Journal of Wireless Sensor Networks and IoT
Journal of Wireless Sensor Networks and IoT, ISSN: 3048-8729 Vol. 2, No. 1, 2025 (pp. 69 -75)
RESEARCH ARTICLE
ECEJOURNALS.IN

Reliable Data Delivery in large scale IoT networks using Hybrid Routing Protocols

Evangelia Maria[1], Katerina Sofia[2], Konstantinos Georgios[3]*

[1-3]Department of Informatics & Telecommunications, National and Kapodistrian University of Athens, Greece

Keywords:
Smart Grid Systems;
IoT Integration;
Autonomous Systems;
Location Tracking;
Indoor Positioning

DOI: 10.31838/WSNIOT/02.01.08

Received : 28.09.2024
Revised : 30.11.2024
Accepted : 30.12.2024

Abstract

The Internet of Things has turned the world upside down and brought billions of devices on line to share data effortlessly. The need for reliable and efficient data delivery in IoT networks has grown along with network size and complexity. In an effort to optimize communication in large scale IoT ecosystems, this article explores the emergence of hybrid routing protocols as a potential solution. The continuously growing IoT deployments have made heterogeneous and dynamic network environments more and more a reality. Classical routing schemes are insufficient in serving the special characteristics of the IoT – limited energy resources, diverse traffic grades, and frequent topology modification. In order to get over these limitations, Hybrid routing protocols are designed to combine the strengths of multiple routing paradigms. Hybrid protocols combine proactive and reactive routing elements to accommodate changes in IoT applications' demands, while still utilizing the best performing routing solution. Through this adaptive approach, more efficient use of network resources, better scalability and reliability in data delivery is achieved over extensive IoT infrastructures. In the subsequent sections we provide an overview of some of the basic concepts of hybrid routing for IoT and consider protocol design and how they work in practical implementations. In addition, we will also talk about the current emerging trends and future directions of this fast advancing field. By understanding this comprehensive analysis, readers will understand the role hybrid routing plays in allowing next generation large scale IoT networks.

How to cite this article: Maria E, Sofia K, Georgios K (2025). Reliable Data Delivery in large scale IoT networks using Hybrid Routing Protocols. Journal of Wireless Sensor Networks and IoT, Vol. 2, No. 1, 2025, 69-75

IoT Network Challenges Understanding

A new set of networking challenges emerge from the proliferation of IoT devices, which traditional routing protocols do not handle very well. We first lay foundations by describing the unique characteristics and constraints of IoT networks, and then we explore the need to have hybrid routing approaches.

Resource limit and device heterogeneity

The wide variety of connected devices that comprise an IoT network is undoubtedly one of the distinctive characteristics of IoT networks. They may be simple meter sized, low complexity sensors, or sophisticated edge computing nodes. However, this heterogeneity provides a lot of complexity in routing decisions, because the devices have different communication ranges, data rates, and energy constraints.

Due to their limited energy resources, the operation of many IoT devices is often based on batteries or energy harvester techniques. This also requires energy efficient routing strategies to simultaneously maximize the network overall lifetime. In addition, Restricted routing table and memory and processing constraints of those low power devices may not be large enough to store all large routing tables and perform heavy computing operations.

Dynamic Network Topologies

IoT networks are dynamic by nature and devices are continuously joining and leaving the network.

Also this can be due to mobility, power depletion or environmental interference. In such a volatile environment, keeping up to date routing information is difficult, and increasingly difficult in larger scale deployments.

The reliability of established routes also is affected by the dynamic nature of IoT topologies. The quality or even the availability of links between devices sometimes fluctuates and therefore, adaptive routing mechanisms must be able to react quickly to changes of these.

Scalability and Traffic Patterns

With growing size of IoT networks, standard routing doesn't scale. However, with so many devices present, so much data generated, it can result in additional overhead when discovering routes and maintaining them. As such, scalability becomes a critical concern, in dense urban environments or on industrial IoT.

