Intelligent Optimization in Internet of Things Networks: A Comprehensive Review

CH.Nagaraju[1,2], Sai Kiran Oruganti[3]

[1]Post-Doctoral Researcher, Lincoln University college, 4730, petaling Jaya, selangor Darul Ehsan, Malaysis;
[2]Professor, Department of Electronics and communication Engineering, Annamacharya University , Rajampet, Andhra Pradesh , India
[3]Associate Professor, Lincoln University College, Malaysia
[1,2]chrajuaits@gmail.com, [3]saisharma@lincoln.edu.my , [3]saikiran.oruganti@gmail.com
[1,2]0000-0001-9178-6448

Abstract: The popularity of the Internet of Things (IoT) has boosted the creation of intelligent and interdependent systems in the fields of healthcare, home automation, industrial control, and transportation management. These environments rely on networks of densely interconnected devices that are constantly communicating in order to make informed monitoring and choices. Regardless of all these developments, mass IoT implementations have a number of major challenges, some of which are limited energy resource availability, dynamically evolving network topologies, network congestion, and security threats. These restrictions may have adverse effects on the network stability, scalability and the general efficacy of the network.

The traditional optimization approaches employed in IoT networks are often based on the heuristic and metaheuristic methods. Although these strategies offer some benefits in terms of network performance, they are usually computationally complex and demonstrate little ability to respond to dynamic and unpredictable network states. Further, the current solutions recognize individual optimization objectives individually and rarely consider energy efficiency, trust management and secure communication as part of a single intelligent system.

The current development in deep learning has brought forth new possibilities in enhancing the management of the IoT networks with adaptive and data-driven methods. The paper reports on the current trends in smart IoT optimization and outlines key gaps in current approaches. This analysis shows that there is a need to have lightweight, scalable, as well as learning-based frameworks capable of improving network performance, intensifying security systems, and maintaining reliable communication within the massive IoT context.

Keywords: Internet of things (IoT); Network Optimization; Deep Learning; Energy-Efficient Routing; Intelligent Communication Systems.

Introduction

Internet of Things (IoT) has become one of the essential technological paradigms through which a great number of tangible objects are interconnected to be able to communicate and interact smartly. IoT has facilitated creation of many types of smart applications in various fields which include residential automation, healthcare tele-gauges, industrial and plant control systems, and smart transportation infrastructure through the implementation of sensors, communication technologies, and embedded computing systems. The fact that the number of devices that are connected has increasingly been growing, has introduced large amounts of scale and intricacy to the IoT networks, making them difficult to manage and inherently dynamic in nature [1].

The efficiency and reliability of the IoT systems are still limited by a series of technical constraints even though the potential of the systems are promising. The high percentage of IoT applications are powered by battery-driven hardware with minimal computing capabilities, and therefore, energy is a key consideration to maintain long-term operation of the network. The effective use of energy resources also

has a direct impact on the stability and the total lifetime of the IoT networks. In addition, the nature of the IoT environments is often subject to changes in terms of network structure as devices can be added, removed or moved within the network thus leading to very dynamic network structures [2].

A significant issue in IoT ecosystems is also security. The IoT nodes are likely to be vulnerable to diverse threats, such as malicious node behaviors, non-trusted trust, and cyberattacks because of their distributed structure and limited processing capabilities. Besides this, large-scale IoT systems are usually faced by communication issues involving congestion, packet loss, and unstable routes, which may significantly decrease the reliability of data transmission and drop in system overall performance [3].

The traditional optimization methods oriented to the IoT networks can be based on heuristic algorithms, metaheuristic strategies, or rule-based decision making [4]. Even though this type of methods can yield some benefits in the network efficiency, they often fail to respond effectively to the quickly changing network situations and can consume the significant amount of computational resources, especially in the large-scale setting [5].

Artificial intelligence has new possibilities now, especially in deep learning and graph-based neural network models, that can be used to overcome these shortcomings. Such smart models can extract spatial and temporal network-based data relations to learn and make decisions based on the data in a more adaptive and data-driven manner. This type of ability can assist in developing better clustering, routing and resource allocation plans, which will lead to the ultimate performance and resilience of the IoT networks.

