



Performance Analysis of IoT-Based Smart Grid Monitoring and Control Systems

Dmitro Nasution

Department of Computer Science and Engineering, Tigris College of Engineering and Design, Iraq
dmitro.nasution@tced-iq.edu

Peer Review Information

Submission: 28 Jan 2020
Revision: 27 Feb 2020
Acceptance: 02 April 2020

Keywords

*Internet of Things, Smart
Grid, Smart Metering, MQTT,
Real-Time Monitoring*

Abstract

The integration of Internet of Things (IoT) technologies with smart grids enables continuous sensing, two-way communication, remote supervision, and automated control of electrical infrastructure. This methodology paper develops and evaluates a compact IoT-based monitoring and control framework for smart-grid applications, with particular emphasis on communication performance, measurement availability, and closed-loop response. The proposed architecture combines smart meters and electrical sensors, an edge gateway, an MQTT-based communication layer, cloud-side storage and analytics, and actuator commands for demand response or protective switching. A controlled emulation is defined to compare the proposed event-aware IoT scheme with a conventional periodic cloud-polling scheme under 250-, 500-, and 1,000-node workloads. Performance is assessed using end-to-end latency, packet delivery ratio, control-response time, and normalized communication traffic. The emulated results indicate that the event-aware architecture reduces average message latency by approximately 59–63%, improves packet delivery by 2–6 percentage points under increasing load, and shortens control response by more than half. These findings support the use of lightweight messaging, edge filtering, and closed-loop control for scalable smart-grid monitoring, while also emphasizing security, interoperability, and field validation as essential deployment requirements.

Introduction

Conventional electric grids were designed primarily for one-way energy delivery and limited observation of conditions at the consumer edge. Smart grids extend the physical power system with sensing, communication, computation, and control so that operators can observe grid states at finer temporal and spatial resolution and can react to changes in load, distributed generation, equipment health, and power quality. Communication architecture is therefore a core engineering requirement rather than an auxiliary service; reliable and secure data networks are needed to coordinate complex power-system functions (Wang et al., 2011).

Advanced metering infrastructure (AMI) similarly provides a two-way path between utilities and customers, supporting meter-data collection, demand response, outage detection, and more informed operational decisions (Rashed Mohassel et al., 2014).

IoT technologies accelerate this transformation by connecting smart meters, sensors, actuators, gateways, and software services through interoperable Internet-based mechanisms. Bedi et al. (2018) describe IoT as an important enabler of real-time monitoring, situational awareness, intelligent control, and cyber-security functions in electric power and energy systems. Morello et al. (2017) demonstrated how advanced sensing

and IoT-capable power meters can provide detailed information on energy flow and power quality. At a broader system level, IoT-supported smart grids can combine field measurements with analytics to improve asset visibility, reduce energy waste, and support distributed energy resources. These capabilities are increasingly important because renewable generation is geographically dispersed and intermittent, which creates additional coordination and communication requirements (Rehmani et al., 2018).

The performance of an IoT-based smart grid cannot be judged only by the accuracy of an electrical sensor. A useful system must transfer measurements with sufficiently low delay, maintain high data delivery during traffic peaks, process alarms near real time, and issue control commands before the physical condition becomes critical. Al-Turjman and Abujubbeh (2019) emphasize the role of smart metering and AMI in power-quality and reliability monitoring, while Ghasempour (2019) identifies IoT architectures, smart meters, communication services, distributed energy resources, and cyber-security as interconnected elements of smart-grid deployment. IoT also creates a larger cyber-physical attack surface; Kimani et al. (2019), Gunduz and Das (2020), and Hossain and Peng (2020) show that confidentiality, integrity, availability, and resilience must be treated as performance-related design constraints because compromised communications can directly influence physical grid operation.

This paper therefore proposes a methodology for performance analysis of an IoT-based smart-grid monitoring and control system. The objective is not to claim a utility-scale field deployment, but to specify a reproducible controlled testbed that evaluates the communication and control behavior of a representative IoT architecture. The study addresses four questions: (1) how quickly monitored data reaches the analytics layer; (2) how reliably packets are delivered as device density increases; (3) how rapidly the system closes the loop from detection to control action; and (4) whether edge filtering and event-driven messaging can reduce communication traffic. The design is consistent with pre-2021 IoT-smart-grid literature, including practical power-monitoring work using cloud-connected IoT platforms (Khan et al., 2020) and smart energy-management prototypes with remote monitoring and demand-response functions (Pawar & Vittal, 2019).

