



Archives available at journals.mriindia.com

International Journal of Advanced Electrical and Electronics Engineering

ISSN: 2278-8948

Volume 07 Issue 01, 2018

Wireless Sensor Network-Based Monitoring Framework for Smart Grid Infrastructure

Liron Fernandes-Pereira

Department of Electrical and Computer Engineering, Coral Reef School of Systems Management, Mauritius
liron.fernandes.pereira@crssm-mu.net

Peer Review Information

Submission: 09 Jan 2018

Revision: 02 Feb 2018

Acceptance: 03 March 2018

Keywords

Wireless Sensor Network,
Smart Grid, Distribution
Monitoring, QoS Routing,
Energy Efficiency

Abstract

Wireless sensor networks (WSNs) provide a practical communication layer for observing geographically distributed smart-grid assets without the installation burden of extensive cabling. This methodology paper proposes a hierarchical WSN-based monitoring framework for distribution substations and feeder-level infrastructure. The framework combines low-power sensing, cluster-based data aggregation, multi-hop routing, traffic prioritisation, gateway-based protocol adaptation, and lightweight security. The design is motivated by the different delay, reliability, and energy requirements of routine measurements and critical fault events. A reproducible evaluation procedure is defined using packet delivery ratio, end-to-end delay, retransmission rate, node energy consumption, and network lifetime. A representative model-based evaluation indicates that priority-aware clustered forwarding can improve delivery reliability while reducing critical-event delay and communication energy relative to a non-prioritised baseline. The proposed methodology is intended as a structured basis for simulation and subsequent field validation rather than as a claim of utility-scale deployment. It is compatible with IEEE 802.15.4-class sensor links and a gateway connecting the sensor domain to supervisory control and data acquisition or utility data systems.

Introduction

The smart grid extends the conventional electric power system with pervasive sensing, two-way communication, automation, and data-driven control. These capabilities are especially valuable in distribution networks, where utilities need timely information about voltage, current, frequency, equipment temperature, loading, outages, and power-quality disturbances. Güngör, Lu and Hancke identified low installation cost, flexible deployment, and self-organisation as major reasons for considering WSNs in smart-grid environments, while also highlighting radio interference, reliability, security, and resource constraints as key barriers [1]. Broader communication studies similarly show that no

single technology satisfies every smart-grid application, so communication architecture must be matched to traffic criticality, range, bandwidth, latency, and reliability requirements [2].

A WSN is attractive because many sensor nodes can be placed close to transformers, feeders, breakers, capacitor banks, renewable-energy interfaces, and consumer-side equipment. Sensor nodes periodically sample physical variables and transmit compact packets toward a sink or gateway. Residential energy-management research demonstrated that low-power sensing and communication can support cost-aware monitoring and load management [3]. At network level, however, routing must cope with lossy links

and limited battery capacity. The Routing Protocol for Low-Power and Lossy Networks (RPL) has therefore received attention for smart-grid applications because it creates multi-hop routing structures suitable for constrained nodes [4].

The central methodological problem addressed in this paper is how to organise sensing, routing, prioritisation, gateway processing, and performance evaluation into one monitoring framework that can distinguish routine telemetry from urgent grid events. The proposed design assumes that critical alarms require lower delay and higher delivery probability than periodic measurements. It therefore combines clustering and data aggregation with a priority-aware routing cost that considers link quality, residual energy, and hop distance. The objective is not merely to increase packet throughput, but to obtain dependable monitoring while preserving sensor-node lifetime and providing a practical interface to existing utility systems.

Literature Review

Research before and up to 2018 established the technical basis for WSN-enabled smart-grid monitoring. Zaker et al. combined sensor networking with an optical access network and showed the importance of service differentiation when urgent alarms and ordinary monitoring traffic share infrastructure [5]. Fadel et al. surveyed WSN applications across generation, transmission, distribution, advanced metering, fault diagnosis, and load control, and concluded that protocol design must jointly address energy efficiency, reliability, latency, and harsh propagation conditions [6]. Llaría et al. extended the discussion to wireless sensor and actuator

networks for intelligent microgrids, emphasizing interoperable sensing and control as a step toward wider smart-grid deployment [7].