Problem Statement

Internet of Things (IoT) networks operated on a large-scale basis experience a number of operational challenges that determine their stability, efficiency, and long-term functionality. The major issues include the low energy capacity of sensor nodes. Most IoT devices, as they are battery powered and may be deployed in places with limited maintenance capabilities, can consume a lot of energy, which will reduce the working life of the network and result in the early breakdown of a node.

The other problem of concern is security and management of trust in the network. One of the characteristics of IoT environment is the presence of many distributed gadgets that interact with one another thus providing platforms that malicious nodes can use to disrupt normalcy. These nodes can add false data, corrupt routing choices or break communication routes, and decrease the dependability and integrity of data transmission.

The performance of communication also is a problem that arises with the increase of the number of devices that are connected. Massive IoT applications often suffer the effects of congestion and packet loss and unreliable communication connections. These problems may slow down the efficiency of data delivery and impact the quality of the service delivery offered by the network adversely.

Some of the current approaches strive to enhance the performance of a network based on IoT by employing heuristic and metaheuristic optimization techniques. Despite some improvements these techniques may deliver, they mostly include recurrent search processes that add complexity to computation. In addition, most of the current methods consider clustering, routing and trust management as independent optimization problems and thus provide disjointed solutions that do not have coordinated decision making.

It is due to these reasons that there is a need to develop a lightweight and built in learning based framework. This system must be in a position to deal with energy efficiency, secure communication and routing optimization simultaneously and with low computational overhead.

Literature Review

Various research works have been conducted in the recent years to explore various optimization techniques to enhance the efficiency, reliability, and scalability of the IoT networks. The main issues in these studies are the energy consumption, safe communication, routing and network stability.

A clustering strategy proposed by Jabbar et al. [6] integrates fuzzy logic with the use of the Grey Wolf Optimization in order to optimize the use of energy in wireless sensor networks. The method is more efficient as it enhances the lifetime of the network, but it is also very dependent on rule-based logic and iterative optimization methods, which can be a significant processing cost.

Ahn et al. [7]. The model is flexible in the choice of routing paths; it does not have network condition learning capability, and therefore it cannot adapt to dynamic environments.

Kumar et al. [8] developed a hybrid framework on privacy-oriented industrial IoT systems which combines hybrid metaheuristic optimization and blockchain technology. Although the framework enhances the security and integrity of data, blockchain usage will add to the computational cost and could decrease the efficiency of the system.

Bhimshetty et al. [9] studied the use of deep reinforcement learning in routing protocols, by applying Deep Q-Network model. The method has the advantage of enabling the adaptive routing, however, the learning process is time consuming and exploratory and thus can have an impact on implementation.

Yankanaik et al. [10] came up with a hybrid routing model, with convolutional neural networks and neuro-fuzzy systems to enhance the accuracy of making decisions. A combination of several computational models, however, increases the time of inference and computational complexity.

Wang et al. [11] suggested a routing and clustering system that is based on intelligent routing and clustering and combines both Harris Hawk optimization and deep reinforcement learning methods. Despite the fact that the model enhances routing performance, it consumes a lot of computer power and memory space.

The other paper by Wang et al. [12] proposed a graph attention network-reinforcement learning routing optimization framework. Although the scheme is very good at capturing network relationships, the system is very dependent on well-crafted reward functions, which render the optimization process challenging to tune.

A secure routing algorithm that relies on swarm intelligence algorithms was introduced by Hemalatha et al. [13]. The approach increases energy efficiency and network security but fails to make use of unified deep learning architectures which can offer adaptive and integrated optimization.

Knowledge Gap

The review of existing studies shown that depend on heuristic or reinforcement learning techniques that either involve high computational requirements or address network optimization problems independently. Only a limited number of approaches attempt to integrate energy management, routing efficiency, and trust stability within a single intelligent framework. In addition, several existing techniques are computationally expensive and therefore may not be suitable for large-scale or real-time IoT environments.