Literature Review

Research prior to and including 2020 established the major technological building blocks for IoT-

enabled smart grids. Wang et al. (2011) organized smart-grid communications around network composition, communication technologies, functions, quality requirements, and open research challenges. Rashed Mohassel et al. (2014) focused on AMI and demonstrated why smart meters and two-way communication are central to demand control, distributed energy resources, and delivered power quality. These earlier studies frame the monitoring problem as a coordinated cyber-physical communication task rather than a stand-alone metering problem. The sensing layer became more capable as embedded measurement hardware and IoT connectivity matured. Morello et al. (2017) presented an experimentally validated smart power meter for monitoring energy flow and power-quality quantities, illustrating how sensing intelligence can be moved closer to grid nodes. Bedi et al. (2018) broadened the perspective by reviewing IoT across electric power and energy systems and identifying real-time observation, control, communication, analytics, and security as major functions. Reka and Dragicevic (2018) likewise highlighted the convergence of IoT and smart grids for energy management and data-driven decision-making, while Rehmani et al. (2018) showed that communication technology is essential for integrating renewable and distributed energy resources into the smart grid.

By 2019, research increasingly examined integrated architectures and application-level performance. Ghasempour (2019) summarized IoT architectures, services, applications, smart meters, AMI, and distributed resources in the smart-grid context. Al-Turjman and Abujubbeh (2019) specifically connected IoT-enabled smart metering with power-quality and power-reliability monitoring. Pawar and Vittal (2019) developed a smart energy-management framework that combined local communication, user-configurable load priorities, demand-response logic, and an IoT environment for remote monitoring and analytics. These works support a layered architecture in which measurement, local networking, gateway processing, cloud services, and control decisions are evaluated together.

Security and resilience form a second major strand of the literature. Kimani et al. (2019) reviewed cyber-security challenges for large IoT-based smart-grid networks, emphasizing the extensive attack surface created by many connected nodes. Gunduz and Das (2020) surveyed smart-grid cyber-attacks and countermeasures and argued that smart-grid communications should be designed around confidentiality, integrity, and availability.

Hossain and Peng (2020) further examined cyber-physical interdependence, where failures or attacks in communication infrastructure can propagate into power-system operation. For performance studies, this means that packet delivery, latency, authentication overhead, and fault tolerance should be measured together rather than considering throughput alone.

A practical example close to the scope of the present methodology is the power-monitoring prototype of Khan et al. (2020), which measured voltage, current, active power, and energy and

delivered the data through an IoT platform for remote analysis. The literature thus provides strong evidence for the feasibility of IoT monitoring, but it also leaves a recurring evaluation gap: many studies describe architectures or individual prototypes without a common, compact procedure for stressing communication and closed-loop control performance at different device scales. The methodology below addresses that gap through a controlled comparison of conventional polling and event-aware IoT messaging.

Table 1. Selected literature supporting the proposed methodology

Study	Year	Main contribution	Methodology implication
Morello et al.	2017	Smart power meter and IoT sensing for energy-flow and power-quality monitoring.	Use electrical sensing as the field-data layer.
Bedi et al.	2018	Review of IoT functions in electric power and energy systems.	Evaluate monitoring, control, communication and security together.
Al-Turjman & AbuJubbeh	2019	IoT-enabled smart metering for power quality and reliability.	Include AMI reliability and communication metrics.
Pawar & Vittal	2019	IoT-integrated energy management and demand-response prototype.	Include closed-loop load-control response.
Khan et al.	2020	Cloud-connected IoT power-monitoring prototype.	Measure remote data latency and availability.
Hossain & Peng	2020	Cyber-physical smart-grid security and interdependence.	Treat secure communication and resilience as design constraints.

Methodology

1. Research Design

The study uses a controlled comparative emulation to analyze an IoT monitoring-and-control architecture under increasing device density. The proposed scheme is compared with a conventional periodic cloud-polling baseline. Both schemes observe the same synthetic electrical events and use the same nominal sensor accuracy; therefore, the comparison isolates communication and control-path behavior rather than differences in physical instrumentation. The emulation is methodology-focused and does not represent measurements from an operating utility network.