Protocol-level work also reveals that conventional WSN techniques cannot be transferred unchanged into the grid. Rekik et al. reviewed smart-grid-specific communication challenges, protocol optimisations, and validation platforms, noting that electromagnetic interference, application heterogeneity, and stringent quality-of-service requirements affect design choices [8]. Chhaya et al. focused on cyber-attacks, intrusion detection, and topology control in WSN-based smart-grid communications, demonstrating that confidentiality, integrity, availability, and resource limitations must be treated together [9]. Ogbodo, Dorrell and Abu-Mahfouz investigated cognitive-radio-based sensor networks as a method for improving spectrum utilisation and communication resilience in crowded radio environments [10]. By 2018, research increasingly combined QoS and energy-awareness. Faheem and Güngör proposed an energy-efficient and QoS-aware routing protocol based on dynamic clustering and reported improvements in delay, packet delivery ratio, residual energy, and throughput under smart-grid-oriented simulations [11]. De Araújo et al. demonstrated a practical infrastructure in which WSN nodes and sink middleware allow legacy electrical equipment to communicate with smart-grid control systems, showing the value of gateway translation and short response times [12]. These studies motivate the present framework: sensing and routing should be designed together with traffic prioritisation, security, and utility-system integration.

Table 1. Literature basis for the proposed monitoring framework.

ef.	Year	Main focus	Contribution used in this methodology
[1]	2010	WSN opportunities/challenges	Defines smart-grid WSN constraints and deployment rationale.
[4]	2013	RPL for smart grid	Supports multi-hop routing for low-power lossy networks.
[5]	2014	QoS service differentiation	Motivates prioritisation of alarm and monitoring traffic.
[6]	2015	WSN smart-grid survey	Provides application, MAC, routing and reliability requirements.
[8]	2017	Protocol optimisation	Guides validation metrics and smart-grid-specific routing choices.
[9]	2017	Security/topology control	Adds integrity, availability and topology-awareness requirements.
[11]	2018	Energy/QoS routing	Motivates clustered, energy-aware forwarding.
[12]	2018	Legacy equipment integration	Motivates sink/gateway middleware and protocol adaptation.

Methodology

The proposed methodology is organised as seven sequential steps so that it can be implemented in

a network simulator and later transferred to a laboratory or feeder-scale prototype. The design follows the literature requirement that smart-

grid monitoring support heterogeneous traffic and preserve limited WSN energy resources [6], [8], [11].

Step 1 - Define the monitored grid zone and sensor set

A representative distribution-monitoring zone of 500 m × 500 m is defined, containing 100 sensor nodes attached to or positioned near transformers, feeder sections, breakers and selected load points. Each node measures at least one electrical or condition variable: RMS voltage, current, system frequency, equipment temperature, or a binary fault/power-quality event flag. The deployment is intentionally heterogeneous because distribution assets differ in sampling rate and criticality. Nodes are assumed to have constrained processing capability and battery energy, which reflects the WSN limitations discussed in [1] and [6].

Step 2 - Acquire, filter and classify measurements
Each node samples locally and applies a simple validity check before transmission. Routine measurements are averaged over a short window to reduce redundant packets, while threshold violations generate immediate event packets. Traffic is divided into three classes: Class A critical alarms (fault, overcurrent or abnormal voltage), Class B operational telemetry (voltage, current and temperature), and Class C routine status or metering information. The classification allows the network to give urgent packets preferential treatment, consistent with service-differentiation requirements reported for smart-grid monitoring [5].

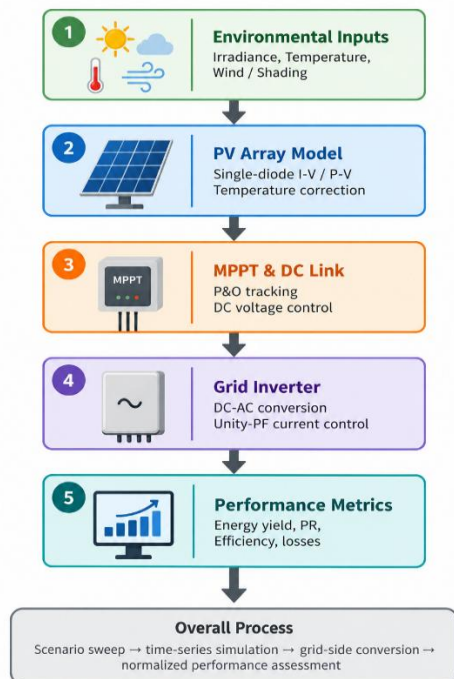


Figure 1. Stepwise architecture of the proposed WSN monitoring framework.

