ISSN 1840-4855
e-ISSN 2233-0046

Original scientific article
http://dx.doi.org/10.70102/afts.2025.1833.001

A NOVEL FRAMEWORK FOR ENHANCING DATA COLLECTION MACRO- STRATEGIES IN HETEROGENEOUS IOT NETWORKS USING ADVANCED MATHEMATICAL MODELING

Abdolrashid Rezvani[1], Abbas Mirzaei[2*], Nasser Mikaeilvand[3*], Babak Nouri-Moghaddam[4], Sajjad Jahanbakhsh Gudakahriz[5]

[1]Department of Computer, Faculty of Engineering, Qeshm International Branch, Islamic Azad University, Qeshm, Iran. e-mail: rezvaniphd95@gmail.com, orcid: https://orcid.org/0009-0006-2685-6466
[2]Department of Computer Engineering, Ard.C., Islamic Azad University, Ardabil, Iran. e-mail: a.mirzaei@iau.ac.ir, orcid: https://orcid.org/0000-0002-4476-2512*
[3]Department of Computer Science and Mathematics, CT.C., Islamic Azad University, Tehran, Iran. e-mail: nasser.mikaeilvand@iau.ac.ir, orcid: https://orcid.org/0000-0003-1240-1306*
[4]Department of Computer Engineering, Ard.C., Islamic Azad University, Ardabil, Iran. e-mail: babaknouriit85@gmail.com, orcid: https://orcid.org/0000-0001-5363-9949
[5]Department of Computer Engineering, Germi.C., Islamic Azad University, Germi, Iran. email: sa.jahanbakhsh84@gmail.com, orcid: https://orcid.org/0000-0001-9397-723X

Received: March 15, 2025; Revised: July 24, 2025; Accepted: August 19, 2025; Published: September 10, 2025

SUMMARY

The explosive growth of Internet of Things (IoT) devices has generated considerable data in diverse networks. This poses serious challenges in collecting timely information and managing frequency resources optimally. In particular, unauthorized access, measurement constraints, and variable channel conditions cause interference, performance degradation, and security compromise, especially in distributed IoT systems. This research presents a comprehensive system for improving data collection in heterogeneous IoT networks. Using complex mathematical models and machine learning algorithms, the system aims to increase the efficiency of frequency resource utilization and reduce interference in network access. A Q-based reinforcement learning method is designed along with an intelligent MAC protocol. Simulation results show that this method increases channel utilization efficiency by 25%, reduces interference probability by 30% compared to traditional methods such as ALOHA, and provides a flexible and scalable solution for frequency resource management. The performance of the proposed system is significantly better than traditional methods, increasing channel utilization efficiency by 25% and reducing the probability of interference by 30%. The system's self-learning capability enables effective frequency resource management even in complex and dense environments. This research presents an innovative method for data collection in IoT networks that combines machine learning and mathematical modeling, providing a secure and scalable solution for the next generation of heterogeneous networks. This system paves the way for designing more stable and efficient networks in various fields, including smart cities and industries.

Key words: *internet of things (iot), heterogeneous networks, data collection, q-learning, mathematical modeling, spectrum access.*

INTRODUCTION

The Internet of Things (IoT) has revolutionized data collection by enabling the connectivity of devices, supporting applications ranging from geological hazard prevention and environmental monitoring to smart agriculture and urban services [1, 29, 3, 7]. Heterogeneous IoT networks, composed of devices with different computational capabilities, energy constraints, and communication protocols, are essential for these ecosystems, enabling real-time data collection in dynamic and geographically dispersed environments [1, 3, 30]. The importance of these networks lies in their ability to provide timely and actionable information, whether for mitigating secondary geological hazards through prioritized sensor data [1], optimizing urban IoT data flows [29][18], monitoring remote ecosystems through satellite links [3], or improving crop management through precision agriculture [7][14]. As IoT deployments continue to expand, efficient data collection strategies are critical to fully exploit the potential of these heterogeneous systems for analytics, decision-making, and service improvement.

Recent advances in IoT data collection demonstrate the convergence of innovative technologies tailored to different operational contexts. Uncrewed aerial vehicles (UAVs) have emerged as versatile mobile collectors, leveraging their adaptability to prioritize critical data in ground-based hazard scenarios [1] and partnering with intelligent, reflective surfaces (IRS) to overcome urban signal obstruction [29][12]. In remote areas lacking terrestrial infrastructure, low-Earth orbit (LEO) satellites provide global connectivity and low-latency transmission, addressing environmental monitoring needs [3]. At the ground level, wireless sensor networks (WSNs) use mobile sinks (MSs) and adaptive sampling techniques to optimize low-power data collection in edge-based IoT systems [5, 31]. Privacy-preserving mechanisms, such as local differential privacy (LDP) designed for key-value data, enhance security for sensitive IoT applications [30], while IoT platforms that integrate agricultural data enable sustainable resource management, as demonstrated in tomato cultivation under different irrigation regimes [7]. These trends are consistent with the evolution of wireless technologies (e.g., 5G, 6G, LoRaWAN) and emphasize scalability, efficiency, and flexibility in data collection [29, 7].