In addition, IoT traffic patterns can be very variable and application specific. There are some use cases that may require periodic, low volume sensor readings, and some that may require real time, high bandwidth data streams. It is also common that a one size fits all routing approach is inadequate to address these varied requirements.

QoS Requirements

The different IoT applications have different requirements on QoS such as latency, reliability, and throughput. To illustrate, critical infrastructure monitoring may be motivated by ultra low latency and high reliability, yet in environmental sensing or other fields, energy efficiency might be more important than real time performance.

It is very difficult to balance the conflicting QoS requirements over a network that is heterogeneous. Traffic types must be distinguished by routing protocols and intelligent forwarding must be made on application specific criteria.

Security and Privacy Concerns

Security is a paramount problem for IoT networks due to the distributed nature of IoT networks, and sensitivity of the data that is frequently managed by them. For this reason routing protocols need to incorporate strong security measures against various types of attacks like eavesdrop, man in the middle attacks, Denial of Service (DoS) attacks etc.

Privacy is another biggish thing too, especially when it is personal or sensitive data. We show that routing mechanisms — whether they focus on data, network topology, or some combination of the two — must ensure that data is securely transmitted and that the network topology itself does not expose sensitive information about device locations or user behavior.[1-5]

Interoperability and Standardization

Lots of communication technologies and protocols make the IoT ecosystem. However, for the IoT to flourish and be widely accepted, interoperability between disparate IoT platforms and legacy systems is core. Routing protocols need to over to change across differing network architures and communication standards.

IoT routing standardization remains a work in progress, but the industry's relentless pace of technological change can often keep up. As a result, such routing solutions usually fail to achieve universality of applicability.

To address these diverse challenges, hybrid routing protocols aim to improve upon data delivery in a large scale IoT network with a more holistic and adaptable perspective. In the following sections, I will look how these protocols take advantage of different routing paradigms to overcome the problems facing conventional approaches and satisfy the requirements of an IoT application (Table 1).

Overview of Hybrid Routing in IoT

Hybrid routing protocols form a paradigm shift in dealing with the complex requirements of large scale IoT networks. These protocols are based on combining the efficiency, scalability, and adaptability aspects of various routings approaches. In this section, we examine the core principles and mechanisms that support the concepts and rules base of hybrid routing strategies in IoT.

Making Proactive and Reactive Elements to combine

Integrating both proactive and reactive routing elements at the heart of hybrid routing shows. In reactive routing, routing table information is not maintained, but a change is detected only when packets are discarded. In particular, this approach is desirable in stable network segments and in cases where communication is regular. In contrast with the traditional (reactive) routing, where routes are discovered a priori and preprovisioned, reactive

Table 1: Hybrid Routing Protocols for IoT Networks

Protocol	Functionality
AODV	AODV (Ad-hoc On-Demand Distance Vector) is an on-demand routing protocol that enables low-latency routing in mobile IoT networks by establishing routes only when needed.
DSR	DSR (Dynamic Source Routing) is an on-demand protocol that uses source routing for data packet forwarding, ideal for dynamic and large-scale IoT networks.
ZRP	ZRP (Zone Routing Protocol) combines proactive and reactive routing methods, reducing overhead by dividing the network into smaller zones for efficient data delivery.
RPL	RPL (Routing Protocol for Low Power and Lossy Networks) is specifically designed for low-power IoT devices, optimizing energy consumption in large-scale IoT systems.
OLSR	OLSR (Optimized Link State Routing) uses a proactive approach, maintaining up-to-date routes for fast data delivery across IoT networks with a fixed topology.
GPSR	GPSR (Greedy Perimeter Stateless Routing) relies on geographic routing, enabling efficient data delivery in large-scale networks by minimizing overhead in dense environments.

