Scientific Journal of Control Engineering
Volume 12 Issue 1, June 2025, PP. 23-30

Research on Energy Consumption Optimization and Stability of IoT Devices in Complex Environments

Yinghao Tang
Xihua University

Abstract

The Internet of Things (IoT) has become an integral part of various industries, from smart cities to healthcare, driving the need for energy-efficient and stable devices, especially in complex and unpredictable environments. This research investigates the optimization of energy consumption and the enhancement of stability in IoT devices operating in such environments. The study addresses key challenges, including resource constraints, fluctuating environmental conditions, and the increasing complexity of IoT networks. It explores various energy optimization techniques, such as low-power communication protocols, edge and cloud computing, and machine learning models, that help reduce energy usage while maintaining performance. Furthermore, it examines stability enhancement strategies, including fault-tolerant mechanisms, resilient network architectures, and real-time monitoring and adaptive control, that ensure the continuous and reliable operation of IoT devices despite external disruptions. The findings of this research contribute to the development of next-generation IoT systems that are both energy-efficient and resilient, thereby promoting sustainable deployment in real-world applications.

Keywords: IoT Devices; Energy Consumption; Stability Enhancement; Complex Environments; Optimization Techniques; Machine Learning; Edge Computing

1 INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has revolutionized industries such as smart cities, healthcare, and industrial automation. However, as IoT networks grow, they face critical challenges in energy efficiency and system stability, particularly in dynamic and resource-constrained environments. Many IoT devices rely on batteries and operate in remote locations, making energy optimization essential to prolong device lifespan and reduce costs. While existing techniques like duty cycling and adaptive transmission help, they often fail to adapt to real-time conditions, necessitating more intelligent energy management. Stability is equally crucial, as network congestion, interference, and hardware degradation can lead to failures, data loss, and service disruptions in mission-critical applications. Addressing these challenges requires advanced fault tolerance, predictive maintenance, and resilient architectures. This research explores AI-driven energy optimization and stability enhancement strategies to develop a holistic approach that minimizes power consumption while strengthening system resilience, contributing to the sustainable deployment of next-generation IoT infrastructures.

2 ENERGY CONSUMPTION IN IOT DEVICES

2.1 Key Factors Affecting IoT Energy Consumption

Energy consumption in IoT devices is influenced by multiple factors, each contributing to the overall efficiency of the system. One of the most significant factors is the hardware architecture of the device. IoT devices range from simple sensors with limited computational capability to sophisticated processors capable of edge computing. Devices with high-performance processors or integrated sensors typically consume more energy due to their increased operational complexity and processing power demands. Additionally, communication protocols play a crucial role in

energy consumption. IoT devices often rely on wireless communication standards such as Wi-Fi, Zigbee, Bluetooth, and LoRaWAN, which exhibit varying power consumption based on range, transmission frequency, and data rate. For instance, long-range communication technologies like LoRaWAN are energy-efficient for low data rate transmissions over long distances, whereas Wi-Fi demands more power for higher data rates and shorter ranges.

Another key factor is the operating environment, as devices in remote or harsh environments tend to experience increased energy usage due to external factors like temperature fluctuations, humidity, or physical obstructions that can affect signal quality and device performance. Furthermore, the duty cycle or the time a device remains active versus in a sleep mode also affects energy consumption. Devices operating in continuous active mode consume more energy compared to those employing adaptive power management strategies, where tasks are scheduled based on demand. Finally, the task complexity is a significant contributor. More energy-intensive tasks, such as processing large datasets, performing real-time analysis, or transmitting high volumes of data, demand more power compared to simpler operations, such as basic sensing or intermittent data reporting[1].

2.2 Energy Consumption Models

To address the challenge of optimizing energy usage in IoT devices, several energy consumption models have been developed. These models are essential for predicting and evaluating the energy performance of IoT systems under various operating conditions and workloads. One of the most commonly used models is the battery lifetime model, which estimates the battery life of IoT devices based on their energy consumption patterns and operational behaviors. This model helps identify energy-saving opportunities and optimize device operation cycles to extend battery life.