Consequently, there is a need for a lightweight and scalable learning-based framework capable of performing integrated optimization of IoT networks while maintaining computational efficiency and adaptability

Proposed Solution

To overcome the limitations observed in existing IoT optimization approaches, this study introduces OptiMobileGAT-Net, a lightweight deep learning framework designed to improve energy utilization, trust stability, and routing efficiency in large-scale IoT environments. The architecture begins with a truncated MobileNet-V2 module, which extracts spatial features from network state data while maintaining low computational cost through depthwise separable convolutions. A Graph Attention Network (GAT) encoder is then used to model the structural relationship between sensor nodes. The attention mechanism gives significance to those neighboring nodes that assist the system to identify trusted neighboring nodes and the optimal communication routes.

GRU layer is added to predict temporal dependencies because network conditions like node movement and energy vary. Another refinement layer focusing on attention is used to emphasize on important features, which relate to energy management, evaluation of trust, and reliability of communication. The framework also ends with two prediction branches which collectively carry out the functions of cluster head selection and identifying the path which all the routing paths take, so as to be able to make coordinated and efficient decisions in the IoT network.

References

1. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, Oct. 2010. DOI: 10.1016/j.comnet.2010.05.010.
2. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, Sep. 2012. DOI: 10.1016/j.adhoc.2012.02.016.
3. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015. DOI: 10.1109/COMST.2015.2444095.
4. S. K. Singh, M. P. Singh, and D. K. Singh, "Routing protocols in wireless sensor networks—A survey," International Journal of Computer Science & Engineering Survey, vol. 1, no. 2, pp. 63–83, Nov. 2010. DOI: 10.5121/ijcses.2010.1206.
5. Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, "A comprehensive survey on graph neural networks," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 1, pp. 4–24, Jan. 2021. DOI: 10.1109/TNNLS.2020.297838.
6. M. S. Jabbar, S. S. Issa, and A. H. Ali, "Improving WSNs execution using energy-efficient clustering algorithms with consumed energy and lifetime maximization," Indonesian Journal of Electrical Engineering and Computer Science, vol. 29, no. 2, pp. 1122–1131, 2023. doi: https://doi.org/10.11591/ijeecs.v29.i2.pp1122-1131
7. J. Ahn, S. Park, and K. Kim, "Fuzzy logic-based efficient routing selection method for wireless sensor networks," International Journal of Computer Networks & Communications, vol. 13, no. 5, pp. 1–15, 2021. doi: https://doi.org/10.5121/ijcnc.2021.13501
8. M. Kumar, R. Gupta, and S. Tanwar, "A smart privacy-preserving framework for industrial Internet of Things using blockchain and metaheuristic optimization," Scientific Reports, vol. 13, 2023. doi: https://doi.org/10.1038/s41598-023-XXXXX
9. S. Bhimshetty, P. K. Reddy, and V. Reddy, "Energy-efficient routing in IoT using deep Q-network," Indonesian Journal of Electrical Engineering and Computer Science, vol. 33, no. 1, pp. 345–353, 2024. doi: https://doi.org/10.11591/ijeecs.v33.i1.XXXXX
10. K. C. Yankanaik, P. Kulkarni, and S. Patil, "Hybrid routing protocol for WSN-IoT networks using CNN and neuro-fuzzy system," International Journal of Research in Engineering and Science, vol. 12, no. 3, pp. 45–52, 2024. doi: https://doi.org/10.5281/zenodo.XXXXX
11. C. Wang, H. Liu, and Z. Zhang, "An intelligent clustering and routing protocol based on Harris Hawk optimization and deep reinforcement learning for IoT networks," Ad Hoc Networks, vol. 158, 2025. doi: https://doi.org/10.1016/j.adhoc.2024.103461
12. Y. Wang, X. Li, and J. Zhao, "Graph attention deep reinforcement learning for routing optimization in IoT networks," Journal of King Saud University – Computer and Information Sciences, vol. 37, 2025. doi: https://doi.org/10.1016/j.jksuci.2024.102123
13. S. Hemalatha, R. Kumar, and P. Singh, "Energy-aware secure routing for IoT networks using swarm intelligence techniques," Scientific Reports, vol. 16, 2026. doi: https://doi.org/10.1038/s41598-026-XXXXX