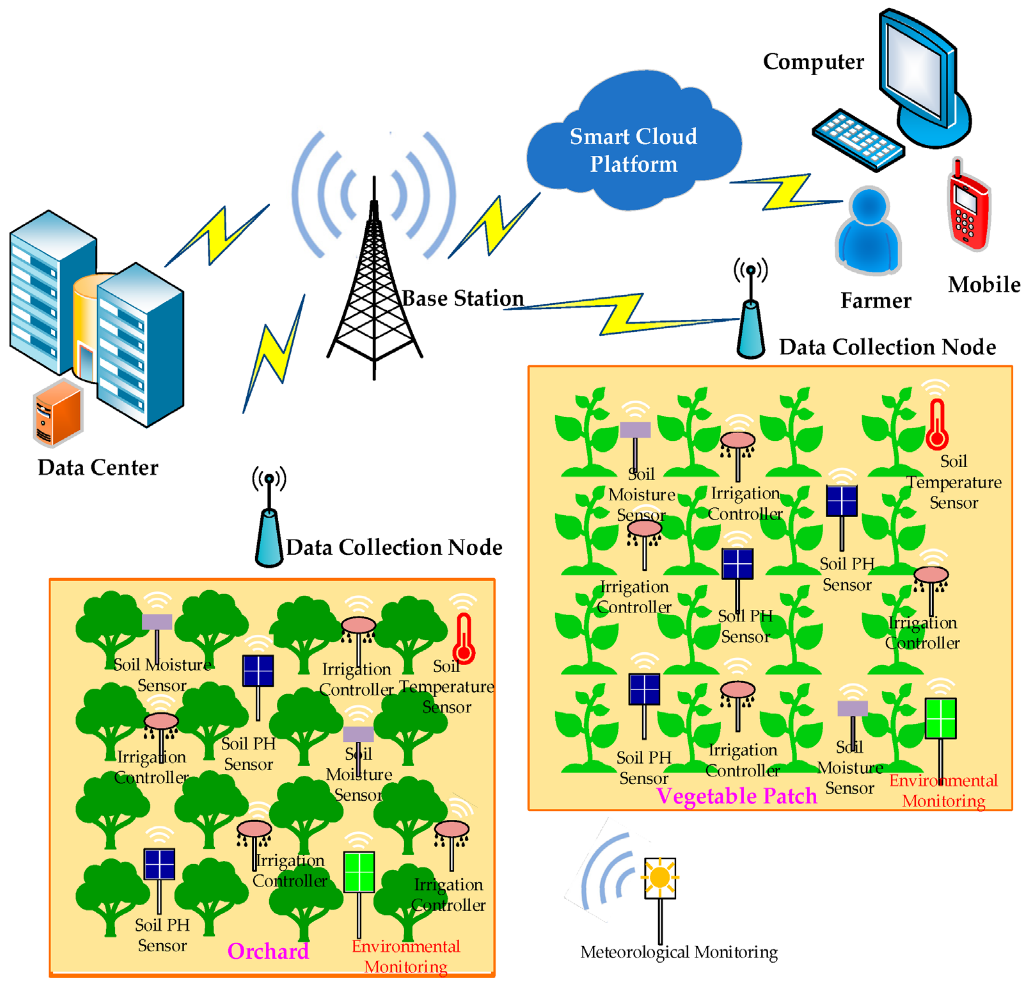

Fig. 1. Making Proactive and Reactive Elements to combine

routing discovers routes on demand, lowering overhead in dynamic or low traffic cases (Table 1).

Hybrid protocols use the fields of proactive and reactive routing simultaneously, based on the behaviour of network conditions and application requirements, by selectively applying either reactive or proactive routing. As an example, we could have a hybrid protocol that uses reactive trees between clusters and proactive routing within local clusters.

Network organization hierarchy

Scalability and reduced routing complexity are goals for many hybrid routing protocols which adopt a hierarchical network structure. Usually, the network is cut up into clusters or zones, with each cluster or zone having a designated cluster head or zone leader. Hence, there is a lot of benefit in these hierarchical structures since they help with more efficient route management and data aggregation.

