Indonesian Journal of Electrical Engineering and Computer Science
Vol. 43, No. 1, July 2026, pp. 335~344
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v43.i1.pp335-344

Insights on routing and scheduling approaches in the IoT from the perspective of energy, QoS, and security–a systematic review

Rajeshwari Kenchammana Hosakote Nanjappa Gowda[1], Manuvinakurike Narasimha Sastry Suma[2]
[1]Department of Electronics and Communication Engineering, Sir M. Visvesvaraya Institute of Technology, Bangalore, India
[2]Department of Electronics and Communication Engineering, B.M.S College of Engineering, Bangalore, India

Article Info

Article history:

Received Oct 9, 2024
Revised Jun 16, 2026
Accepted Jun 27, 2026

Keywords:

Communication scheduling
Energy efficiency
Internet of things
Medium access control
Quality of service
Secure routing

ABSTRACT

The internet of things (IoT) has been conceptualized to bring more efficient and seamless connectivity to a large number of low-power and low-cost embedded devices. In the context of IoT, limited radio resources create new challenges, such as collisions and access conflicts. Another challenge arises in dealing with energy constraints, as battery-powered IoT sensors have limited energy capacity in the sensing layer. Consequently, routing mechanisms play a fundamental role in dealing with route optimization and reliable data transmission problems in the transport layer, whereas broadcast and link scheduling are also considered as appealing solutions for fulfilling the energy efficiency, collision-free transmissions and latency requirements in the IoT. Also, security vulnerabilities are hard to identify in the IoT perception and transport layer due to its ad-hoc network topological factors. Thus, deploying efficient routing schemes in IoT demands effective collaborative solutions for cost-effective and secure route formation with energy-aware scheduling performance, which were not, explored much in the past. This investigation thereby analyses the strengths and limitations of existing efficient routing and scheduling solutions in IoT and extracts the critical findings which could provide quick survey to many researchers in this application area.

Corresponding Author:

Rajeshwari Kenchammana Hosakote Nanjappa Gowda
Department of Electronics and Communication Engineering, Sir M. Visvesvaraya Institute of Technology
International Airport Road, Hunasamaranahalli, Yelahanka, Bangalore, India
Email: rajeswari_ec@sirmvit.edu

1. INTRODUCTION

Wireless sensor networks (WSNs) are essential internet of things (IoT) technology [1]. For this reason, they continue to gain more popularity among the research communities. WSNs provide data collection and communication for IoT devices by connecting them to the internet via a gateway. As IoT applications spread across industries such as agriculture, healthcare, and transportation, they require more data transfer, increasing energy consumption and putting a strain on sensor nodes with limited capacity. The fast growth of connected devices, which is expected to exceed 40 billion by 2025, emphasizes the need for energy-efficient communication techniques that provide long lifespan and low latency [2]-[4]. IoT networks are often divided into four layers: perception, communication, support, and application, with low power wireless personal area networks (LoWPAN) playing an important role in energy management and reliable data transfer in low-power, lossy situations [5], [6].

Due to the complex networking environments, IoT-based sensor networks need these abilities, including extended service periods, wide coverage, self-organization, dynamic cooperation and efficient transmission capabilities [7]. However, unlike other wireless networks, IoT-based sensor networks demand solutions to prolong the network lifetime, which can be achieved through energy-efficient communication scheduling methods and efficient routing conventions. Researchers have also agreed that the root improvement in IoT communication can be started from the lower layers such as sensing or perception and data link layers [8]. Medium access control (MAC) based scheduling approaches have gained much attention from researchers to decrease the energy consumption in IoT devices and realize enhanced connectivity and increased capacity with significantly reduced delay. However, in the wireless communication environment of IoT, communication links could be unstable. Also, several factors, such as the breakdown of nodes due to an increased rate of power depletion or other factors, joining or leaving of the network nodes, location change of mobile IoT nodes, and wireless signal interference cause dynamic changes to the topology which brings new challenges to the allocation and optimization of network resources and restrict fairness in packet scheduling, latency, collision-free transmission, and effective bandwidth utilization [9]. Thereby, in traditional IoT scheduling, appropriate time-slot allocation has become a crucial challenge [10].

Scheduling communication in IoT's MAC layer is an NP-hard problem, with existing algorithms having to deal with difficulties like as changing network topology, traffic circumstances, and delays. They enhance energy efficiency and network longevity, but have low allocation efficiency, high energy consumption, and synchronization overhead. These algorithms also have issues with fairness, congestion, and packet loss, which reduce data delivery performance [11], [12]. Traditional routing methods have challenges in dense IoT contexts, such as poor route selection, excessive energy consumption, and security vulnerabilities, especially under the IPv6 and 6LoWPAN standards. Optimizing routing performance and guaranteeing reliable, secure data delivery in IoT networks remain significant problems [13]-[15].

Hence the statement of the problem considered in this proposed study is formulated as follows: “Performing a thorough systematic investigational study on popular scheduling and routing approaches in IoT and reviewing a potential research gap is quite challenging”.

The study explores the popular energy-aware routing and communication scheduling methods for delay-sensitive applications in IoT and finds their strength and limitations. Also, the methodology further identifies the loopholes in existing IoT routing protocols from energy optimization and security aspects. Finally, the identified issues in existing routing and scheduling conventions help showcase the significant research gap. In contribution, the study also provides precise detail on the strengths and weaknesses of various scheduling and routing methods in IoT; this brings insights into the research trends and the areas where improvement is needed. The organization of this manuscript is as follows: section 2 provides perspective on the proposed method towards carrying out the proposed review work. Section 3 further provides insight into popular routing and scheduling schemes in IoT, whereas section 4 discusses popular security techniques for low power networks IoT-LPN. Finally, section 5 provides a critical discussion of findings, which discusses the trend pattern of research publication and research gaps. Finally, the conclusion is drawn in section 6.