Another important model is the energy-performance trade-off model, which highlights the balance between energy consumption and system performance. IoT devices often face a trade-off between performing complex computations and minimizing energy consumption. By modeling this trade-off, designers can choose optimal strategies to either prioritize energy savings or ensure peak performance when needed. Additionally, dynamic power consumption models are used to monitor and control energy consumption in real-time. These models track energy usage based on workload variations, device states (e.g., active, idle, or sleep modes), and environmental factors, providing insights into when and how to adjust device operation for maximum energy efficiency.

A more advanced approach involves the network-level energy consumption model, which extends energy optimization to the entire IoT network. This model considers the interactions between multiple devices and network components, optimizing energy usage by considering the collective behavior of devices, communication protocols, and network topology. For example, models like the link quality model assess how the quality of the communication channel affects energy consumption, encouraging devices to adjust transmission power levels or change communication routes to reduce energy costs.

3 STABILITY CHALLENGES OF IOT DEVICES IN COMPLEX ENVIRONMENTS

3.1 Impact of Complex Environments on IoT Stability

IoT devices are increasingly deployed in a wide range of environments, many of which are complex and unpredictable. These environments, whether they are urban, industrial, or natural, introduce a variety of factors that can significantly impact the stability and reliability of IoT systems. One of the primary challenges in such environments is the variability of communication channels. In many real-world applications, IoT devices rely on wireless communication protocols such as Wi-Fi, Bluetooth, Zigbee, or cellular networks. However, these wireless communication links are susceptible to interference from physical obstructions, atmospheric conditions, and the presence of other electronic devices. For instance, buildings, trees, or other infrastructure can create signal attenuation, leading to weak or unstable connections, especially in densely populated areas or remote locations where network coverage is sparse. The result is often intermittent connectivity, high packet loss, and degraded overall system performance.

Additionally, environmental factors such as temperature, humidity, vibrations, and electromagnetic interference (EMI) can have direct effects on the hardware and software stability of IoT devices. Extreme temperatures can cause

thermal stress, leading to failures in the components or affecting the sensor accuracy, while high humidity can lead to corrosion of the device components, reducing their operational lifespan. Electromagnetic interference from nearby machinery or power lines may disrupt device communication or cause erroneous data readings, further compromising the device's ability to function reliably[2].

Resource constraints are another significant challenge when deploying IoT devices in complex environments. Many IoT devices, especially those operating in remote or harsh locations, are designed to be low-power and compact to extend their battery life and reduce maintenance needs. However, these resource-constrained devices may struggle to perform complex operations in demanding environments. For instance, devices deployed in industrial settings may need to process large volumes of data from multiple sensors in real-time, but they may not have sufficient processing power, memory, or energy resources to do so effectively, leading to operational instability or failures.

Furthermore, the heterogeneity of IoT devices and networks can lead to compatibility issues in diverse environments. Devices from different manufacturers may operate on proprietary communication protocols, use different data formats, or rely on incompatible security mechanisms. This lack of standardization complicates interoperability and creates a fragmented ecosystem where seamless communication and coordination are difficult to achieve. In critical applications like smart cities or healthcare, where real-time data processing and coordination are paramount, these stability challenges can have far-reaching consequences, including system downtime, inefficient operation, and safety risks.

3.2 Failure Modes and Stability Issues

IoT devices are prone to a range of failure modes when deployed in complex environments, primarily due to the factors mentioned above. These failure modes can manifest in various ways, each affecting the system's overall stability and reliability. One of the most common failure modes is communication failure. In many IoT systems, the failure of communication links between devices or between devices and the central server can lead to significant disruptions. For instance, intermittent or lost packets can prevent devices from sending critical data to the cloud or coordinating with other devices in a network, resulting in degraded performance or complete system failure. Communication failures are particularly problematic in mission-critical IoT applications such as healthcare or industrial automation, where continuous data flow and real-time decision-making are essential[3].