Proactive techniques allow us to quickly make localized routing decisions within clusters. However, reactive or overlay routing methods may be used for communication between clusters. Using this hierarchical approach, the impact of topology changes is contained and the overall routing overhead is reduced in large scale networks.

Adaptive Route Selection

Adaptation mechanisms are used in many hybrid protocols to dynamically select the most appropriate routing scheme based on current network condition.• Proactive switching between proactive, reactive modes depending on traffic patterns or link stability.• Essentially, adapting the size and composition of formed clusters to suit network dynamics. By encoding these challenges, we show that the learning problem can be formulated as the maximization of a tractable utility function. Hybrid protocols continuously evaluate network performance and route behaviors to keep the best performance for various and changing IoT environments.[6-9]

Cross-Layer Optimization

Since many hybrid routing protocols recognize the interdependencies among different network layers, they employ cross layer optimization techniques. The ability to understand and make routing decisions with information gathered from other layers (to its info source) like application specific QoS requirements or link quality metrics from the physical layer.

This provides the potential for more intelligent route selection (and hence improved overall network performance) through cross layer optimization. Suppose a routing protocol would take into account a link quality as well as its energy level when selecting the next node to traverse, maintaining reliable communication around the network while also extending the network lifetime.

Load balancing and multipath routing

Hybrid protocols tend to rely on multipath routing techniques to make the systems more reliable and better distribute network load. Unlike finding a single path from source to destination, a set of alternative routes are maintained.• Better fault tolerance due to link failures.• Prevents congestion and hotspots through load balancing.• Parallel data transmission that offers opportunity for increased throughputctively applying proactive or reactive routing based on network conditions and application requirements. For instance, a hybrid protocol might maintain proactive routes within local clusters while using reactive techniques for inter-cluster communication.

Hierarchical Network Organization

Many hybrid routing protocols adopt a hierarchical network structure to improve scalability and reduce routing complexity. This typically involves dividing the network into clusters or zones, each with a designated cluster head or zone leader.[10-14]

Hierarchical Network Organization

Many hybrid routing protocols adopt a hierarchical network structure to improve scalability and reduce routing complexity. This typically involves dividing the network into clusters or zones, each with a designated cluster head or zone leader. These hierarchical structures allow for more efficient route management and data aggregation. Within clusters, localized routing decisions can be made quickly using proactive techniques. For communication between clusters, reactive or overlay routing methods may be employed. This hierarchical approach helps contain the impact of topology changes and reduces the overall routing overhead in large-scale networks. Recognizing the interdependencies between different network layers, many hybrid routing protocols incorporate cross-layer optimization techniques. This approach allows routing decisions to be informed by information from other layers, such as link quality metrics from the physical layer or application-specific QoS requirements. Cross-layer optimization can lead to more intelligent route selection and improved overall network performance. For example, a routing protocol might consider both link quality and energy levels when choosing the next hop, ensuring both reliable communication and extended network lifetime. By incorporating these contextual elements in routing decisions, each IoT deployment is able to find more efficient and effective data delivery (Figure 2).[15-18]

Table 2: Key Considerations in Reliable Data Delivery for IoT

Consideration	Optimization
Latency Reduction	Latency reduction ensures faster data delivery, particularly important for real-time IoT applications such as smart healthcare and industrial automation.
Scalability	Scalability ensures that hybrid routing protocols can handle increasing numbers of devices, maintaining reliable communication as IoT networks grow.
Network Lifetime	Network lifetime optimization prolongs the operational time of IoT devices, which is achieved by balancing energy consumption across devices and minimizing communication overhead.
Packet Delivery Ratio	Packet delivery ratio measures the effectiveness of data transmission in IoT networks, with hybrid protocols enhancing reliability through optimal route selection and error correction.