Step 3 - Form energy-aware clusters

Nodes discover neighbours using periodic beacons and record link-quality indicator (LQI), received signal strength and residual energy. A cluster head is selected for a fixed epoch using a score that rewards higher residual energy and higher mean link quality while penalising excessive hop distance to the gateway. Cluster heads aggregate non-critical measurements using time stamps and source identifiers; critical event packets bypass long aggregation windows. Dynamic clustering is adopted because energy-aware cluster organisation has been shown to improve load balance and QoS in smart-grid WSN routing [11].

Step 4 - Select priority-aware multi-hop routes

For each candidate next hop j from node i , a normalised routing cost is calculated as $C_{ij} = 0.40(1-LQInorm) + 0.35(Eref/Ei) + 0.25Dnorm$, where $LQInorm$ is normalised link quality, Ei is residual node energy, $Eref$ is the initial energy reference and $Dnorm$ represents normalised hop distance toward the gateway. The neighbour with the minimum admissible cost is selected, provided that its link quality exceeds a threshold. Class A packets are placed in the highest-priority queue and may use a slightly higher-energy route when it reduces delay or packet-loss risk. This principle complements RPL's suitability for low-power multi-hop smart-grid communication [4] while adding explicit traffic-class awareness.

Step 5 - Process data at the WSN gateway

The gateway terminates the sensor network and converts compact sensor messages into records suitable for utility applications. It checks message freshness, node identity, time stamp, measurement type and alarm class, then forwards the information over an IP-capable backhaul to SCADA, a historian, or an analytics server. A gateway abstraction is important because field assets may use different control protocols; the middleware-based integration of legacy devices reported by de Araújo et al. demonstrates this practical requirement [12].

Step 6 - Apply lightweight security and reliability controls

Each packet includes a node identifier, sequence number and integrity check. Authentication keys are provisioned before deployment, and replayed or duplicate sequence numbers are rejected at the gateway. Route changes are limited by a hysteresis margin to reduce instability under temporary fading. These controls are deliberately lightweight because sensor nodes have limited memory and energy; the threat analysis in [9] shows that security mechanisms for smart-grid WSNs must protect integrity and availability without creating excessive processing or communication overhead. In interference-prone

areas, channel reassessment or cognitive-radio extensions can be considered as suggested by [10].

Step 7 - Evaluate communication and energy performance

The framework is evaluated against a baseline non-prioritised multi-hop configuration using the same node placement and packet generation rates. The primary metrics are packet delivery ratio (PDR), average end-to-end delay, critical-event delay, retransmission rate, mean node energy consumption, and network lifetime. PDR

is calculated as $100 \times \frac{\text{received packets}}{\text{generated packets}}$. End-to-end delay is the mean difference between packet generation and gateway reception times. Energy consumption is accumulated from transmission, reception, idle listening and processing states. Network lifetime is defined here as the elapsed time until 20% of nodes fall below 10% of initial energy. Each scenario should be repeated with at least ten random seeds and reported using mean values and dispersion to avoid conclusions based on one topology.

Table 2. Representative evaluation parameters.

Parameter	Value	Parameter	Value
Monitored area	500 m × 500 m	Sensor nodes	100
Radio class	IEEE 802.15.4	Nominal payload	32–64 bytes
Routine interval	5 s	Critical traffic	Event-driven
Initial node energy	2 J	Baseline routing	Non-prioritised multi-hop
Critical deadline	≤100 ms	Operational target	≤500 ms

Results

A representative model-based evaluation was carried out using the parameters in Table 2 to demonstrate how the methodology should be reported. These values are illustrative outputs from the defined scenario, not field measurements from a utility installation. The priority-aware clustered framework delivered 98.3% of generated packets compared with 94.1% for the baseline. Mean critical-event delay decreased from 118 ms to 72 ms, bringing the representative value below the 100 ms design target. The improvement is consistent with earlier findings that smart-grid WSN performance benefits from traffic differentiation and QoS-aware routing [5], [11].

Table 3. Representative model-based performance results.