2. METHOD

The proposed study strategizes a methodology for performing a systematic review of literature where it emphasizes exploring the popular scheduling and routing strategies in IoT from the perspective of energy, delay and security indices. It also ensures concise discussion on adopting slot-based scheduling and popular energy-efficient and secure routing strategies. This serves as a primary motive for this research study, potentially influencing the collection of appropriate information (i.e., identification of most relevant technical literature) from the digital libraries. Figure 1 exhibits the block-based overview of the research methodology adopted in this presented review work.

The first process in the adopted research methodology involves exploring digital libraries to locate very recent scientific and technical journals related to routing and scheduling approaches in IoT. While exploring digital libraries, it has been observed that the Institute of Electrical and Electronics Engineers (IEEE) digital library and Multidisciplinary Digital Publishing Institute (MDPI) provide a massive number of articles on the intended research topic that are easily accessible to researchers. Further, a primary shortlisting is performed based on the keyword-based search. This method reviews the title and abstract while screening perspectives, helps decide whether the articles follow inclusion and exclusion criteria. This primary shortlisting process also eliminates the selection of repetitive publications in a very early stage. The selection of rich scientific journals has defined both inclusion and exclusion criteria. Here, the inclusion criteria consider the most recent (i.e., from 2017 till date) and relevant studies that have either talked about energy-efficient scheduling or routing strategies in IoT to improve the data reliability aspect, followed by exploring efficient and optimized secure routing approaches.

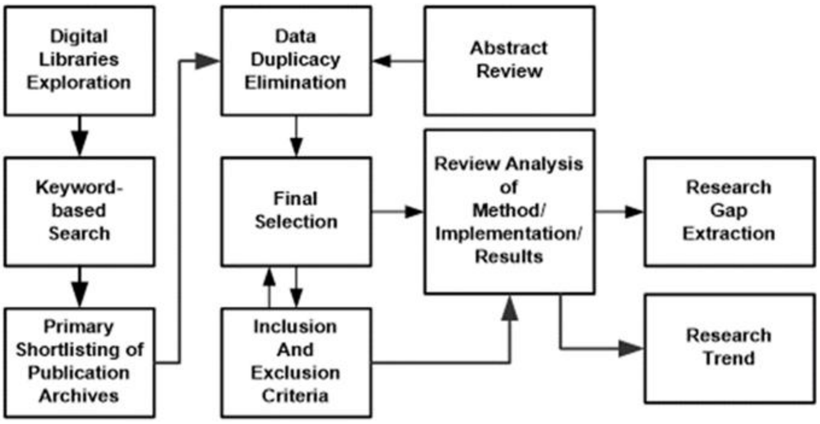

Figure 1. Research methodology adopted in proposed review work

Based on inclusion criteria, the methods and their implementations, along with the simulation parameters, are thoroughly reviewed, whereas exclusion criteria mostly discard the much older journals on IoT published before 2017 and do not discuss energy, delay, and security from implementation standpoints. It also excludes theory or conceptual journals and publications on hardware-based models. In this stage, this method eliminates replicated articles if it is found that the same author has written multiple journals published on different websites. Also, there could be a possibility where journals depict similar methodological implementation flow and hence discarded. This approach in the proposed research method performs the final selection of papers. Finally, based on the learning outcome, the research gap is formulated, reflecting the current research trend of popular methods and their strengths and weaknesses.

3. RESULT AND DISCUSSION

Table 1 presents highlights of effectiveness associated with existing studies. Jiang *et al.* [16] studied the potential aspects of joint link scheduling and routing methods for two-tier wireless backhaul networks. They aim to formulate the shortest time division multiple access (TDMA) link schedule that fulfills routers' traffic demand and optimizes IoT devices' energy consumption. A linear programming method is derived to formulate both routing and scheduling solutions, whereas a heuristic link scheduler, namely transmission set generation (TSG), has been proposed to handle the transmit power allocation problem in routers. The method also incorporates W-Dijkstra for optimal routing solution. The experimental outcome shows that the presented method achieves shorter schedules when compared with other link schedulers, and the method offers better energy management policies and also improves power allocation along with data transfer in IoT. However, the TSG algorithm is more complex, which restricts its employment in more dense IoT deployments. Also, W-Dijkstra poses longer routing time as the number of routers increases. Sah *et al.* [17] address the problem of time-bounded data delivery and explore efficient sensor sleep cycle management in the industrial internet of things (IIoT). They further propose a heuristic method that helps the backbone sensor node balance the incoming traffic for scheduling. The method explores TDMA-driven MAC and schedules the nodes for data forwarding within the allotted time slot corresponding to each time frame. The scheduling method, namely aggressive scheduling medium access control, offers an appropriate slot-management scheme for both owner nodes and needy nodes. The uniqueness of this method is that it outperforms TDMA for any given load. The study considers several evaluation criteria, including packet delivery rate, packet drop, energy consumption and time frame requirement for different numbers of sensor nodes.