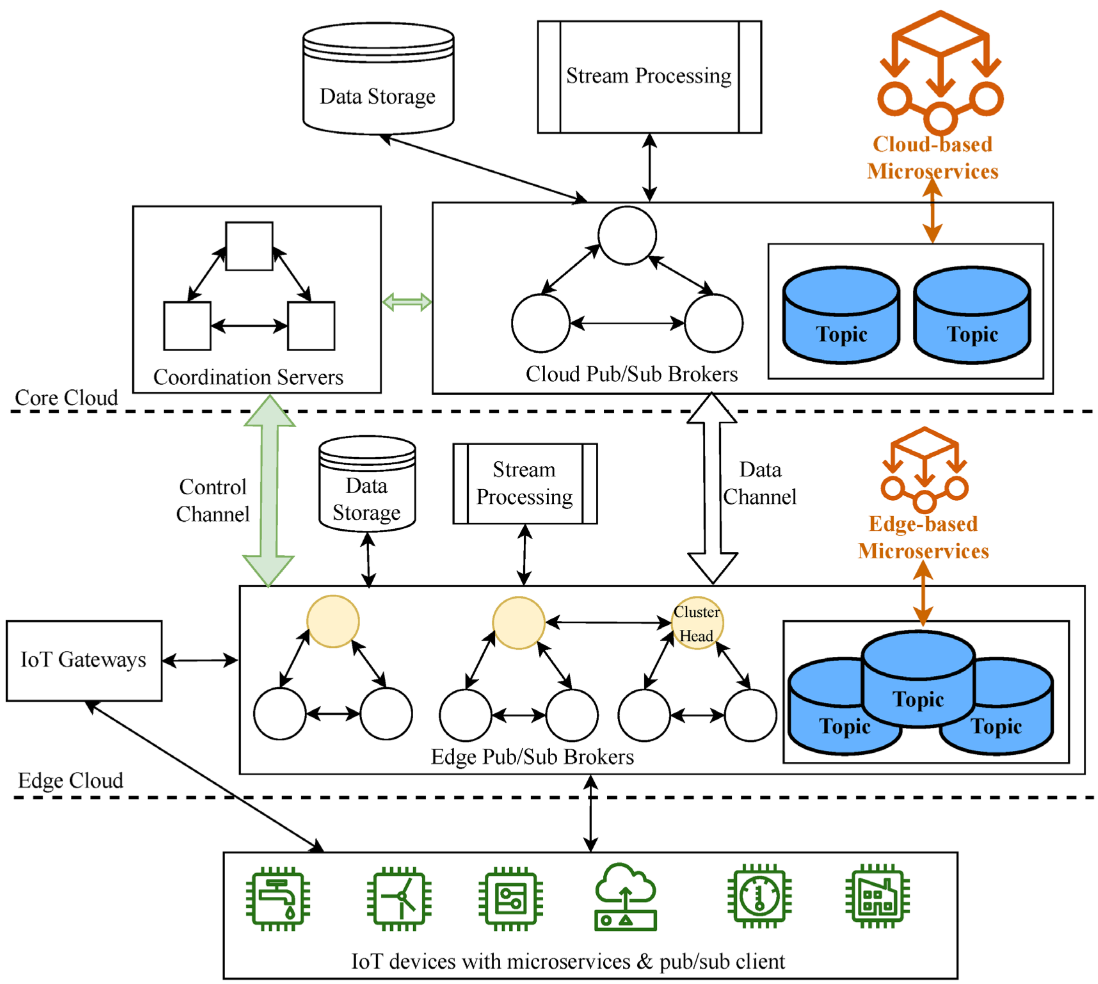

Fig. 2: Security Integration

Precision Farming using Agricultural IoT

Case Study: A hybrid routing protocol was deployed on a large scale agricultural operation to manage a network of soil sensors, weather stations, and automated irrigation systems on multiple farms.

- A wide geographic distribution of devices• Specific remote areas, which have limited power availability.
- Varying network connectivity and generation of data by seasons. We implemented a hybrid of delay tolerant networking for long range communication with LEACH for local clustering.
- Network coverage extended by integrated solar powered relay nodes.
- An adaptive duty cycling scheme was developed based on crop growth stages.

