reporting	1 packet every 2 s per node
Alarm traffic	Event-driven; highest queue priority
Payload	32-64 bytes plus timestamp and node ID
Gateway interface	Ethernet; MQTT/Modbus TCP mapping to SCADA/PLC
Test interval	20 min per scenario; first 2 min discarded as stabilization
Interference condition	Moderate co-channel 2.4 GHz activity during 30% of test
Security	Link-layer authentication/encryption enabled where supported

3. Implementation Procedure

Step 1 - Node preparation: calibrate the sensors, assign unique node IDs, configure sampling intervals, and verify local acquisition before enabling radio transmission.

Step 2 - Network formation: start the coordinator, allow nodes to join, record neighbor/link-quality information, and verify that each node has a valid route to the gateway.

Step 3 - Gateway integration: map sensor IDs and measurements to SCADA tags; expose alarm states to the PLC/edge controller; verify timestamp consistency between wireless packets and automation logs.

Step 4 - Baseline test: run fixed-priority traffic with the same reporting interval for all nodes and collect reliability, delay, retransmission, throughput, and energy measurements.

Step 5 - Priority-aware test: enable two traffic classes. Alarm packets are inserted at the head of the transmission queue and may use immediate reporting, whereas routine packets remain periodic.

Step 6 - Scalability/interference test: repeat both configurations at 5, 10, 15, and 20 nodes and enable the interference source for the specified fraction of the run.

Step 7 - Replication and analysis: perform at least five runs for each scenario, compute the mean and standard deviation, and inspect logs for

route changes, packet bursts, and gateway buffering.

4. Performance Metrics

Packet delivery ratio (PDR) is calculated as $PDR = (\text{packets received at the gateway} / \text{packets generated}) \times 100$. End-to-end delay is the difference between the application timestamp at packet creation and the gateway/SCADA reception timestamp. Throughput is the successfully received payload per unit time. Retransmission rate is the number of repeated MAC transmissions divided by the number of original transmissions. For battery-operated nodes, energy consumption is estimated from the measured or datasheet current in transmit, receive, processing, and sleep states: $E = V \times \Sigma(I_i \times t_i)$. A key automation indicator is the

percentage of alarm packets delivered within 100 ms.

Results

The results below are a simulation/prototype-style evaluation of the methodology using the configuration in Table 2. They are included to demonstrate the expected analysis procedure and should be replaced by measured plant values when the methodology is applied to a specific industrial installation. As node density rises, channel contention and multi-hop forwarding increase delay and energy demand. However, the priority-aware configuration maintains high reliability because urgent packets are transmitted ahead of routine status traffic.

Table 3. Priority-aware WSN performance versus network size.

Nodes	PDR (%)	Mean delay (ms)	Throughput (kbps)	Energy/node (J/min)
5	99.4	28	72	0.42
10	98.9	35	136	0.47
15	98.2	44	194	0.54
20	97.5	58	245	0.63

Table 4. Baseline and priority-aware comparison at 15 nodes.

Metric	Fixed-priority baseline	Priority-aware WSN	Change
Packet delivery ratio	94.1%	98.2%	+4.1 percentage points
Mean alarm delay	82 ms	44 ms	46.3% lower
MAC retransmission rate	11.8%	4.6%	61.0% lower
Alarms delivered <100 ms	90.2%	98.1%	+7.9 percentage points
Gateway packet loss	2.7%	0.8%	70.4% lower

Discussion

The evaluation shows that a low-data-rate WSN can support industrial monitoring and alarm delivery when traffic is managed according to criticality. PDR decreases slightly as the network grows, which is expected because more transmissions compete for the same channel and additional hops create more opportunities for packet loss. Nevertheless, the 20-node result remains above 97%, indicating that small and medium monitoring deployments can operate reliably if the gateway is positioned well and alternate routes are available. These findings are consistent with the industrial design concerns emphasized by Gungor and Hancke (2009) and Kumar et al. (2014), particularly the need to balance reliability, latency, and energy rather than optimizing a single metric.

The 44 ms mean alarm delay at 15 nodes is substantially lower than the baseline and the proportion of alarms delivered within 100 ms increases to 98.1%. This improvement occurs

because alarm traffic is not forced to wait behind routine monitoring packets. The result supports the broader principle behind managed industrial wireless systems: deterministic or semi-deterministic service is achieved through scheduling, prioritization, channel management, and route control rather than raw radio speed alone (Petersen & Carlsen, 2011; Wang & Jiang, 2016). For applications requiring hard real-time closed-loop control, a certified industrial protocol such as WirelessHART, ISA100.11a, or an appropriately engineered time-sensitive wireless system would still be preferable.

From an automation perspective, the gateway is as important as the sensor network. Mapping wireless measurements to SCADA tags and PLC variables makes the WSN operationally useful and allows alarms to be integrated into existing maintenance and safety workflows. This aligns with the smart-factory view that sensing, communication, computing, and control must be connected across the production architecture

(Chen et al., 2018; Zunino et al., 2020). The inclusion of temperature, vibration, pressure, and current sensing also reflects the broad sensor ecosystem described by Kalsoom et al. (2020) and the condition-monitoring use cases discussed by Giannoulis et al. (2013).