Another failure mode is sensor malfunction or inaccurate data readings. Environmental factors like temperature fluctuations, humidity, or physical stress can lead to sensor drift, calibration issues, or outright failure of sensing components. Inaccurate data readings not only compromise the quality of the information being processed but can also lead to incorrect decisions, especially in systems that rely on real-time data for control or automation. In industrial IoT systems, for example, incorrect sensor readings can trigger false alarms, shut down critical operations, or even damage machinery due to erroneous feedback loops.

Power failures are another significant stability issue in IoT devices. IoT devices that rely on battery power or energy harvesting techniques may experience performance degradation or complete failure when their power sources are depleted. In environments with limited or inconsistent access to power, such as remote monitoring applications in agriculture or environmental monitoring, the failure to maintain an adequate energy supply can lead to prolonged downtime or even device failure. Even in cases where energy harvesting is employed (such as solar or kinetic energy), the inconsistency of the energy source in complex environments adds a layer of uncertainty that can affect device stability.

Additionally, software failures such as bugs, memory leaks, or firmware malfunctions can cause IoT devices to crash or operate erratically. Complex software systems managing the device's functionality may encounter errors due to unpredictable environmental conditions or poor optimization, resulting in the freezing or rebooting of devices, which disrupts system stability. In environments where updates or patches are infrequent due to connectivity limitations or remote deployment, these software failures may go unnoticed, leading to prolonged instability and decreased system reliability.

Finally, network congestion and overload are common causes of instability in IoT networks, particularly when large

numbers of devices are deployed in a localized area. As the network load increases, communication delays, bottlenecks, and even network outages may occur, affecting the performance of the entire system. In complex environments, where high device density is often the norm, IoT devices must contend with congestion from numerous other devices, leading to delayed data transmission, packet loss, or failures in coordinating activities between devices.

4 ENERGY OPTIMIZATION STRATEGIES FOR IOT DEVICES

4.1 Energy-Efficient Communication Protocols

Energy efficiency in communication is one of the most critical aspects of optimizing the power consumption of IoT devices, especially given the limited energy resources of many devices. Communication protocols define how devices exchange data, and optimizing these protocols is essential to reducing the energy required for wireless communication. Several strategies can be employed to design energy-efficient communication protocols that minimize power usage while maintaining the performance of IoT networks.

Low-Power Wide-Area Networks (LPWAN), such as LoRaWAN, Sigfox, and NB-IoT, have emerged as popular communication solutions for IoT devices that need to operate in power-constrained environments. These networks are designed to support long-range communication with minimal energy consumption, making them ideal for IoT devices deployed in remote or hard-to-reach areas. By using low-duty cycle transmissions and minimizing the amount of data transmitted, LPWANs enable energy-efficient communication without compromising the coverage area.

Another key strategy is duty cycling in communication protocols. Duty cycling refers to the practice of putting IoT devices into a low-power sleep mode during periods of inactivity, waking them up only when data transmission or reception is required. This approach significantly reduces the average power consumption of devices by minimizing the time spent in active communication modes. Protocols like IEEE 802.15.4, which underpins standards like Zigbee and Thread, are designed to allow devices to operate with periodic wake-up schedules, thus balancing communication needs with energy efficiency.

The adaptive transmission power is also an effective strategy for reducing energy consumption. Communication protocols that adjust the transmission power based on the distance between devices or the quality of the communication link can reduce energy usage. Devices can lower their transmission power when they are in close proximity to each other, thereby reducing the overall energy required for data transmission. This strategy is especially useful in environments with varying signal strengths, such as urban areas where obstructions and interference can impact the communication range[4].

Moreover, protocol optimization for short-range communication also plays a significant role. Protocols such as Bluetooth Low Energy (BLE) and Zigbee use energy-efficient mechanisms like low-power advertising, efficient frequency hopping, and minimal packet size to reduce power consumption while ensuring that devices can communicate over short to medium distances. By optimizing these protocols for the specific needs of IoT applications, the power consumption of communication activities can be minimized.

4.2 Edge and Cloud Computing-Based Optimization

Energy optimization in IoT systems is increasingly being supported by edge and cloud computing paradigms. These computing architectures allow for the processing of data closer to where it is generated (edge computing) or at centralized data centers (cloud computing), which can lead to substantial reductions in the energy required by devices and networks.