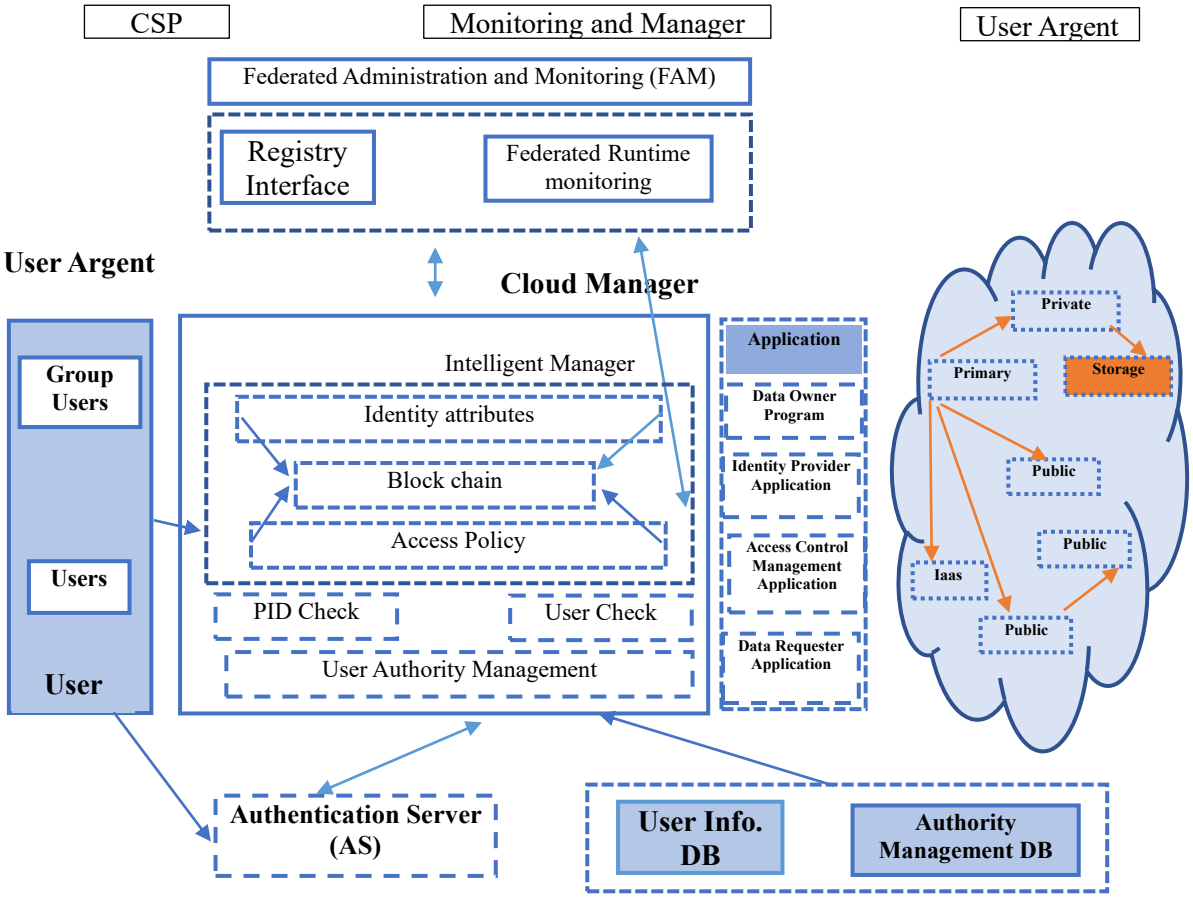

Figure 1. Heterogeneous IoT devices environment [32]

Figure 1 illustrates the heterogeneous IoT devices environment, depicting a diverse ecosystem of interconnected sensors, cluster heads, and communication protocols operating within a dynamic network topology. This schematic highlights the complexity of data collection in heterogeneous IoT networks, where devices with varying computational capabilities and energy constraints—such as low-power sensors and mobile sinks—interact across mesh and star architectures. The figure underscores the need for advanced mathematical modeling, such as the Q-learning-based framework proposed in this study, to optimize multi-channel access and resource allocation, ensuring efficient data flow amidst environmental uncertainties and device diversity.