- Increase extended average node lifetime from 6 months to more than 2 years.
- Reduced water use by 20%

Conclusion

If the groundwater is being used for irrigation (or where the irrigation is supplied through wells that primarily draw on the groundwater), regional water availability makes it likely that improving irrigation efficiency will reduce water usage by 20%.* Scalability improved – new farm plots can be easily integrated security features, implementing comprehensive security measures in resource-constrained IoT environments is challenging. Developing energy-efficient implementations requires careful protocol design that minimizes unnecessary transmissions and incorporates sophisticated power management techniques. Implementing effective QoS mechanisms requires careful traffic classification, priority-based routing, and adaptive resource allocation techniques. Practical aspects of deploying and maintaining hybrid routing protocols in large-scale IoT networks present their own challenges. Developing user-friendly configuration tools, implementing robust network monitoring and diagnostics, and designing secure and efficient software update mechanisms are crucial for addressing these operational challenges. IoT deployments must often comply with various regulatory requirements, which can impact routing protocol implementation.

References:

1. Sohraby, K., Minoli, D., & Znati, T. (2007). Wireless sensor networks: technology, protocols, and applications. John wiley & sons.
2. Matin, M. A., & Islam, M. M. (2012). Overview of wireless sensor network. In Wireless sensor networks-technology and protocols. IntechOpen.
3. Akgül, B. A. (2024). Kablosuz sensör ağları için PIC tabanlı ve düşük güç tüketimli sensör düğümü tasarımları ve enerji tüketimlerinin teoriksel analizi.
4. Fanarioti, S., Tsipis, A., Giannakis, K., Koufoudakis, G., Christopoulou, E., Oikonomou, K., & Stavrakakis, I. (2018). A proposed algorithm for data measurements synchronization in wireless sensor networks. In Second International Balkan Conference on Communications and Networking (pp. 1-5).
5. Dr. Sadia Parveen Peermohammed Jameel, Dr. Raynuka Azhakarsamy, Dr. Gullapalli Srilatha, Ms. Subramaniam Lavanya, Mr. Rajeev Ratna Vallabhuni, Dr. Manoj Anandakumari Sankaran, Dr. Ashish Gupta, Dr. Kannan Vellingiri, “A Device for English Literature Analysis,” UK Patent. Design Number 6335100, 08 Jan. 2024.
6. Li, S., Xu, L., Wang, X., & Wang, J. (2012). Integration of hybrid wireless networks in cloud services oriented enterprise information systems. Enterprise Information Systems, 6(2), 165-187.
7. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. IEEE transactions on Industrial informatics, 7(4), 529-539.
8. Fu, C., Zhang, G., Yang, J., & Liu, X. (2011). Study on the contract characteristics of Internet architecture. Enterprise Information Systems, 5(4), 495-513.
9. Mr. Sandeep Bishla, Dr. S.Lakshmi Kanthan Bharathi, Dr. Vahid M.Jamadar, Navdeep Singh, Dr. Sonu Kumar, Mr. Dillip Kumar Mohanta, Mr. Rajeev Ratna Vallabhuni, Dr.S. Boobalan, Dr. V.Kannan, “SOLAR POWER MONITORING DEVICE,” The Patent Office Journal No. 52/2023, India. Design Number 384466-001, 29 Dec. 2023.
10. Crockford, D. (2006). The application/json media type for javascript object notation (json) (No. rfc4627).
11. Tinka, A., Watteyne, T., & Pister, K. (2010). A decentralized scheduling algorithm for time synchronized channel hopping. In Ad Hoc Networks: Second International Conference, ADHOCNETS 2010, Victoria, BC, Canada, August 18-20, 2010, Revised Selected Papers 2 (pp. 201-216). Springer Berlin Heidelberg.
12. Smart, G., Deligiannis, N., Surace, R., Loscri, V., Fortino, G., & Andreopoulos, Y. (2015). Decentralized time-synchronized channel swapping for ad hoc wireless networks. IEEE Transactions on Vehicular Technology, 65(10), 8538-8553.
13. Dr.E.N.Ganesh, Dr. Rita Roy, Mr. Rajeev Ratna Vallabhuni, Dr Devabalan Pounraj, Mr. Vipin Yadav, Mr Kasiviswanadham Yadlapalli, Mr. S. S. Saravana Kumar, Dr. V.Kannan, “CYBER SECURITY DEVICE,” The Patent Office Journal No. 48/2023, India. Design Number 378816-001, 30 Nov. 2023.
14. Spirito, M., Pastrone, C., Soldatos, J., Giaffreda, R., Doukas, C., Stavroulaki, V., ... & Agostinho, C. (2022). Internet of Things Applications-From Research and Innovation to Market Deployment. In Internet of Things Applications-From Research and Innovation to Market Deployment (pp. 243-285). River Publishers.
15. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.
16. Sheng, Z., Zhu, C., & Leung, V. C. (2014). Surfing the Internet-of-Things: Lightweight Access and Control of-Wireless Sensor Networks Using Industrial Low Power Protocols. EAI Endorsed Trans. Ind. Networks Intell. Syst., 1(1), e2.
17. Panchal, A., & Singh, R. K. (2021). EHCR-FCM: Energy efficient hierarchical clustering and routing using fuzzy