Edge computing is a promising solution for energy optimization in IoT systems, as it reduces the need for continuous data transmission to centralized servers. By processing data locally on the edge devices or nearby edge nodes, the amount of data that needs to be transmitted to the cloud is significantly reduced. This local processing minimizes the energy consumption associated with data transmission and alleviates network congestion. Additionally, edge devices can make real-time decisions without relying on distant servers, further reducing latency and the energy required for

communication. For example, in applications such as smart cities, where IoT devices constantly monitor environmental data, edge computing can filter and preprocess this data before transmitting only relevant information to the cloud, thereby reducing the data load and energy consumption.

Cloud computing, on the other hand, provides a centralized platform for more complex data analysis, storage, and decision-making. While cloud computing itself may require significant energy resources, it can contribute to energy optimization by offloading resource-intensive tasks from IoT devices. Instead of relying on battery-powered IoT devices to perform computation-heavy tasks, the data can be sent to the cloud, where more powerful servers can handle the processing. This reduces the power consumption of the IoT devices by transferring computational burdens to cloud servers that are typically more energy-efficient at scale. Additionally, cloud platforms can implement advanced load balancing and virtualization techniques, which optimize resource allocation and help reduce overall energy consumption in the system.

4.3 AI and Machine Learning for Energy Optimization

Artificial Intelligence (AI) and Machine Learning (ML) have proven to be powerful tools in optimizing energy consumption in IoT devices. By leveraging advanced algorithms, IoT systems can make more intelligent decisions about how, when, and where to use energy, improving the overall energy efficiency of the network.

AI-driven energy management focuses on learning from data patterns and usage behavior to predict when and how devices should operate to minimize energy consumption. For instance, predictive models based on AI can forecast periods of high or low activity, allowing devices to adjust their operating schedules accordingly. Machine learning algorithms can continuously learn from environmental factors and usage patterns, allowing the system to optimize energy consumption in real-time based on dynamic conditions.

A key application of AI in energy optimization is the use of intelligent scheduling for communication and computation tasks. By using AI models, IoT devices can dynamically adjust their duty cycles, wake-up times, and data transmission intervals based on their operational context. For example, in an industrial IoT setting, AI can analyze real-time data from multiple devices and predict when certain machines are likely to be idle, allowing their communication to be scheduled for off-peak times, thus conserving energy. In addition, AI can be used to optimize the load distribution across devices, ensuring that energy consumption is balanced across the network, thereby avoiding unnecessary power drains[5].

Reinforcement learning (RL), a subset of machine learning, can also be applied to optimize energy consumption in IoT networks. In RL, devices are trained to make decisions based on feedback from their environment, where the objective is to minimize energy use while achieving specific performance goals. Through iterative learning and trial-and-error approaches, IoT devices can adapt their behavior to optimize energy usage based on varying conditions, such as network congestion, communication distances, and environmental factors. This dynamic adjustment of operational parameters can significantly improve the overall energy efficiency of the IoT system.

Furthermore, AI can enable the optimization of resource allocation across the network. Using machine learning algorithms, IoT systems can predict network congestion, data traffic, and device energy levels, and optimize how resources are allocated to minimize energy consumption while maintaining performance. AI can also be used for anomaly detection, where it identifies unexpected spikes in energy usage or failure modes, allowing the system to take corrective action before these issues lead to major disruptions.

5 STABILITY ENHANCEMENT TECHNIQUES FOR IOT DEVICES

5.1 Fault-Tolerant Mechanisms

Fault tolerance is a critical aspect of ensuring the stability and reliability of IoT devices, particularly in environments where device failure could have serious consequences. Fault-tolerant mechanisms are designed to enable IoT systems to continue operating correctly even in the presence of hardware or software failures, thereby enhancing their stability and reducing downtime[6].

One fundamental approach to fault tolerance is redundancy, where critical system components, such as communication modules, power supplies, or processing units, are duplicated to prevent a single point of failure. For instance, IoT devices can be equipped with backup communication channels that automatically switch over in case the primary channel experiences disruption, ensuring continuous data flow even in adverse conditions. Similarly, power redundancy through battery backups or energy harvesting methods can prevent devices from shutting down unexpectedly in case of power loss, thus maintaining stability.