The pervasiveness of the Internet of Things (IoT) is reported by many studies. Beyond all anticipations, loT continues to argument lives and improve the standards of living for many people. The benefits associated with linking sensor data or networking between sensors is extensively applied in many fields, including environmental monitoring, disaster management human motions, health, smart cities, and understanding social phenomena [9], to mention a few. For scientific communities, and the provision of services for data-intensive research, loT makes it possible to access large number of heterogeneous sensors that provide a variety of datasets. However, uncertain factors and other services in the environment may affect the service severely, resulting in users' low satisfaction [33].

Despite these innovations, heterogeneous IoT networks face substantial challenges. Scalability is a persistent issue as device numbers and coverage areas expand, complicating coordination across multi-tier architectures [1, 29, 3, 31]. Energy efficiency remains a critical constraint, with IoTDs, UAVs, and WSNs limited by battery life, necessitating optimized sampling and transmission strategies to extend network longevity [1, 29, 3, 5, 31]. Security and privacy are equally pressing, as sensitive data—whether key-value pairs from IoT devices [30] or environmental readings transmitted via satellites [3]—must be protected against vulnerabilities in exposed, dynamic environments. Furthermore, operational uncertainties, such as transmission rate fluctuations caused by environmental factors [3], variable signal dynamics in urban environments [29], or changing product conditions [7], require adaptive and robust solutions that traditional approaches often fail to address [1, 3, 5] adequately. These challenges highlight the need for advanced mathematical modeling, such as reinforcement learning [1, 29], cross-entropy optimization [3], or machine learning-based sampling [5], to design macro strategies that increase the efficiency, usefulness, and sustainability of data collection in heterogeneous IoT networks[8][10][6].

Problem Statement

Although Internet of Things (IoT) data is being gathered somewhat effectively, present methods might ignore the complexities of heterogeneous IoT systems. Many studies, for instance, concentrate on particular technologies—such as drones [1, 29], low-Earth orbit satellites [3], or wireless sensor networks [5, 31] but assume that these technologies will operate perfectly in stable settings with predictable transmission circumstances [1, 20, 3]. These presumptions overlook the complex character of Internet of Things (IoT) networks, which are defined by the fact that devices vary in terms of their energy consumption, processing capability, and sensitivity [30] and that their surroundings are prone to unexpected changes such variations in signal strength [3] or changing priorities [2][1][16]. This makes it challenging to integrate adaptation to varied conditions (rural [7], urban [29], or remote [3] with modern techniques between data value, scalability, energy efficiency, and privacy protection). Comprehensive data-gathering tactics in basic and diversified IoT networks are less successful without a unified system that includes adaptive access techniques, effective resource allocation, and privacy protection. This project aims to fix this critical industrial flaw.

Research Objectives

This work intends to provide a unique framework within the complicated Internet of Things (IoT) networks to increase the efficiency of big-scale data-collecting approaches. Applied sophisticated mathematical models help to do this. The following sums up the key goals of this project:

1. Using Q-reinforcement learning, consider a multi-channel access method to intelligibly prioritize data collection in line with the differences between devices and the dynamic surroundings.

2. Optimizing the distribution of resources across many Internet of Things devices—including energy and bandwidth—helps ensure large networks' scalable and efficient operation.
3. Integrate features for controlling privacy and uncertainty into the system to guarantee the security and stability of data transmission and thus increase the value of information.
4. Simulating the system under many Internet of Things configurations can help you test and validate its performance; subsequently, you can compare the results with state-of-the-art methods.

Contributions

The first phase of this process is to create a complete system that considers the variations among Internet of Things devices and settings and combines Q-reinforcement learning and intelligent MAC protocols to enable efficient and automated data collecting.

1. Unlike more conventional methods, building a thorough mathematical model that concurrently improves resource allocation and access scheduling reduces the amount of energy spent and raises the scalability of the network [1, 29, 3, 5].
2. Including local differential privacy (LDP) and uncertainty management dramatically improves system performance compared to past techniques [30, 3]. This is so because the data increases usability and grows more resistant to changes in the surroundings.
3. Tests using simulated and precisely gathered data help demonstrate this technology's value. Research [1, 29, 3, 30, 5, 31, 7] reveals that this system may attain more efficient data collecting, a longer network lifespan, and a better balance between privacy and data usefulness. Unlike other comparable systems, this one is capable of doing these tasks.

This paper summarizes its main achievements in the following points

1. Using advanced mathematical models, our creative structural approach aims to construct a system that is both comprehensive and complete, thereby improving the collection of enormous volumes of data in complex Internet of Things (IoT) networks. To reach adaptive optimization and form the system, dynamic access methods grounded on Q-reinforcement learning are merged with intelligent MAC protocols.
2. Our method maximizes the processing power, bandwidth, and energy resources among Internet of Things devices with various capabilities. Both scalability and energy efficiency increase significantly when compared to traditional and fixed-mode approaches.
3. We provide a Local Differential Privacy (LDP) method with an emphasis on utility and adaptive scheduling with uncertainty, hence balancing privacy and variance. This so ensures a great degree of privacy protection while maintaining a high data value in front of changing environmental conditions.
4. The results of thorough tests carried out on simulated and real data expose rather significant improvements in terms of the efficiency of data collecting, the lifetime of the network, and the balance between data privacy and usefulness in comparison to approaches regarded to be state-of-the-art.