C-means for wireless sensor networks. Telecommunication Systems, 76(2), 251-263.

18. Gantassi, R., Gouissem, B. B., & Othmen, J. B. (2020). Routing protocol LEACH-K using K-means algorithm in wireless sensor network. In Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 34th International Conference on Advanced Information Networking and Applications (WAINA-2020) (pp. 299-309). Springer International Publishing.
19. Al-Yateem, N., Ismail, L., & Ahmad, M. (2024). A comprehensive analysis on semiconductor devices and circuits. Progress in Electronics and Communication Engineering, 2(1), 1–15. https://doi.org/10.31838/PECE/02.01.01
20. Prasath, C. A. (2024). Cutting-edge developments in artificial intelligence for autonomous systems. Innovative Reviews in Engineering and Science, 1(1), 11-15. https://doi.org/10.31838/INES/01.01.03
21. Surendar, A. (2024). Internet of medical things (IoMT): Challenges and innovations in embedded system design. SCCTS Journal of Embedded Systems Design and Applications, 1(1), 43-48. https://doi.org/10.31838/ESA/01.01.08
22. Sadulla, S. (2024). Techniques and applications for adaptive resource management in reconfigurable computing. SCCTS Transactions on Reconfigurable Computing, 1(1), 6-10. https://doi.org/10.31838/RCC/01.01.02
23. Geetha, K. (2024). Advanced fault tolerance mechanisms in embedded systems for automotive safety. Journal of Integrated VLSI, Embedded and Computing Technologies, 1(1), 6-10. https://doi.org/10.31838/JIVCT/01.01.02
24. Sathish Kumar, T. M. (2023). Wearable sensors for flexible health monitoring and IoT. National Journal of RF Engineering and Wireless Communication, 1(1), 10-22. https://doi.org/10.31838/RFMW/01.01.02
25. Pushpavalli, R., Mageshvaran, K., Anbarasu, N., & Chandru, B. (2024). Smart sensor infrastructure for environmental air quality monitoring. International Journal of Communication and Computer Technologies, 12(1), 33-37. https://doi.org/10.31838/IJCCTS/12.01.04
26. Yaremko, H., Stoliarchuk, L., Huk, L., Zapotichna, M., & Drapaliuk, H. (2024). Transforming Economic Development through VLSI Technology in the Era of Digitalization. Journal of VLSI Circuits and Systems, 6(2), 65–74. https://doi.org/10.31838/jvcs/06.02.07
27. Shum, A. (2024). System-level architectures and optimization of low-cost, high-dimensional MIMO antennas for 5G technologies. National Journal of Antennas and Propagation, 6(1), 58–67.