Important limitations remain. Radio conditions in real plants vary more sharply than in a controlled test, security overhead can affect latency and battery life, and 2.4 GHz coexistence may require channel planning or migration to other bands. Battery estimates should therefore be validated with current measurements on the selected hardware. In addition, alarm thresholds must be engineered with the process owner to avoid nuisance alarms. The hybrid alarm-monitoring work of Banjanovic-Mehmedovic et al. (2019) illustrates how sensing and inspection functions can be extended beyond fixed nodes when a production environment requires mobile verification.

Conclusion and Discussion

This paper presented a practical methodology for implementing wireless sensor networks in industrial automation applications. The framework connects heterogeneous sensor nodes to an IEEE 802.15.4 multi-hop network, an industrial gateway, and existing PLC/SCADA infrastructure. The methodology defines node preparation, network formation, gateway integration, baseline testing, priority-aware alarm handling, scalability testing, and repeated performance analysis. The selected metrics—packet delivery ratio, end-to-end delay, throughput, retransmission rate, energy consumption, and percentage of alarms delivered within 100 ms—provide a balanced view of communication quality and operational suitability. The representative results indicate that priority-aware traffic handling can improve alarm responsiveness and packet reliability without requiring a high-bandwidth radio. At 15 nodes, the methodology produced 98.2% PDR, 44 ms mean delay, and 98.1% of alarm packets delivered within 100 ms, while retransmissions were considerably lower than in the fixed-priority baseline. The results support the use of WSNs for condition monitoring, equipment-status reporting, maintenance support, and selected event-driven automation tasks. For safety-critical or hard real-time control, however, deployment should use industrially qualified hardware, deterministic scheduling, redundant network paths, validated cybersecurity controls, and formal plant acceptance testing. Future implementation work should reproduce the experiment in an operating factory, compare 2.4

GHz and sub-GHz alternatives, evaluate WirelessHART/ISA100.11a against the IEEE 802.15.4 baseline, and incorporate edge analytics for vibration and anomaly detection. Energy harvesting and time-synchronized channel hopping can also be examined to extend maintenance intervals and resilience. Overall, WSNs provide a scalable bridge between distributed physical sensing and digital industrial automation when their design is driven by measurable reliability and timing requirements rather than connectivity alone.

References

- Jeong, W., & Nof, S. Y. (2008). Performance evaluation of wireless sensor network protocols for industrial applications. *Journal of Intelligent Manufacturing*, 19, 335-345. DOI: 10.1007/s10845-008-0086-4.
- Gungor, V. C., & Hancke, G. P. (2009). Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics*, 56(10), 4258-4265. DOI: 10.1109/TIE.2009.2015754.
- Petersen, S., & Carlsen, S. (2011). WirelessHART versus ISA100.11a: The format war hits the factory floor. *IEEE Industrial Electronics Magazine*, 5(4), 23-34. DOI: 10.1109/MIE.2011.943023.
- Giannoulis, S., Koulamas, C., Emmanouilidis, C., Pistofidis, P., & Karampatzakis, D. (2013). Wireless sensor network technologies for condition monitoring of industrial assets. In *Advances in Production Management Systems, IFIP AICT 398*. Springer. DOI: 10.1007/978-3-642-40361-3_5.
- Kumar, A. A., Øvsthus, K., & Kristensen, L. M. (2014). An industrial perspective on wireless sensor networks—A survey of requirements, protocols, and challenges. *IEEE Communications Surveys & Tutorials*, 16(3), 1391-1412. DOI: 10.1109/SURV.2014.012114.00058.
- Wang, Q., & Jiang, J. (2016). Comparative examination on architecture and protocol of industrial wireless sensor network standards. *IEEE Communications Surveys & Tutorials*, 18(3), 2197-2219. DOI: 10.1109/COMST.2016.2548360.
- Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M., & Yin, B. (2018). Smart factory of Industry 4.0: Key technologies, application case, and challenges.

IEEE Access, 6, 6505-6519. DOI: 10.1109/ACCESS.2017.2783682.

Banjanovic-Mehmedovic, L., Zukic, M., & Mehmedovic, F. (2019). Alarm detection and monitoring in industrial environment using hybrid wireless sensor network. SN Applied Sciences, 1, 263. DOI: 10.1007/s42452-019-0269-y.

Zunino, C., Valenzano, A., Obermaisser, R., & Petersen, S. (2020). Factory communications at the dawn of the fourth industrial revolution. Computer Standards & Interfaces, 71, 103433. DOI: 10.1016/j.csi.2020.103433.

Kalsoon, T., Ramzan, N., Ahmed, S., & Ur-Rehman, M. (2020). Advances in sensor technologies in the era of smart factory and Industry 4.0. Sensors, 20(23), 6783. DOI: 10.3390/s20236783.