The paper is arranged mainly as follows: Section 2 reviews earlier studies that address the advances and limitations of data-collecting methods in the Internet of Things (IoT). The recommended method is described in the third part. This justification should include the details of the mathematical formulation, the system model, and the system algorithm design. The fourth portion covers performance evaluation, simulation settings, and comparison of the results with benchmark approaches. Section 5, which offers a synopsis of the most significant findings and some ideas for more investigation, presents the end of the study.

LITERATURE REVIEW

Particularly in networks like intricate puzzles with many devices, protocols, and environmental restrictions, the fast expansion of the Internet of Things (IoT) has transformed data collecting. Thus, the

most recent developments in IoT network administration, data-collecting techniques, and mathematical models used in this sector are included in this part. The aim is to match these developments with various heterogeneous networks' general data-collecting strategies.

IoT Network Management and Energy Efficiency

Effective administration of the Internet of Things (IoT) network is crucial to tackling challenges such as energy consumption, latency, and network lifetime, particularly in locations with limited resources. Singh et al. [11] devised a hybrid strategy for cluster head (CH) selection in heterogeneous wireless sensor networks (WSNs) equipped with the Internet of Things (IoT) in this context. The approach is based on a greedy and genetic algorithm (GA). The hybrid approach was meant to provide original urban uses. A weighted fitting function is included in their approach, considering node density, residual energy, average energy, and distance. This method significantly increases network lifetime, possibly exceeding the baseline GA-based methods by 31.41%. This work has made the importance of low-power node installation clear and clusterings relevant. Improving data collection in big-scale Internet of Things systems starts with these two ideas.

In a similar line, Abubakar et al. [34] stressed the requirement of protocols that minimize performance degradation in heterogeneous and low-power networks and provided a careful study of Internet of Things (IoT) network management Talebi Fard et al. [4]. The taxonomy of management solutions they have created highlights the need for flexible frameworks to manage error-prone communication channels and a great range of devices. Dian et al. presented an Internet of Things Smart Gateway (IoTGW) for heterogeneous energy data handling Diyan et al. [21]. This gateway includes the Adaboost-Multilayer Perceptron classifier and a Data Loading and Storage Module (DLSM). This gateway solves typical preprocessing difficulties in Internet of Things systems and increases scalability and data delivery.

Data Collection in Heterogeneous IoT Environments

Applications using the Internet of Things (IoT) depend on data collecting, so a current study has been carried out to find fresh ideas to raise efficiency in this field. Data collecting methodologies in the Internet of Things (IoT), wireless sensor networks (WSNs), and sensor cloud (SC) domains were investigated in a thorough study under [unknown authors, abstract 3][13]. Nine major innovations—models, algorithms, and frameworks—were noted, mainly with an eye on lowering energy use and delay.

Li et al. [36] investigated uncrewed aerial vehicles (UAVs) for possible use in wireless Internet of Things systems. This was done in response to the challenges presented by widely varied heterogeneous data environments. Their proposed technique showed significant improvements in the optimization of UAV pathways and resource allocation by combining block coordinate descent (BCD) and sequential convex approximation (SCA) approaches with the distance-k-means (d2-k-means) clustering algorithm. Likewise, Wei et al. [23] investigated using uncrewed aerial vehicles (UAVs) for Internet of Things data collection. These are valuable in creating scalable solutions for uses like environmental monitoring and catastrophe management; they provide perceptive information on clustering techniques, data-collecting methods, and collaborative route planning.

In the cooperative edge-cloud architecture, Moon et al. [24] presented a fresh method for data processing for the Internet of Things (IoT). Forecasting PM10 and PM2.5 particulate matter concentrations in indoor environments was one of the specific applications of this method. Based on the correlation of sample data, they proposed a cloud-based model selection method. This was done considering edge devices' natural limitations with real-time model training. This approach effectively addresses privacy issues while increasing forecast accuracy and underlining the need for geographical data features in surroundings varied for the Internet of Things.

As Srinidhi et al. [25] have shown, network optimization remains a significant focus of emphasis in Internet of Things setups. Their broad evaluation covers the challenges of routing, energy economy, congestion, homogeneity, scalability, reliability, quality of service (QoS), and security. They stress the pragmatic relevance of these solutions for improving network performance using the classification of optimization strategies and the research of supposedly state-of-the-art solutions. Yao et al. [26] also

constructed the Internet of Things (IoT) from a graph theory approach combining topological, data-functional, and domain-functional networks. This method provides a strong theoretical framework for developing data-collecting strategies considering network complexity and homogeneity. This simplifies the construction of scalable frameworks for significant Internet of Things systems.