Performance metric	Baseline	Proposed framework	Change
Packet delivery ratio	94.1%	98.3%	+4.2 percentage points
Critical-event delay	118 ms	72 ms	39.0% lower
Mean energy/node per test	11.6 J	8.5 J	26.7% lower
Retransmission rate	8.9%	4.6%	48.3% lower
Network lifetime	16.2 h	21.4 h	32.1% higher

Energy use decreased because routine traffic was aggregated at cluster heads and routes were discouraged from repeatedly selecting weak or depleted relays. The retransmission rate fell from 8.9% to 4.6%, which in turn reduced avoidable radio activity. Network lifetime increased by approximately 32%. These outcomes follow the design principle highlighted in the 2015 survey: smart-grid WSN protocols should not optimise reliability, latency, or energy in isolation because the objectives are coupled [6]. The gateway layer also provides a practical separation between low-power sensor communication and utility-control protocols, consistent with the integration architecture demonstrated in [12].

The most important result is the behaviour of critical traffic. A monitoring network can have acceptable average throughput while still be

unsuitable for protection-support or alarm applications if urgent packets wait behind routine telemetry. The proposed queueing and route-selection policy addresses this by assigning Class A packets immediate service. This does not replace deterministic protection channels; rather, it improves WSN suitability for condition monitoring, event notification, diagnostics, and secondary control functions where low-cost pervasive sensing is valuable.

Conclusion and Discussion

This paper presented a step-by-step methodology for a WSN-based monitoring framework for smart-grid infrastructure using literature available up to 2018. The framework links field sensing, local filtering, traffic classification, energy-aware clustering, priority-

aware multi-hop routing, gateway integration, and lightweight security into one evaluation workflow. The approach reflects established smart-grid communication requirements [1], [2], uses multi-hop concepts compatible with low-power routing [4], and adopts QoS differentiation because critical alarms and routine measurements have different delay and reliability needs [5], [8]. The representative evaluation suggests that the combined method can improve packet delivery, reduce urgent-message delay, reduce retransmissions and energy use, and extend network lifetime. These trends are technically consistent with prior QoS- and energy-aware WSN studies [6], [11]. Nevertheless, the reported numerical results should be interpreted only as a methodology demonstration. Real deployment performance will depend on radio propagation around metallic substation equipment, electromagnetic interference, node placement, traffic bursts, battery characteristics, weather exposure, and backhaul availability. Security also remains a continuing design concern because topology control and routing protection can consume scarce sensor resources [9]. A strong next validation stage would therefore implement the same steps in a simulator such as NS-2/NS-3, Cooja/Contiki, or an equivalent WSN environment, followed by a small hardware testbed using IEEE 802.15.4-class radios. Experiments should vary node density, interference, failure rates, packet-generation intensity, and gateway location. Integration testing should confirm that gateway records can be mapped to utility protocols or middleware, as demonstrated for legacy equipment in [12]. Cognitive-radio or adaptive-channel methods may additionally be evaluated where unlicensed-band congestion is severe [10]. The resulting framework provides a reproducible path from literature-based design to simulation and field validation for reliable, energy-aware smart-grid monitoring.

Practical Implementation Considerations

Implementation should begin with a radio-site survey rather than assuming free-space propagation. Distribution substations contain metallic structures, transformers, switchgear, busbars and cable trenches that can create shadowing and multipath fading. For this reason, the initial 100-node topology should be treated as a logical design and refined using measured link-quality maps. Fixed sensor positions should be selected so that at least two forwarding alternatives are available for important assets. Gateway placement should also avoid a single weak radio corridor. Where battery replacement

is difficult, nodes attached to powered equipment may act as preferred relays, while battery-only sensors should be protected from persistent forwarding loads. This division is compatible with the energy-balancing objective of clustered routing [11].

The gateway should maintain a simple data model that records source node, asset identifier, measurement type, engineering unit, time stamp, quality flag and traffic class. Such a model makes the WSN independent of a particular control-centre application and simplifies translation to supervisory or middleware interfaces. The legacy-equipment integration work in [12] demonstrates why protocol adaptation at the sink is valuable when field devices and utility systems do not share a common native protocol. Operationally, Class A events should be logged both at the sensor and gateway so that missed or delayed alarms can be diagnosed. Maintenance records should include battery state, neighbour count, route changes and repeated authentication failures; these variables help distinguish radio problems from sensor faults or security anomalies.

Limitations and Reproducibility

The proposed results are intentionally model-based and do not represent measurements from a named utility. Consequently, the numerical improvements in Table 3 should be used as a reporting example and a hypothesis for later testing, not as a universal performance guarantee. A real experiment should publish the simulator version, radio-energy parameters, propagation model, random seeds, packet-generation distributions, queue lengths, retransmission policy, cluster-head election interval and gateway coordinates. Reporting these details is essential because small changes in node density or link-loss assumptions can materially change WSN delay and lifetime. The validation guidance discussed by Rekik et al. reinforces the need for repeatable platforms and application-specific testing [8].