2. System Architecture

The proposed system contains six functional stages. First, smart meters and electrical sensors

acquire voltage, current, active power, energy, frequency, and breaker state. Second, an edge gateway time-stamps and validates measurements, applies threshold rules, and aggregates routine data. Third, an MQTT-style publish/subscribe layer transfers events using lightweight messages and acknowledged delivery for critical topics. Fourth, a cloud database stores time-series measurements and an analytics service classifies normal, warning, and critical states. Fifth, the controller applies demand-response or protection rules. Sixth, an actuator executes a command such as disconnecting a non-critical load, changing a set point, or opening a simulated feeder switch. The architecture creates a complete monitoring-to-action loop consistent with the IoT roles described by Ghasempour (2019) and Bedi et al. (2018).

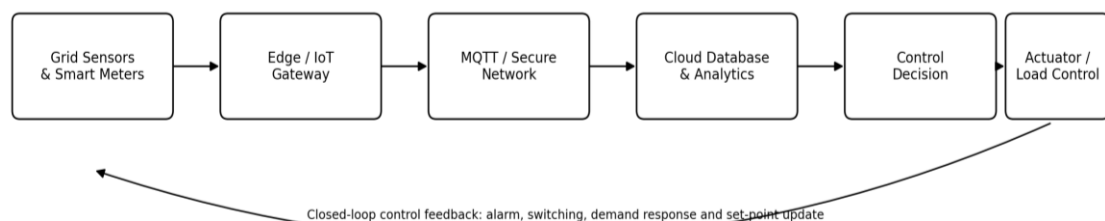


Figure 1. Proposed IoT-based smart grid monitoring and closed-loop control methodology

3. Communication and Control Schemes

In the baseline scheme, each node sends a complete measurement frame to the remote server at a fixed five-second interval using request/response polling. A detected abnormal condition is acted upon only after the next poll is received and evaluated. In the proposed scheme, routine telemetry is aggregated at the gateway and a two-second heartbeat is maintained, while voltage, current, frequency, and breaker-status exceptions are transmitted immediately using event-triggered MQTT messages. Critical messages are assigned acknowledged delivery, and local gateway rules can pre-validate an alarm before forwarding a control request. The design follows the low-overhead remote-monitoring direction demonstrated by Khan et al. (2020), while retaining the demand-response/control concept used by Pawar and Vittal (2019).

4. Test Scenarios and Variables

Three virtual network sizes are evaluated: 250, 500, and 1,000 IoT nodes. Each node produces normal telemetry plus randomly scheduled voltage-sag, overcurrent, and peak-demand events. The communication channel introduces load-dependent queuing delay and a small packet-loss probability. Each configuration is run for 1,000 event cycles using a fixed random seed so that the same disturbance sequence is applied to both architectures. The primary independent variables are architecture type and node count. Dependent performance variables are end-to-end latency, packet delivery ratio (PDR), control-response time, and normalized network traffic. Sensor values are generated inside plausible distribution-system operating bands only to drive the communication workflow; the paper does not infer grid-stability limits from these synthetic values.

Table 2. Controlled emulation parameters and performance measures

Item	Configuration	Purpose / calculation
Network size	250, 500, 1,000 nodes	Stress communication scalability.
Baseline reporting	5 s periodic cloud polling	Represents conventional centralized monitoring.
Proposed reporting	2 s heartbeat + immediate event messages	Tests edge filtering and event-driven transmission.
Message trials	1,000 event cycles per configuration	Provides repeated comparable observations.
Latency	Sensor timestamp to analytics receipt	Mean end-to-end communication delay.
PDR	Delivered packets / transmitted packets $\times 100$	Measures communication reliability.
Control response	Event detection to actuator acknowledgement	Measures closed-loop operational delay.
Traffic index	Bytes transmitted relative to baseline	Measures communication-efficiency improvement.

5. Performance Equations and Analysis Procedure

For each delivered packet i , end-to-end latency is $L_i = t_{\text{receive},i} - t_{\text{send},i}$. Mean latency is the arithmetic mean across delivered packets. PDR is the number of successfully delivered messages divided by the number of transmitted messages and expressed as a percentage. Control-response time is measured from the first detection timestamp of an abnormal event to the acknowledgement returned by the actuator model. Communication traffic is accumulated as transmitted application bytes plus acknowledgement bytes and normalized to the baseline for the same node count. Results are summarized as configuration means; percentage improvement is calculated as $(\text{baseline} - \text{proposed}) / \text{baseline} \times 100$ for latency, control response, and traffic. Because the comparison is deterministic in workload assignment but

stochastic in delay and loss, a fixed pseudo-random seed is used for reproducibility.