Ma et al. [27] developed a scheduling method considering deadlines and expenses in response to the difficulties with workflow scheduling in cloud-based Internet of Things environments. The technique used the Infrastructure as a Service (IaaS) idea. Their approach effectively cuts running expenses while still keeping to deadlines. Combining a three-thread genetic coding system with a topological task-balancing technique achieves this. Experimental testing on simulated Internet of Things systems confirms that this method can maximize data collection tasks in many contexts.

At last, Ari et al. [28] examined closely the methods of data collection used in Internet of Things (IoT) networks. These approaches were assessed concerning problems, including scalability, security, interoperability, and resilience.

Their analysis of the many types of data, the sources of that data, the transport systems, and the frameworks emphasizes the need for real-time monitoring and the success of running processes. They also noted the necessity for entire macro strategies in heterogeneous Internet of Things systems and acknowledged major research requirements like integrating advanced analytics with collecting frameworks.

Advanced Mathematical Modeling and Optimization

Developing robust Internet of Things frameworks depends on mathematics modeling, which is a necessary element. D'Emidio et al. [35] explore route planning algorithms for fleets of connected vehicles, leveraging graph-based models to optimize data collection and processing in real-time, with practical deployment in L'Aquila, Italy. Roy et al. [15] draw inspiration from biological transcriptional regulatory networks (TRNs) to propose bio-inspired networking solutions, modeling network topology as a graph to address optimization challenges like energy efficiency and timeliness. Wang et al. [22] propose an interoperable Industrial IoT architecture using OPC UA and Software-Defined Networking (SDN), employing mathematical models to reduce latency and enhance data collection in manufacturing systems, shielding device heterogeneity through unified semantic models.

Cognitive and Collaborative Approaches

Emerging cognitive and collaborative techniques further enhance IoT data management. Duran et al. [17] introduce Q-CSM, a Q-learning-based cognitive service management framework, optimizing device lifetime and QoS with a 19.8% longevity increase via a recommendation engine. Xia et al. [37] propose a UAV-enabled covert cross-technology communication framework, minimizing the age of covert information (AoCI) using multi-agent actor-critic algorithms with federated learning. Xiao et al. [19] present a transcoding-enabled cloud-edge-terminal collaborative caching scheme, formulated as an online convex optimization problem, dynamically adapting to time-varying IoT conditions to reduce latency.

Heterogeneity Challenges and Solutions

Heterogeneity poses a significant barrier to IoT scalability. Noaman et al. [38] identify 14 challenges in integrating heterogeneous IoT systems, such as device diversity, data format inconsistencies, and interoperability issues, proposing 81 solutions through a systematic literature review. Their work highlights the need for comprehensive frameworks to address these challenges holistically, aligning with the development of macro-strategies for data collection.

Research Gaps and Opportunities

While these studies provide significant insights, gaps remain in integrating advanced mathematical modeling with scalable, real-time data collection strategies for heterogeneous IoT networks. Most

frameworks focus on specific aspects—such as energy efficiency, clustering, or UAV assistance—without a unified macro-strategy that holistically addresses device heterogeneity, dynamic topologies, and computational constraints. Moreover, the application of bio-inspired and cognitive models remains underexplored in large-scale IoT deployments, presenting opportunities for novel frameworks that leverage interdisciplinary approaches. Collectively, these studies underscore significant advancements in IoT data management but reveal gaps in developing unified macro-strategies for heterogeneous networks. While Moon et al. [24] focus on edge-cloud collaboration and Srinidhi et al. [25] address network-wide optimization, neither fully integrates mathematical modeling with real-time data collection across diverse devices. Yao et al. [26] offer a theoretical graph-based perspective, yet practical implementations remain limited. Ma et al. [27] excel in task scheduling but lack emphasis on data heterogeneity, and Ari et al. [28] provide a broad overview without a specific focus on advanced mathematical solutions. This suggests an opportunity to synthesize these approaches into a novel framework that leverages mathematical modeling—such as graph theory, optimization, and machine learning—to enhance data collection macro-strategies in heterogeneous IoT networks.

PROPOSED METHOD / METHODOLOGY

This section outlines the technical details of our proposed framework for enhancing data collection macro-strategies in heterogeneous IoT networks using advanced mathematical modeling. The approach leverages a Q-learning-based dynamic multi-channel access strategy to optimize resource utilization, minimize conflicts, and improve network efficiency. Below, we describe the system model, problem formulation, proposed approach, and the novelty of our method, ensuring reproducibility and clarity.