Abdullah *et al.* [18] also worked in a similar line of research in IoT and attempted to enhance the lifetime of battery-powered sensor nodes, which positively influences the overall network lifetime. The study explores message scheduling in an IoT environment, employing group-based communication among IoT nodes where it enables a broker node in which the message scheduler operates and decides the priority of packets to be delivered to the sink. The presented algorithm follows cross-layer architecture at the application level and network level whereas the experimental outcome exhibits that the presented method outperforms LEACH concerning different energy metrics while stabilizing the response time of the messages. Chanak and Banerjee [19] identify the congestion problem during the data gathering process in IoT-enabled WSNs. As a result of congestion and missing packets, a decrease in reliability and throughput could occur, which degrades the communication performance in IoT. The study thereby introduces a distributed congestion control method that also incorporates a priority-based data routing strategy. The experimental outcome shows that it offers an improved lifetime, the average received packet ratio and hop-by-hop delay measures compared to the popular baseline strategies. Kim *et al.* [20] explore the IEEE 802.15.4 standard, popular for short-range, low-rate wireless communications in IoT. The authors identify the challenge in cross-layer design in IoT and realize the significance of efficient medium access control (MAC) and routing protocols to mitigate interference and improve reliability. Further, an energy-efficient cross-layer protocol for the MAC layer and routing layer, namely TSMR, is introduced to satisfy the requirements of IoT. The method enables scalable and reliable mesh networking in IEEE 802.15.4 standard, offering enhanced connectivity and reliable route formulation procedures. The experimental outcome shows that TSMR significantly reduces control overhead and end-to-end delay while improving network reliability.

Yang *et al.* [21] explored the problem of MAC scalability under variation of network traffic. The authors propose a machine learning (ML)-assisted MAC framework to address this issue. The experimental outcome shows stable throughput. However, the method lacks effectiveness due to high communication and computational overhead and also, ML models require offline training, which incurs higher costs. On the other hand, Kalita *et al.* [22] introduce the QoS-Aware MAC protocol to balance the QoS provisioning in M2M communications in IoT. The method offers superior throughput compared to the carrier sensing multiple access (CSMA) method and ensures fairness for low-priority applications. However, a prominent drawback of this approach is that it doesn't provide a relationship between a number of possible successful devices and available time slots. The presented method also doesn't offer energy optimization at MAC, restricting its applicability from energy-aware data transmissions. Shitiri *et al.* [23] introduced the orthogonal coded medium access control (OrMAC) method to deal with contention collisions and loss of delay-sensitive data. The method offers a better throughput and packet delivery ratio than DCQA but suffers from excessive delay and false prioritization of devices. This method also does not much emphasize energy optimization.

Bui *et al.* [24] introduce the free access distributed queue (FADQ) Method to reduce synchronization access issues in M2M communications. The method not only reduces access delay but also improves the access success probability. However, the method could suffer due to the possibility of a very long queue in large-scale IoT (LS-IoT) and pose more overheads due to sub-header inclusion. Nawaz *et al.* [25] address the problem of uniform grouping in RAW for 802.11ah. In this regard, the authors introduce a group-synchronized distributed coordinated method. The experimental analysis shows better throughput performance while suffering high delays for LS-IoT networks. Also, the study has not stressed on control frame overhead problem, which also affects the energy performance in IoT. Xu *et al.* [26] formulate a route optimization problem under TCAM capacity constraints and further demonstrate approximation algorithms with different complexities to handle this problem. The performance metrics exhibit better link utilization under limited TCAM capacity. However, the computational complexity associated with the global optimal strategy and node optimal strategy is found to be comparatively higher; also, no evaluation of energy metrics is found. Han *et al.* [12] also focuses on energy-saving and route optimization problems for underwater acoustic networks (UANs) and further introduce a connectivity and energy-aware layering routing (CELR) protocol. The protocol accomplishes better energy and QoS metrics when compared with depth-based routing (DBR) and layer-based and energy-efficient routing (LEER). However, the protocol performance based on multi-objective optimization has yet to be tested on mobile data sources environment of IoT.

In a similar direction, the authors Kaur *et al.* [14] introduced a DRL-based intelligent routing strategy, which comes under the category of cluster-based routing. The method does not ensure reliability and adequate collision control during packet scheduling. A self-organizing cognitive routing method, namely MRoute, is proposed by Ghosh *et al.* [27] to deal with dynamic network behavior in IoT. However, the algorithm poses higher complexity during path computation. Taghizadeh *et al.* [28] introduce the EM-RPL protocol, which suffers from delay constraints under heavy traffic. Also, another version of RPL, namely ARMOR, introduced by the authors Mohammadsalehi *et al.* [29] lacks energy optimization efficiency and cannot deal with delay constraints properly. The DDSLA-RPL protocol, introduced in the study by Homaei *et al.* [30] suffers from high control overhead when compared with the NCRM method. The authors Kim *et al.* [31] introduce the MobiRPL protocol, which ensures a better packet delivery ratio but has limitations due to improper routing decisions. Also, additional parameter tuning is required for better energy efficiency, which is not cost-effective. The improper routing decisions also lead to high delay constraints.

Han *et al.* [32] introduced a routing optimization method based on ant colony optimization (ACO). Here, the scheme aims to find the optimal routing path under both energy and delay constraints. The experimental results have demonstrated positive implications for the measures of shortest path selection, energy, and delay and throughput performance. However, the study doesn't cover the challenges, such as routing optimization under dynamic traffic conditions and does not retain a balance between energy consumption and data transmission reliability. Also, attention should be paid to data security in terms of data encryption and privacy protection. The authors (Deepa and Sridhar [33]) talk about the popularity and profitability of WSN routing conventions in IoT smart environments. It also talks about how the mobility of nodes in IoT significantly impacts network performance. The study introduces an IoT-assisted mobility-aware routing protocol (IoT-MARP) offering improved data routing strategy in Mobile Adhoc Networks (MANET) over IoT. The study outcome shows significant improvement over energy and QoS performance (e.g., latency, PDR, and throughput) with low communication overhead, but the focus on dynamic network traffic conditions and IoT sensing/perception layer and transport layer data security is missing [33]. In a similar line of research, the authors (Wang et al.) applied the grey wolf optimization method and fuzzy logic to enhance the routing performance in IoT. The data-oriented RPL algorithm reduces the chances of duplicate data transmission and optimizes energy and delay performance [34]. Similarly, the researchers in [35] and [36] introduced efficient and intelligent cluster-based routing schemes for IoT. However, these algorithms do not offer much scope for optimized secure routing.