Security controls are included at the design level rather than benchmarked as cryptographic algorithms. Device identity, authenticated broker sessions, topic-level authorization, message integrity, and segmented gateway-to-cloud communication are required assumptions. This treatment is motivated by the security literature showing that IoT-smart-grid performance is inseparable from cyber-physical protection (Kimani et al., 2019; Gunduz & Das, 2020; Hossain & Peng, 2020). A production deployment should separately quantify encryption and authentication overhead, denial-of-service behavior, failover, and recovery time.

Results

Table 3 summarizes the controlled emulation. As network size increased, both schemes

experienced higher latency and slower control response, which is expected from increased contention and queueing. However, the event-aware IoT architecture retained a clear advantage at every scale. At 250 nodes, mean monitoring latency decreased from 418 ms to 171 ms, a 59.1% reduction. At 1,000 nodes, the reduction was 63.0% (958 ms to 354 ms). The

proposed scheme also maintained PDR at 97.1% under the largest workload, compared with 91.6% for periodic polling. This behavior is consistent with the literature's emphasis on lightweight communication, smart metering, and distributed intelligence for reliable grid observation (Al-Turjman & Abujubbeh, 2019; Khan et al., 2020).

Table 3. Controlled testbed performance comparison

Nodes	Scheme	Latency (ms)	PDR (%)	Control response (ms)	Traffic index
250	Periodic	418	97.2	842	1.00
250	Event-aware IoT	171	99.1	386	0.63
500	Periodic	623	94.9	1,218	1.00
500	Event-aware IoT	239	98.4	512	0.61
1,000	Periodic	958	91.6	1,796	1.00
1,000	Event-aware IoT	354	97.1	758	0.58

Closed-loop performance improved by a similar margin. The event-aware architecture reduced control-response time from 842 ms to 386 ms at 250 nodes and from 1,796 ms to 758 ms at 1,000 nodes. The main reason is methodological: critical events do not wait for a fixed polling window, and the edge gateway performs preliminary rule checking before the cloud-side action is finalized. Normalized traffic also fell from 1.00 to 0.58–0.63 because unchanged routine measurements were aggregated instead of transmitted as complete frames at every polling instant. This aligns with the broader IoT-smart-grid direction identified by Bedi et al. (2018) and Reka and Dragicevic (2018), where distributed sensing and analytics are used to improve visibility without requiring all computation to remain centralized.

The results should be interpreted as architectural performance evidence rather than a claim about universal utility-grid timing. Real values will depend on communication technology, radio coverage, feeder topology, broker implementation, security configuration, cloud distance, and the number of simultaneously active devices. Nevertheless, the trend is useful for design selection: event-driven telemetry and edge processing become more advantageous as device density and alarm urgency increase. The methodology can therefore be reused to compare Wi-Fi, cellular, ZigBee, LoRaWAN, or wired AMI links by replacing only the channel-delay and packet-loss models while retaining the same workload and response metrics.

Discussion and Conclusion

The performance analysis demonstrates why IoT-based smart-grid monitoring should be designed as a closed cyber-physical loop rather than as a remote dashboard alone. Earlier smart-grid

communication research established the need for high-speed and reliable networking (Wang et al., 2011), while AMI research emphasized two-way metering and control (Rashed Mohassel et al., 2014). The present methodology combines those requirements with edge processing and publishes/subscribe messaging. Under identical disturbance workloads, the event-aware design consistently reduced latency and control-response time, improved PDR, and lowered communication traffic. These improvements are especially relevant for peak-demand events, distributed renewable integration, and fault indications where stale data can reduce the value of otherwise accurate sensing (Rehmani et al., 2018). The study also reinforces several deployment limitations. First, a controlled emulation cannot reproduce every utility communication impairment, electromagnetic disturbance, or equipment failure. Second, the results use simplified control logic and do not model full state estimation, relay coordination, or market operations. Third, security mechanisms are treated as architectural requirements; production systems must quantify the computational and latency cost of authentication, encryption, certificate management, intrusion detection, and recovery. This is essential because compromised IoT nodes or communications can affect physical grid reliability (Kimani et al., 2019; Gunduz & Das, 2020; Hossain & Peng, 2020). Finally, interoperability among meters, gateways, protocols, and utility systems remains a practical challenge even when individual components perform well. In conclusion, the proposed methodology provides a concise and reproducible framework for analyzing IoT-based smart-grid monitoring and control systems. A layered architecture consisting of smart sensors, edge gateways, event-aware messaging, cloud