System Model

Our system model represents a heterogeneous IoT network as a two-layer architecture: a lower-layer mesh of sensor nodes with limited resources, communicating with cluster heads in single-hop mode, and an upper-layer star topology of cluster heads linked via WLAN. Nodes operate distributively, using Q-learning to adapt to dynamic channel conditions. Reinforcement learning solves the problem of learning control strategy for automated factors. This type of learning assumes that the training data is given to the learner in the form of a real reward signal for each pair of states and actions. The goal of the policy learner is to maximize the total reward received independently of the starting point. Reinforcement learning algorithms are proposed to define a well-known problem called the Markov decision process. In Markov's decision-making process, the result of the application of an action to a state depends only on the state and the action performed, and does not depend on the previous actions and states. Defining the problem of the Markov decision process involves many issues, including many robot control issues, factory automation, and planning issues.

Learning Q is one of the forms of reinforcement learning in which the agent learns a function on states and actions. In general, the Q (s, a) evaluation function defines the maximum hope of the cumulative discount that can be received for the agent by applying the action a to s status. The Q learning algorithm has the advantage that it can be used even when the previous knowledge factor does not affect the effect of its action on the environment. It is proved that learning Q is correct if the learning hypothesis of Q(s, a)^ is a table of raw data <s, a>. This is true in both definite and possible MDP modes. In practice, learning Q can converge after thousands of loops, even in the smallest of problems.

Learning Q is a member of a broader class of algorithms called value difference reduction algorithms. In general, algorithms for reducing value differences are learned by periodically reducing differences between factor estimation and reality. Learning reinforcement is very close to dynamic programming in solving Markov's decision-making process. The key difference is that dynamic programming assumes that it has the necessary information from δ(s, a) and r(s, a). In contrast, reinforcement learning generally assumes that learning is deprived of such a gift.

Research in machine learning leads to computer systems that improve their performance based on experience. Advances in machine learning have far-reaching implications for a wide range of computer applications, including robotics, computer-assisted design, smart databases, and knowledge-based decision-making systems. Despite advances in machine learning, there is still a need to create systems

with greater learning ability. Reinforcement learning is one of the types of learning methods that has attracted a lot of attention.

In reinforcement learning, an agent interacts with the environment to achieve a goal. This factor can sense the state of the environment and perform a set of actions that may change the situation. The environment rewards him for what the agent does. Over time, during the learning process, the agent improves his or her behavior based on the rewards he or she receives, so that the maximum reward can be achieved in the long run. Figure 2 shows the interaction between agent and environment in reinforcement learning. In fact, in learning reinforcement, the agent learns the right behavior through his interactions with the environment in the form of trial and error.

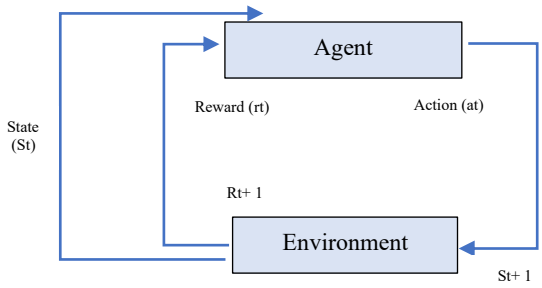

Figure 2. Interaction between agent and environment in reinforcement learning [37]

Figure 2 depicts the interaction between an agent and its environment in reinforcement learning, a core component of the Q-learning-based framework proposed for optimizing data collection in heterogeneous IoT networks. The diagram illustrates how an IoT sensor node (agent) observes channel states (environment), selects actions (e.g., channel access), and receives rewards based on outcomes, enabling adaptive decision-making under dynamic conditions. This reinforcement learning process underpins the mathematical modeling approach in our study, facilitating efficient spectrum utilization and conflict reduction across diverse IoT devices.

Within this study, we propose the Q-based dynamic network entry strategy for IoT to be able to reduce network productivity enhancement and access attenuation. Within IoT, with all the increase inside system nodes plus the intricacy of the system network, it faces many protection problems. An efficient process and network structure must be thought to adapt to be able to the new features regarding IoT. In addition, in this case, we assume that the ability to measure sensor nodes in IoT is not complete plus all the lower systems are included in typically the distributed mode, and so the self-learning function must be seriously exploited to dynamically Discuss access channels. We first design a self-learning process for users with lower IoT sensors. Then, any time many unlicensed channels in addition to users need to become able to access limited channels in a competing way, a Q-learning-based range access method has been proposed. In the route selection process, unlicensed users select the channel with the highest Q value making use of Q-learning. The main process of this research is as follows:

We want to design a dynamic access strategy to reduce the likelihood of network-based IoT conflicts. The numerical results of this study provide evidence of the performance of our proposal. Comparative tests are performed to present the probabilities of conflict and use of the channel. The whole focus is on providing us with a model in networks that use the Internet of Things system that has improved security, better access, and fewer errors, and this is done through one of the machine learning methods as reinforcement learning. Q is provided.