Table 1. Summary of popular scheduling/routing-methods in internet of things

Reference	Problems	Mechanism	Advantage	Limitation
[16]	Effective communication scheduling	Transmission set generation, W-Dijkstra	Optimizes energy demands for IoT devices	Longer routing time in W-Dijkstra, complexity in TSG
[17]	Time-bounded data delivery	AS-MAC	Appropriate slot management for nodes	No implementation of energy-efficient routing protocol
[18]	Energy consumption	Message scheduling and joint routing	Extends network lifetime	No effective benchmarking
[19]	Congestion problem in IoT	Class-based congestion management method	Improved lifetime, delay, received packet ratio	High message complexity
[20]	Challenge in cross-layer design	Topological structure mesh routing (TSMR)	Improved energy performance, delay, reliability	Packet loss during the handover process, no effective benchmarking
[21]	MAC scalability under variation of network traffic	A scalable ML assisted MAC framework	Near stable throughput	High communication and computational overhead, offline training required
[22]	QoS provisioning	QoS-aware MAC	Best throughput over CSMA, fairness for low –priority applications	No relationship between no. of possible successful devices and no. of available time-slots
[23]	Elimination of contention collisions, loss of delay-sensitive data	Orthogonal coded medium access control (OrMAC)	Better throughput and packet delivery ratio than DCQA	Excessive delay, false prioritization of devices
[24]	Synchronization access issue	Free access distributed queue (FADQ)	Reduces access delay, improves access success probability	Possibility of very long queue, more overheads due to inclusion of sub-headers
[25]	Uniform Grouping in RAW for 802.11ah	Group-synchronized distributed coordinated method	Better throughput	High delays for LS-IoT networks
[26]	Route optimization problem under TCAM capacity constraints	Approximation algorithms with different complexity	Better link utilization, under limited TCAM capacity	High complexity in global optimal strategy and node optimal strategy
[12]	Energy-saving and reliable routing in UANs	connectivity-and-energy-aware layering routing (CELR) protocol	Superior packet delivery rate, energy consumption, end-to-end delay	No Multi-objective optimization evaluation on mobile, data sources environment
[14]	High communication delay, poor network lifetime in IoT	DRL-based Intelligent routing (cluster-based)	Enhanced network lifetime, reduced delay	No talk on reliability and collision control during scheduling
[29]	Dynamic network behavior in IoT	Self-organized cognitive routing method (MRoute)	Reduces latency, link reliability	High time complexity to compute path
[30]	Limitations in IPv6 routing protocol	EM-RPL	Outperforms RPL in terms of network lifetime and packet loss ratio	Delay constraints under heavy traffic
[31]	Mobility support in IPv6 routing protocol	ARMOR	Better packet delivery ratio, long lasting reliable path	Lack of energy optimization, delay constraints
[32]	Quality of routing services in IoT	DDSLA-RPL	Better energy fairness index, latency, lifetime and packet delivery rate	High control overhead compared to NCRM
[33]	Mobile routing issues in LLNs	MobiRPL	Better packet delivery ratio	Improper routing decisions, additional parameter tuning required for better energy efficiency, high delay

WSNs in IoT (WSN-IoT) consist of multiple embedded devices (sensors and actuators) with limited resources in which they connect via low-power and lossy manner. Thereby, due to low-power and lossy network characteristics and mobility of IoT devices, data security in IoT has also become crucial to ensure data delivery reliability under IoT-LPN. The proposed study further explores the strengths and limitations of IoT Routing strategies and also assesses their performance against different security threats.

3.1. Popular security tecniques in IoT

Hussain and Hanapi talk about the security vulnerabilities in WSNs in IoT (WSN-IoT) and how these networks are affected by threats such as sniffing, spoofing and intruders. The study also explored the RPL protocol's security features against routing assaults, which have not been addressed much in the past. It has been observed that RPL security features have been partially implemented in Contiki OS with the addition of preloaded secure mode (PSM) and optimal protection system. The authors confirm that RPL security features provide superior protection against neighbor attacks (NA) but need more optimization to reduce their impact on energy usage. The exploration also reveals that RPL Protocol Variants in IoT-LPN architecture yield latency and packet delivery rate (PDR) when subjected to selective forwarding (SF) and Black-hole attacks and are not strong enough against wormhole (WH) attacks [37].

Airehrour *et al.* [38] introduced a trust model in ContikiRPL that can defend both Rank and Sybil attacks. The technique employs a time-based trust-aware routing protocol that doesn’t consider the mobility of nodes and suffers from significant packet loss rate, high energy consumption and delay. Similarly, the authors in [39] also introduce a trust model for RPL to combat RPL attacks. This approach is found to be defensive only against Blackhole, Sybil and Rank attacks whereas the computing power performance could be improved. Another trust-based RPL protocol implementation can be found in the study of [40], which suffers from a significant packet loss rate, lack of mobility of devices and poses higher energy consumption and end-to-end delay.

However, this approach can also defend against only a few attacks, such as blackhole, and selective forwarding. Another trust-based security model is introduced in the study of [41], which enables recommendation evaluation via belief functions. However, this approach is found not suitable for IoT routing protocols. In the study from Ali *et al.* [42] machine learning-based scalable and lightweight security approach is introduced for IoT devices, which considers privacy issues related to behavior logs. However, this method is also unsuitable for IoT routing protocols. Sakthivel and Chandrasekaran [43], a fuzzy logic and dummy packet-based acknowledgement framework is introduced to resist different packet-dropping attacks in IoT. However, packet drops occur due to the mobility of devices, and network operations create high packet overhead and high energy consumption and, in this case, no RPL-specific attacks are considered. Shayesteh *et al.* [44] another security model is proposed considering Bayesian learning. This presented data trust model can identify the malicious behavior of nodes; however, this method does not consider dynamic mobile and heterogenous IoT environments and handling of trust dynamics. On the other hand, the security approach in the study of [45] introduces the JDICA technique to detect blackhole attacks. In this study, only PDR is evaluated, whereas no evaluation of energy, delay and RPL-specific attacks is found.