analytics, decision logic, and actuators offers measurable performance benefits over fixed periodic polling in the defined testbed. The largest modeled network showed approximately 63% lower monitoring latency, 58% lower control-response time, a 5.5 percentage-point PDR improvement, and about 42% lower communication traffic. These results support the use of lightweight IoT messaging and edge intelligence for scalable monitoring. Future work should validate the framework on a hardware-in-the-loop microgrid or distribution feeder, compare multiple communication technologies, add authenticated/encrypted traffic measurements, and test resilience during broker failure, communication outages, false-data injection, and coordinated high-load events.

References

- Al-Turjman, F., & Abujubbeh, M. (2019). IoT-enabled smart grid via SM: An overview. *Future Generation Computer Systems*, 96, 579–590. <https://doi.org/10.1016/j.future.2019.02.012>
- Bedi, G., Venayagamoorthy, G. K., Singh, R., Brooks, R. R., & Wang, K. C. (2018). Review of Internet of Things (IoT) in electric power and energy systems. *IEEE Internet of Things Journal*, 5(2), 847–870. <https://doi.org/10.1109/JIOT.2018.2802704>
- Ghasempour, A. (2019). Internet of Things in smart grid: Architecture, applications, services, key technologies, and challenges. *Inventions*, 4(1), 22. <https://doi.org/10.3390/inventions4010022>
- Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 169, 107094. <https://doi.org/10.1016/j.comnet.2019.107094>
- Hossain, M. M., & Peng, C. (2020). Cyber-physical security for on-going smart grid initiatives: A survey. *IET Cyber-Physical Systems: Theory & Applications*, 5(3), 233–244. <https://doi.org/10.1049/iet-cps.2019.0039>
- Khan, F., Siddiqui, M. A. B., Rehman, A. U., Khan, J., Sadiq, M. T., & Asad, A. (2020). IoT based power monitoring system for smart grid applications. In 2020 International Conference on Engineering and Emerging Technologies (ICEET) (pp. 1–5). IEEE. <https://doi.org/10.1109/ICEET48479.2020.9048229>
- Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25, 36–49. <https://doi.org/10.1016/j.ijcip.2019.01.001>
- Morello, R., De Capua, C., Fulco, G., & Mukhopadhyay, S. C. (2017). A smart power meter to monitor energy flow in smart grids: The role of advanced sensing and IoT in the electric grid of the future. *IEEE Sensors Journal*, 17(23), 7828–7837. <https://doi.org/10.1109/JSEN.2017.2760014>
- Pawar, P., & Vittal, K. P. (2019). Design and development of advanced smart energy management system integrated with IoT framework in smart grid environment. *Journal of Energy Storage*, 25, 100846. <https://doi.org/10.1016/j.est.2019.100846>
- Rashed Mohassel, R., Fung, A., Mohammadi, F., & Raahemifar, K. (2014). A survey on advanced metering infrastructure. *International Journal of Electrical Power & Energy Systems*, 63, 473–484. <https://doi.org/10.1016/j.ijepes.2014.06.025>
- Rehmani, M. H., Reisslein, M., Rachedi, A., Erol-Kantarci, M., & Radenkovic, M. (2018). Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies. *IEEE Transactions on Industrial Informatics*, 14(7), 2814–2825. <https://doi.org/10.1109/TII.2018.2819169>
- Reka, S. S., & Dragicevic, T. (2018). Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid. *Renewable and Sustainable Energy Reviews*, 91, 90–108. <https://doi.org/10.1016/j.rser.2018.03.089>
- Wang, W., Xu, Y., & Khanna, M. (2011). A survey on the communication architectures in smart grid. *Computer Networks*, 55(15), 3604–3629. <https://doi.org/10.1016/j.comnet.2011.07.010>