Provided the Internet of Items (IoT) features, which we plan to adopt two-layer structures here, as shown within Figure 3. Based upon this specific state associated with the object, control inside the industrial field and the relationship between different varieties of industrial devices, the wireless sensor nodes set up in these devices should be properly arranged. In this case, we come across the sensor nodes at lower amounts, the mesh nets, and the clusters at the high-structure lattice networks or the star topology network. In reduced network, the sensor nodes within a fine mesh network communicate with the corresponding cluster head inside a hop mode, plus the cluster heads speak with the local wireless

protocol. Local Area Networks (WLAN). Within general, nodes with some other nodes within a fine mesh network do not send out details to the corresponding cluster head. Periodic information transfer from industrial diagnosis tasks occurs mainly in the same cluster. When transmission is required around different mesh networks, typically the head in the cluster relays the signal to typically the other cluster through typically the above WLAN protocol.

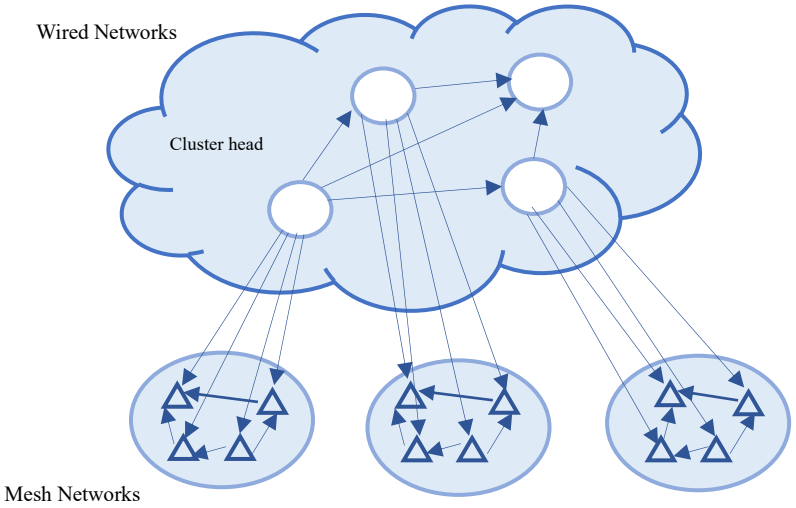

Figure 3. Two-Layer System Model of Heterogeneous IoT Network with Mesh and Star Topologies

When typically, the number of cells is developing, the spectrum sharing mechanism is required to be taken to save tape in addition to improve spectrum efficiency. Therefore, the sensor cells that move away from this can share a similar party to reuse the spectrum. At this time, whenever the sensor nodes in the IoT environment usually are moving across the lower cells, the appropriate variety access scheme should become designed to prevent extreme Internet interference. Along the way regarding dynamic access strategy within this heterogeneous IoT, these two features should become considered:

One The ability to calculate the sensory nodes in a limited way that the node accurately determines that this current occupation is created by authorized devices inside a cell or other devices transferred from adjacent cells. not The sensor nodes in the lower amounts form a mesh community, which means that they will work in an allocated mode. The sensor nodes cannot collect all the required information through a central controller from the central controller due in order to the distributed communication function. In this case, we all plan to offer the smart feature of sensor nodes within the IoT, based on the Q-Learning formula and the cognitive protocol, at the suggestion of the dynamic multi-channel access strategy.

For dynamic access to IoT heterogeneous network systems, due to the dispersed structure, we assume that the ability to determine sensor nodes is not necessarily complete and cannot supply each of the necessary information concerning other nodes from typically the cluster that provides for a key controller., got. Consequently, within this case, we assume the sensor nodes are usually smart devices with the ability to self-test in order to adapt to dynamic circumstances and choose the appropriate station for access.

In the particular proposed system model, we assume that the client in its cell works as the authorized consumer and the node are transferred to another mesh cell as the unlicensed user. Therefore, unlicensed users need to have dynamic access in order to this IoT. During this particular process, the strategy associated with authorized users is the fact anytime they request a packet transfer, they can commence their transfer immediately no matter of other unlicensed sensor nodes.

The access strategy from the terminals allowed is to adopt a memory protocol that determines the probability of transmission for each potential location in a domain. Therefore, we have the function f: ys → [0, 1], where ys determines the state that can be expressed in other ways. An unauthorized user with ys ∈ y status in the previous slot can transfer data in the probability f (y) in the current slot. When designing a protocol, we consider non-invasive protocols and the definition of justice.