Djedjig *et al.* [46] also introduce a secure routing strategy for RPL, capable of resisting black hole and rank attack. The method is efficient regarding PDR and energy consumption but lacks consideration of IoT-LPN mobility factors. A lightweight cross-layer security approach is also introduced in the study of [47], which doesn’t much emphasize attack prevention and does not much emphasize RPL attacks. Nandhini and Vivekanandan [48], an energy-efficient and secure routing method is introduced to resist Greyhole attacks. However, the method is not superior against routing attacks. Thulasiraman and Wang [49] introduce a secure, lightweight, trust-based RPL protocol that can resist DoS and Sybil attacks but lacks consideration for blackhole and RPL-specific attacks. Similarly, Kiran *et al.* [50] do not address RPL attacks but identify routing misbehavior and packet-dropping attacks. It is also observed that the existing secure RPL routing conventions in IoT also suffer from certain loopholes in scheduling methods, causing unnecessary energy and resource burdens to delay-sensitive applications.

3.2. Critical disussion on findings

The study also provides a critical discussion of the findings after analyzing the recent literature on scheduling and routing approaches from energy, QoS, and security perspectives. It explores the statistics on research publications for popular problem domains in IoT, such as routing, scheduling, and security.

The findings are important to the audience because they illustrate fundamental issues and gaps in IoT routing, scheduling, and security, all of which are essential for improving energy economy, assuring dependable performance, and protecting data. Addressing these concerns can enhance IoT network design and application performance, especially in dynamic and resource-constrained contexts.

The search criteria consider the timeline from 2020 to 2024 to analyse the recent trend in publication in journals and articles from both IEEE and MDPI. Figure 2 presents discussion of the trends of research publication to showcase that the pattern of frequencies of papers related to routing problem, scheduling issues, and secure routing solution. Figure 2(a) shows that more publication is witnessed for scheduling while less for secure routing in IEEE digital library. Figure 2(b) shows that routing related publications are fairly more in number in contrast to scheduling and secure routing.

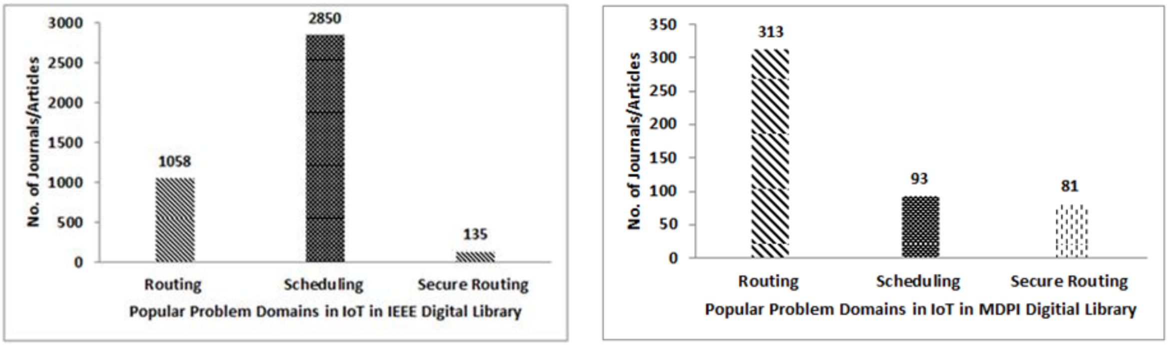

Figure 2. No. of journals/articles retrieved on popular problem domain in IoT (year: 2020-2024) (a) in IEEE xplore digital library and (b) in MDPI digital library

3.3. Research gap

The analysis of the M2M communication shows that in IoT, both non-critical and time-critical traffic can coexist. Also, the possibility of bursty and spontaneous traffic poses heterogeneity and induces networking complexities and challenges in sharing channel resources. The conventional standalone MAC protocols, such as CSMA and TDMA, cannot be directly applied to M2M networks as CSMA suffers from high collision rates and relatively high overhead. In contrast, TDMA suffers from low channel usage, scalability problems, and high traffic loads. The crucial findings of the study are as follows- i) it has been observed that majority of existing MAC-based scheduling approaches in IoT do not implement energy-efficient routing strategies (for example the case of AS-MAC), also ii) many of the scheduling approaches imposes communication and collision overhead with high message complexity and also lack proper benchmarking, iii) Very lesser emphasize has been given on devising joint scheduling and route optimization scheme to balance the trade-off between energy and QoS constraints in IoT, iv) Majority of the RPL routing protocols in IoT lacks effectiveness due to lack of energy consumption optimization , device mobility factors and delay constraints (e.g., EM-RPL and ARMOR), these protocols also poses high control overhead during dynamic traffic, v) The analysis on security protocols in IoT also reveals that majority of the security schemes are highly complex in nature and can able to resist very limited attacks, vi) Even though majority of the trust-based security schemes in IoT better packet delivery ratio but not much evaluation of energy, complexity and delay under RPL-specific attacks is found till date.

Future research can build on these findings by building integrated routing and scheduling solutions that optimize energy, QoS, and security at the same time. Key studies should include testing joint optimization methods in dynamic traffic situations, evaluating energy-efficient and safe protocols in real-world IoT systems, and investigating the efficacy of novel security mechanisms against RPL-specific attacks. The takeaway message is that efficient IoT network architecture necessitates integrated solutions that balance energy economy, QoS, and security while addressing current gaps to enhance performance in dynamic and resource-constrained contexts.