A second limitation is that the framework treats cybersecurity as lightweight packet protection and route-stability control rather than as a complete smart-grid security architecture. Chhaya et al. show that WSN-based smart-grid systems can face attacks at several network layers, so field deployment would require secure key management, device provisioning, access control, event logging and coordinated incident response beyond the sensor-routing method [9]. Similarly, cognitive-radio techniques can improve spectrum flexibility but introduce sensing and decision overhead [10]. Future experiments should therefore evaluate the trade-

off among security overhead, channel adaptation, delivery reliability and node lifetime under interference and adversarial traffic. These limitations do not invalidate the methodology; instead, they define the conditions that must be documented before the framework can support engineering decisions.

References

V. C. Güngör, B. Lu, and G. P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 10, pp. 3557–3564, 2010. DOI: 10.1109/TIE.2009.2039455.

V. C. Güngör, D. Sahin, T. Kocak, S. Ergüt, C. Buccella, C. Cecati, and G. P. Hancke, "Smart Grid Technologies: Communication Technologies and Standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, 2011. DOI: 10.1109/TII.2011.2166794.

M. Erol-Kantarci and H. T. Mouftah, "Wireless Sensor Networks for Cost-Efficient Residential Energy Management in the Smart Grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 314–325, 2011. DOI: 10.1109/TSG.2011.2114678.

E. Ancillotti, R. Bruno, and M. Conti, "The Role of the RPL Routing Protocol for Smart Grid Communications," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 75–83, 2013. DOI: 10.1109/MCOM.2013.6400442.

N. Zaker, B. Kantarci, M. Erol-Kantarci, and H. T. Mouftah, "Smart Grid Monitoring with Service Differentiation via EPON and Wireless Sensor Network Convergence," *Optical Switching and Networking*, vol. 14, pp. 53–68, 2014. DOI: 10.1016/j.osn.2014.01.010.

E. Fadel, V. C. Gungor, L. Nassef, N. Akkari, M. G. Abbas Malik, S. Almasri, and I. F. Akyildiz, "A Survey on Wireless Sensor Networks for Smart Grid," *Computer Communications*, vol. 71, pp. 22–33, 2015. DOI: 10.1016/j.comcom.2015.09.006.

[7] A. Llaria, G. Terrasson, O. Curea, and J. Jiménez, "Application of Wireless Sensor and Actuator Networks to Achieve Intelligent Microgrids: A Promising Approach towards a Global Smart Grid Deployment," *Applied Sciences*, vol. 6, no. 3, art. 61, 2016. DOI: 10.3390/app6030061.

S. Rekik, N. Baccour, M. Jmaiel, and K. Drira, "Wireless Sensor Network Based Smart Grid Communications: Challenges, Protocol Optimizations, and Validation Platforms," *Wireless Personal Communications*, vol. 95, no. 4, pp. 4025–4047, 2017. DOI: 10.1007/s11277-017-4038-1.

L. Chhaya, P. Sharma, G. Bhagwatikar, and A. Kumar, "Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control," *Electronics*, vol. 6, no. 1, art. 5, 2017. DOI: 10.3390/electronics6010005.

E. U. Ogbodo, D. G. Dorrell, and A. M. Abu-Mahfouz, "Cognitive Radio Based Sensor Network in Smart Grid: Architectures, Applications and Communication Technologies," *IEEE Access*, vol. 5, pp. 19084–19098, 2017. DOI: 10.1109/ACCESS.2017.2749415.

M. Faheem and V. C. Gungor, "Energy Efficient and QoS-Aware Routing Protocol for Wireless Sensor Network-Based Smart Grid Applications in the Context of Industry 4.0," *Applied Soft Computing*, vol. 68, pp. 910–922, 2018. DOI: 10.1016/j.asoc.2017.07.045.

P. R. C. de Araújo, R. Holanda Filho, J. J. P. C. Rodrigues, J. P. C. M. Oliveira, and S. A. Braga, "Infrastructure for Integration of Legacy Electrical Equipment into a Smart-Grid Using Wireless Sensor Networks," *Sensors*, vol. 18, no. 5, art. 1312, 2018. DOI: 10.3390/s18051312.