Another key fault-tolerant strategy is error detection and correction. IoT devices can be designed to continuously monitor their own operational state and detect anomalies in real-time. Through error detection algorithms, devices can identify discrepancies in their performance, such as communication errors or sensor malfunctions. When an error is detected, error correction mechanisms—such as retransmission protocols or software-based corrections—can be deployed to restore normal operation. This proactive error management helps mitigate the impact of faults before they escalate into system failures.

Additionally, self-healing capabilities can be integrated into IoT devices to enhance their resilience. Self-healing mechanisms allow devices to automatically reconfigure themselves or restart certain functions in response to detected faults, reducing the need for human intervention. For example, if a sensor becomes faulty or unresponsive, the system could automatically switch to a backup sensor or activate an alternative processing algorithm. Such self-healing techniques can dramatically improve the overall fault tolerance of IoT systems and ensure continued operation in the face of unpredictable failures.

5.2 Resilient Network Architectures

As IoT systems increasingly rely on networks for communication and data exchange, the stability of the entire system is often contingent on the robustness of the underlying network architecture. In dynamic and complex environments, where devices may frequently experience communication failures, congestion, or interference, resilient network architectures are crucial for maintaining continuous and reliable system operation.

One approach to building resilient IoT networks is distributed network architectures, where the load and responsibilities are spread across multiple nodes rather than being concentrated in a single point of failure. For instance, mesh network architectures, such as those used in Zigbee or Thread, allow IoT devices to communicate with one another through multiple paths. If one device or communication link fails, the network can reconfigure itself, ensuring that communication can continue through alternate routes. This self-healing capability makes mesh networks highly resilient to disruptions and ensures the stability of the IoT system[7].

Multi-path communication is another strategy used to increase network resilience. By enabling data to be transmitted over multiple communication paths simultaneously, the system can ensure that even if one path is blocked or degraded, the data can still reach its destination via an alternative route. This is particularly important in IoT systems deployed in environments with unreliable or unpredictable wireless conditions, such as industrial settings or urban areas with high interference. The ability to reroute communication dynamically based on network conditions further enhances the overall stability of the IoT system.

To further enhance resilience, network slicing can be employed in IoT systems, especially those utilizing 5G networks. Network slicing allows IoT systems to create virtual, isolated network segments with dedicated resources and customized quality-of-service (QoS) parameters. By segmenting the network, IoT systems can ensure that critical communications are prioritized and are less susceptible to congestion or interference from non-critical traffic. This type of resilience ensures that essential IoT applications, such as healthcare monitoring or industrial control systems, can maintain their functionality even under heavy network load or external disruptions.

Adaptive routing protocols are also essential for maintaining stability in complex environments. These protocols adjust the routing decisions based on real-time data, such as the network's topology, traffic load, and link quality. Through this dynamic routing, the network can avoid congestion points and ensure that the communication remains reliable, even as the network conditions change. Furthermore, these protocols are designed to react to network failures or degradation, automatically rerouting data through alternate paths to preserve system stability.

5.3 Real-Time Monitoring and Adaptive Control

Real-time monitoring and adaptive control play a vital role in enhancing the stability of IoT devices, particularly in environments where conditions change frequently or are unpredictable. By continuously monitoring device performance and environmental variables, IoT systems can detect potential issues before they lead to failures and adapt to the evolving conditions in real-time.

Continuous monitoring of IoT devices and the network infrastructure is essential for identifying emerging problems, such as increased latency, reduced signal strength, or device malfunctions. IoT systems can integrate sensors and diagnostic tools to track vital parameters, such as power consumption, communication reliability, temperature, and processing performance. This data is collected and analyzed in real-time to provide a comprehensive view of the system's health. In the event of a detected anomaly, such as a sharp increase in energy consumption or a drop in communication quality, the system can trigger alerts and take corrective actions to mitigate the problem.