4. CONCLUSION

In this study, an investigational analysis of popular routing and scheduling approaches in IoT-LPN where the research has been narrowed down to the problems on energy, QoS and security metrics. It also offers the learning outcome while systematically exploring related work that adheres proposed research method. A significant research trend in publications and the research gap is also illustrated based on the review and analysis study, which directs future research work. It has also created opportunities for researchers to develop new solutions. In future lines of work, considerable effort should be given towards ensuring simplified, efficient and optimized data transmission modeling with energy-aware cluster-based routing schemes for IoT-LPN. Also, integration of efficient scheduling strategies with cluster-based routing and slot management could ensure collision-free transmission with shorter delay and optimized energy usage under variable network traffic. Finally, new efficient and lightweight security mechanisms are needed to ensure high data security against potential threats in IoT-LPN.

This study emphasizes the need for integrated routing and scheduling solutions in IoT that optimize energy, QoS, and security, building on previous research that has frequently overlooked these combined factors; future research should focus on joint optimization methods and real-world testing of energy-efficient and secure protocols, with the key takeaway being that addressing these challenges is critical for improving IoT network performance in dynamic environments.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Rajeshwari Kenchammana Hosakote Nanjappa Gowda	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Manuvinakurike Narasimha Sastry Suma		✓		✓		✓		✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] P. Phalaagae, A. M. Zungeru, B. Sigweni, and S. Rajalakshmi, “Authentication schemes in wireless internet of things sensor networks: a survey and comparison,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 33, no. 3, pp. 1876–1888, Mar. 2024, doi: 10.11591/ijeecs.v33.i3.pp1876-1888.

[2] Z. Li and A. Zhong, “Resource allocation in wireless powered virtualized sensor networks,” *IEEE Access*, vol. 8, pp. 40327–40336, 2020, doi: 10.1109/ACCESS.2020.2976476.

[3] O. Ali, M. K. Ishak, M. K. L. Bhatti, I. Khan, and K. Il Kim, “A comprehensive review of internet of things: technology stack, middlewares, and fog/edge computing interface,” *Sensors*, vol. 22, no. 3, p. 995, Jan. 2022, doi: 10.3390/s22030995.

[4] L. Xing, “Reliability in Internet of Things: Current Status and Future Perspectives,” *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6704–6721, Aug. 2020, doi: 10.1109/JIOT.2020.2993216.

[5] B. S. Awoyemi, A. S. Alfa, and B. T. Maharaj, “Network restoration in wireless sensor networks for next-generation applications,” *IEEE Sensors Journal*, vol. 19, no. 18, pp. 8352–8363, Sep. 2019, doi: 10.1109/JSEN.2019.2917998.

[6] H. Kharrufa, H. Al-Kashoash, and A. H. Kemp, “A Game Theoretic Optimization of RPL for mobile internet of things applications,” *IEEE Sensors Journal*, vol. 18, no. 6, pp. 2520–2530, Mar. 2018, doi: 10.1109/JSEN.2018.2794762.

[7] Z. Al Aghbari, A. M. Khedr, W. Osamy, I. Arif, and D. P. Agrawal, “Routing in wireless sensor networks using optimization techniques: a survey,” *Wireless Personal Communications*, vol. 111, no. 4, pp. 2407-2434, Apr. 2020, doi: 10.1007/s11277-019-06993-9.

[8] M. Kherbache, O. Sobirov, M. Maimour, E. Rondeau, and A. Benyahia, “Reinforcement learning TDMA-based MAC scheduling in the industrial internet of things: a survey,” *IFAC-PapersOnLine*, vol. 55, no. 8, pp. 83–88, 2022, doi: 10.1016/j.ifacol.2022.08.014.

[9] F. Amin, R. Abbasi, S. Khan, and M. A. Abid, "An overview of medium access control and radio duty cycling protocols for internet of things," *Electronics*, vol. 11, no. 23, p. 3873, Nov. 2022, doi: 10.3390/electronics11233873.

[10] Y. Li, X. Zhang, J. Zeng, Y. Wan, and F. Ma, "A distributed TDMA scheduling algorithm based on energy-topology factor in internet of things," *IEEE Access*, vol. 5, pp. 10757–10768, 2017, doi: 10.1109/ACCESS.2017.2710304.

[11] K. A. Darabkh, J. N. Zomot, Z. Al-qudah, and A. F. Khalifeh, "Impairments-aware time slot allocation model for energy-constrained multi-hop clustered IoT nodes considering TDMA and DSSS MAC protocols," *Journal of Industrial Information Integration*, vol. 25, p. 100243, Jan. 2022, doi: 10.1016/j.jii.2021.100243.

[12] D. Han, X. Du, and X. Liu, "CELR: Connectivity and energy aware layering routing protocol for UANs," *IEEE Sensors Journal*, vol. 21, no. 5, pp. 7046–7057, Mar. 2021, doi: 10.1109/JSEN.2020.3039808.

[13] C. M. Kim, S. K. Lim, J. D. Jeong, Y. Choi, and S. J. Koh, "6LoWPAN over optical wireless communications for IPv6 transport in internet of things networks," *IEEE Wireless Communications Letters*, vol. 11, no. 6, pp. 1142–1145, Jun. 2022, doi: 10.1109/LWC.2022.3159257.

[14] G. Kaur, P. Chanak, and M. Bhattacharya, "Energy-efficient intelligent routing scheme for IoT-enabled WSNs," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11440–11449, Jul. 2021, doi: 10.1109/JIOT.2021.3051768.

[15] S. M. Muzammal, R. K. Murugesan, and N. Z. Jhanjhi, "A comprehensive review on secure routing in internet of things: mitigation methods and trust-based approaches," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4186–4210, Mar. 2021, doi: 10.1109/JIOT.2020.3031162.

[16] M. Jiang, K. W. Chin, T. He, S. Soh, and L. Wang, "Joint link scheduling and routing in two-tier RF-energy-harvesting IoT networks," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 800–812, Jan. 2022, doi: 10.1109/JIOT.2021.3085862.

[17] D. K. Sah, T. N. Nguyen, K. Cengiz, B. Dumba, and V. Kumar, "Load-balance scheduling for intelligent sensors deployment in industrial internet of things," *Cluster Computing*, vol. 25, no. 3, pp. 1715–1727, Jun. 2022, doi: 10.1007/s10586-021-03316-1.

[18] S. Abdullah, M. N. Asghar, M. Ashraf, and N. Abbas, "An energy-efficient message scheduling algorithm with joint routing mechanism at network layer in internet of things environment," *Wireless Personal Communications*, vol. 111, no. 3, pp. 1821–1835, Apr. 2020, doi: 10.1007/s11277-019-06959-x.

[19] P. Chanak and I. Banerjee, "Congestion free routing mechanism for IoT-enabled wireless sensor networks for smart healthcare applications," *IEEE Transactions on Consumer Electronics*, vol. 66, no. 3, pp. 223–232, Aug. 2020, doi: 10.1109/TCE.2020.2987433.

[20] J. W. Kim, J. Kim, and J. Lee, "Cross-layer MAC/routing protocol for reliability improvement of the internet of things," *Sensors*, vol. 22, no. 23, p. 9429, Dec. 2022, doi: 10.3390/s22239429.

[21] B. Yang, X. Cao, and L. Qian, "A scalable MAC framework for internet of things assisted by machine learning," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, IEEE, Aug. 2018, pp. 1–5. doi: 10.1109/VTCFall.2018.8690737.

[22] A. Kalita, N. Ahmed, H. Rahman, and M. I. Hussain, "A QoS-aware MAC protocol for large-scale networks in Internet of Things," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, IEEE, Dec. 2018, pp. 1–6. doi: 10.1109/ANTS.2017.8384132.

[23] E. Shitiri, I. S. Park, and H. S. Cho, "OrMAC: A hybrid MAC protocol using orthogonal codes for channel access in M2M networks," *Sensors*, vol. 17, no. 9, p. 2138, Sep. 2017, doi: 10.3390/s17092138.

[24] A. T. H. Bui, C. T. Nguyen, T. C. Thang, and A. T. Pham, "Free access distributed queue protocol for massive cellular-based M2M communications with bursty traffic," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, IEEE, Aug. 2018, pp. 1–5. doi: 10.1109/VTCFall.2018.8690880.

[25] N. Nawaz, M. Hafeez, S. A. R. Zaidi, D. C. McLernon, and M. Ghogho, "Throughput enhancement of restricted access window for uniform grouping scheme in IEEE 802.11ah," in *2017 IEEE international conference on communications (ICC)*, IEEE, May 2017, pp. 1–7. doi: 10.1109/ICC.2017.7996899.

[26] S. Xu, G. Yang, J. Ren, S. Wang, and X. Wang, "Routing optimization for cloud services in SDN-based Internet of Things with TCAM capacity constraint," *Journal of Communications and Networks*, vol. 22, no. 2, pp. 145–158, Apr. 2020, doi: 10.1109/JCN.2020.000006.

[27] S. Ghosh, T. Dagiuklas, M. Iqbal, and X. Wang, "A cognitive routing framework for reliable communication in IoT for industry 5.0," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5446–5457, Aug. 2022, doi: 10.1109/TII.2022.3141403.

[28] S. Taghizadeh, H. Elbiaze, and H. Bobarshad, "EM-RPL: enhanced RPL for multigateway internet-of-things environments," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8474–8487, May 2021, doi: 10.1109/JIOT.2020.3047079.

[29] A. Mohammadsalehi, B. Safaei, A. M. H. Monazzah, L. Bauer, J. Henkel, and A. Ejlali, "ARMOR: a reliable and mobility-aware RPL for mobile internet of things infrastructures," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 1503–1516, Jan. 2022, doi: 10.1109/JIOT.2021.3088346.

[30] M. H. Homaei, S. S. Band, A. Pescape, and A. Mosavi, "DDSLA-RPL: dynamic decision system based on learning automata in the RPL protocol for achieving QoS," *IEEE Access*, vol. 9, pp. 63131–63148, 2021, doi: 10.1109/ACCESS.2021.3075378.

[31] H. Kim, H.-S. Kim, and S. Bahk, "MobiRPL: Adaptive, robust, and RSSI-based mobile routing in low power and lossy networks," *Journal of Communications and Networks*, vol. 24, no. 3, pp. 365–383, Jun. 2022, doi: 10.23919/JCN.2022.000004.

[32] H. Han, J. Tang, and Z. Jing, "Wireless sensor network routing optimization based on improved ant colony algorithm in the Internet of Things," *Heliyon*, vol. 10, no. 1, p. e23577, Jan. 2024, doi: 10.1016/j.heliyon.2023.e23577.

[33] S. Deepa and K. P. Sridhar, "Design of routing protocol with the internet of things devices over mobile ad hoc networks," *Signal, Image and Video Processing*, vol. 17, no. 8, pp. 4513–4522, Nov. 2023, doi: 10.1007/s11760-023-02685-x.

[34] Z. Wang, Z. Jin, Z. Yang, W. Zhao, and M. Trik, "Increasing efficiency for routing in internet of things using binary gray wolf optimization and fuzzy logic," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 9, p. 101732, Oct. 2023, doi: 10.1016/j.jksuci.2023.101732.