The integration of adaptive control systems allows IoT devices to modify their operating conditions in response to real-time data. For example, an adaptive control algorithm could adjust the device's duty cycle based on the battery level, the current network traffic, or the device's proximity to other IoT nodes. In an industrial setting, adaptive control might involve adjusting the sensing frequency of an IoT device based on environmental factors like temperature or humidity, which could otherwise interfere with sensor readings. By dynamically adapting to changing conditions, IoT systems can maintain stable performance despite fluctuations in environmental variables[8].

Furthermore, predictive analytics powered by machine learning can be incorporated into real-time monitoring systems to foresee potential stability issues before they occur. By analyzing historical and real-time data, AI algorithms can predict failures, network congestion, or other disturbances that might affect system stability. Based on these predictions, IoT devices can preemptively adjust their behavior, such as reducing transmission power to avoid network congestion or switching to a backup communication protocol when interference is detected.

In some cases, real-time monitoring can be enhanced by edge computing, which enables devices to process data locally and make instant decisions without the need for cloud-based intervention. Edge computing can be particularly useful in situations where network latency is critical, such as in healthcare monitoring or autonomous vehicle applications, where immediate responses are necessary to maintain system stability and prevent failures. By incorporating local processing, IoT systems can respond to real-time events faster and more effectively, leading to increased reliability and overall system performance.

6 CONCLUSION

The research presented in this study highlights the critical importance of both energy optimization and stability enhancement for IoT devices deployed in complex environments. As IoT ecosystems continue to expand and evolve, addressing these challenges will be crucial to ensuring the sustainability and reliability of IoT systems in real-world applications. The integration of advanced techniques such as low-power communication protocols, edge computing, and machine learning-based energy management offers promising solutions for minimizing energy consumption while maintaining high system performance. Additionally, the implementation of fault-tolerant mechanisms, resilient network architectures, and real-time monitoring allows IoT systems to remain operational even in the face of environmental uncertainties and hardware failures.

The proposed strategies for energy optimization and stability enhancement not only contribute to the longevity and efficiency of IoT devices but also pave the way for their widespread adoption in mission-critical applications such as smart cities, healthcare, and industrial automation. By combining energy efficiency with robust fault tolerance and adaptive control mechanisms, this research lays the foundation for the development of highly reliable, long-lasting, and resource-efficient IoT systems. Future research in this field should focus on further refining these strategies, integrating them into large-scale IoT networks, and exploring their practical deployment in various industrial and environmental contexts.

REFERENCES

[1] Yu S, Yanyi W, Gaoxiang J, et al. Deep learning-based power usage effectiveness optimization for IoT-enabled data center[J]. Peer-to-Peer Networking and Applications,2024,17(3):1702-1719.

[2] Yinghua T. Energy Consumption Optimization of an IoT Monitoring Center Based on a Max-Min Ant Colony Algorithm[J]. Wireless Communications and Mobile Computing,2023,2023

[3] Wang C W, Dwijendra A K N, Sayed T B, et al. Internet of Things Energy Consumption Optimization in Buildings: A Step toward Sustainability[J]. Sustainability,2023,15(8):

[4] Poh K L, Wei C C, Ling D T, et al. Optimizing Energy Consumption on Smart Home Task Scheduling using Particle Swarm Optimization[J]. Procedia Computer Science,2023,220195-201.

[5] Imran, Naeem I, Hyeun D K. IoT Task Management Mechanism Based on Predictive Optimization for Efficient Energy Consumption in Smart Residential Buildings[J]. Energy & Buildings,2022,257

[6] Ullah I, Fayaz M, Aman M, et al. An optimization scheme for IoT based smart greenhouse climate control with efficient energy consumption[J]. Computing,2021,104(2):1-25.

[7] Aladdin M, Muhannad A. Toward IoT fog computing-enabled system energy consumption modeling and optimization by adaptive TCP/IP protocol.[J]. Peer J. Computer science,2021,7e653-e653.

[8] Zhongyang W, Du X. Online optimization of intelligent reflecting surface-aided energy-efficient IoT-edge computing[J]. Future Generation Computer Systems,2023,141611-625.