[35] W. K. Ghamry and S. Shukry, "Multi-objective intelligent clustering routing schema for internet of things enabled wireless sensor networks using deep reinforcement learning," *Cluster Computing*, vol. 27, no. 4, pp. 4941–4961, Jul. 2024, doi: 10.1007/s10586-023-04218-0.

[36] H. Wang, K. Liu, C. Wang, and H. Hu, "Energy-efficient, cluster-based routing protocol for wireless sensor networks using fuzzy logic and quantum annealing algorithm," *Sensors*, vol. 24, no. 13, p. 4105, Jun. 2024, doi: 10.3390/s24134105.

[37] M. Z. Hussain and Z. M. Hanapi, "Efficient secure routing mechanisms for the low-powered IoT network: a literature review," *Electronics*, vol. 12, no. 3, p. 482, Jan. 2023, doi: 10.3390/electronics12030482.

[38] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: a secure trust-aware RPL routing protocol for Internet of Things," *Future Generation Computer Systems*, vol. 93, pp. 860–876, Apr. 2019, doi: 10.1016/j.future.2018.03.021.

[39] S. Y. Hashemi and F. Shams Aliee, "Dynamic and comprehensive trust model for IoT and its integration into RPL," *Journal of Supercomputing*, vol. 75, no. 7, pp. 3555–3584, Jul. 2019, doi: 10.1007/s11227-018-2700-3.

[40] D. Airehrour, J. Guttierrez, and S. K. Ray, “A trust-based defence scheme for mitigating blackhole and selective forwarding attacks in the RPL routing protocol,” *Journal of Telecommunications and the Digital Economy*, vol. 6, no. 1, pp. 41–59, Mar. 2018, doi: 10.18080/jtde.v6n1.138.

[41] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, A. MacDermott, and X. Wang, “CTRUST: A dynamic trust model for collaborative applications in the internet of things,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5432–5445, Jun. 2019, doi: 10.1109/JIOT.2019.2902022.

[42] T. Ali, M. Nauman, and S. Jan, “Trust in IoT: dynamic remote attestation through efficient behavior capture,” *Cluster Computing*, vol. 21, no. 1, pp. 409–421, Mar. 2018, doi: 10.1007/s10586-017-0877-5.

[43] T. Sakthivel and R. M. Chandrasekaran, “A dummy packet-based hybrid security framework for mitigating routing misbehavior in multi-hop wireless networks,” *Wireless Personal Communications*, vol. 101, no. 3, pp. 1581–1618, Aug. 2018, doi: 10.1007/s11277-018-5778-2.

[44] B. Shayesteh, V. Hakami, and A. Akbari, “A trust management scheme for IoT-enabled environmental health/accessibility monitoring services,” *International Journal of Information Security*, vol. 19, no. 1, pp. 93–110, Feb. 2020, doi: 10.1007/s10207-019-00446-x.

[45] A. J. C. Sunder and A. Shanmugam, “Jensen–shannon divergence based independent component analysis to detect and prevent black hole attacks in healthcare WSN,” *Wireless Personal Communications*, vol. 107, no. 4, pp. 1607–1623, Aug. 2019, doi: 10.1007/s11277-019-06347-5.

[46] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “Trust-aware and cooperative routing protocol for IoT security,” *Journal of Information Security and Applications*, vol. 52, p. 102467, Jun. 2020, doi: 10.1016/j.jisa.2020.102467.

[47] S. B. Thigale, R. K. Pandey, P. R. Gadekar, V. A. Dhotre, and A. A. Junnarkar, “Lightweight novel trust based framework for IoT enabled wireless network communications,” *Periodicals of Engineering and Natural Sciences*, vol. 7, no. 3, pp. 1126–1137, Aug. 2019, doi: 10.21533/pen.v7i3.624.

[48] A. S. Nandhini and P. Vivekanandan, “A novel security and energy efficient data aggregation for medical internet of things using trust,” *Journal of Medical Imaging and Health Informatics*, vol. 10, no. 1, pp. 249–255, Jan. 2019, doi: 10.1166/jmihi.2020.2851.

[49] P. Thulasiraman and Y. Wang, “A lightweight trust-based security architecture for RPL in mobile IoT networks,” in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, Jan. 2019, pp. 1–6. doi: 10.1109/CCNC.2019.8651846.

[50] V. Kiran, S. Rani, and P. Singh, “Towards a light weight routing security in IoT using non-cooperative game models and dempster–shaffer theory,” *Wireless Personal Communications*, vol. 110, no. 4, pp. 1729–1749, Feb. 2020, doi: 10.1007/s11277-019-06809-w.

BIOGRAPHIES OF AUTHORS

Rajeswari Kenchammana Hosakote Nanjappa Gowda received B.E degree in electronics and communication engineering from Bangalore University. And M.Tech. in electronics under Visvesvaraya Technological University India. Currently working as an assistant professor in the department of electronics and communication engineering at Sir MVIT, Bengaluru. She is having teaching experience of 13 years and Industry experience of 12 years. Her area of research interest is network security, wireless sensor network, IoT, and wireless communication. She can be contacted at email: rajeswari_ec@sirmvit.edu.

Dr. Manuvinakurike Narasimha Sastry Suma currently working as professor in the department of electronics and communication engineering, B.M.S College of Engineering, Bangalore, Karnataka, India. She has 26 years of teaching experience and 2 and half years of industrial experience. Has published over 38 papers in peer reviewed journal/conferences. She is reviewer of many journals and conferences. Area of research interests are wireless communications, communications signal processing, machine learning. She can be contacted at email: suma.ece@bmsce.ac.in.