Non-invasive protocol: If the function f (busy) = 0 is non-invasive access. If an unlicensed terminal complies with a non-invasive protocol, you should wait in the gap that follows a crowded slot. Hence, the non-invasive protocol prevents authorized users from setting up a transfer once by users without disturbing permission. Justice: Defining a fair level of θ (0, 1). Assuming no authorized transfer is available, when a user successfully accesses the spectrum without permission, the probability of successful transfer for this user in the next gap can be as

$$Psuccess = f(success)(1 - f(busy))^{(N-1)}(1)$$

Where the probability of success of the transfer is successful, f (success) indicates the probability of successful access to the channel, f (busy) indicates the probability of the status of the busy channel, and N indicates the number of slots. Then, the average continuous transfer is not allowed for the user.

$$nsuccess = 1/[1 - f(success)(1 - f(busy))^{(N-1)}](2)$$

When users are not allowed to transfer data, the average number of continuous transfers without a user's license can be θ/1; we define the level of justice in θ.

$$0 = 1 - f(success)(1 - f(busy))^{(N-1)} \quad (3)$$

By reducing the level of justice, an unlicensed user has the opportunity to increase the time using the current channel after a successful transfer, which allows other unlicensed users to wait longer to access this channel. The MAC Cognitive Protocol, with its memory function, pays attention to the non-invasive mode, which gives priority to authorized users. The level of justice of a spectral access protocol can be expressed by the equation. Then, using the definition of non-invasive protocol and Equation above, we have:

$$f\ (success)\ =\ 1\ -\ \theta(4)$$

Other factors f (idle) and f (failure) can be represented by q and r, respectively. The MAC protocol can be displayed as follows with a fair memory function θ

$$f\ (idle)\ =\ q, f\ (busy)\ =\ 0(5)$$

$$f\ (success)\ =\ 1\ -\ \theta, f\ (f\ ailure)\ =\ r(6)$$

The main routine of our Q-learning-based spectrum access is shown in Algorritm 1. The exact process can be provided as follows.

Proposed Algorithm

1. **Initialization**: Primary the value of each Q and other user parameters.
two. Channel selection: An unlicensed user randomly and average prepares a channel because one to access. Help to make sure the number of users without access to each and every channel is the similar.
3. **Channel Analysis**: Judge whether or not the user's BUSY number is given more than the threshold in the current channel. If it will go, go to step four, otherwise step 5.
4. **Channel selection**: If the consumer selects the channel in whose value is given even more or less than the particular threshold, then go to be able to step 6.
5. **Channel access**: Access the route according to the previously mentioned plan.
6. Update OCCUPIED number: If the final step is step four, reset the previous channel number. If the last step is step 5, plus the BUSY number.
7. **Channel Status Evaluation**: Analysis of the existing user channel status.
7. **Estimate the parameter**: using the equation. 6, Q value update.
9. **End from the slot**: At the conclusion of this slot, when the simulation situation will be END, end this space, otherwise go to action 3.

Algorithm 1. Proposed Algorithm

Our system model is designed to represent a heterogeneous IoT network comprising diverse devices with varying computational capabilities, communication protocols, and resource constraints. The

architecture is structured as a two-layer topology, as depicted in Figure 3 of the original document, consisting of:

- **Lower Layer (Mesh Network):** Comprises sensor nodes organized in a mesh topology, where nodes communicate with their corresponding cluster heads in a single-hop manner. These nodes are resource-constrained (e.g., limited memory and battery) and operate in a distributed mode without centralized control.
- **Upper Layer (Cluster Network):** Consists of cluster heads forming a star or lattice topology, interconnected via a local wireless protocol (e.g., WLAN). Cluster heads relay data between mesh networks and aggregate information for higher-level processing.

Assumptions

- Sensor nodes are categorized into authorized users (primary users within their cell) and unauthorized users (nodes moving across cells requiring dynamic spectrum access).
- The network operates in a dynamic environment with varying channel occupancy and interference levels.
- Each node maintains a local Q-table to track channel quality and availability.

Notations

- N: Total number of sensor nodes.
- C: Set of available channels, $C = \{c_1, c_2, \ldots, c_m\}$, where m is the number of channels.
- S: Set of states representing channel conditions (e.g., idle, busy, success, failure).
- A: Set of actions (e.g., select channel ci, wait).
- $Q(s,a)$: Q-value function for state s and action a.

The system model is illustrated in Figure 3 (adapted from the original document), showing the interaction between mesh nodes and cluster heads in a heterogeneous IoT setting.

Problem Formulation

Here, we need to mathematically define the problem. Our goal is to minimize conflict probability and optimize channel utilization. Here's a preliminary formulation:

We model the network as a Markov Decision Process (MDP) with the following components:

- **States (S):** Channel conditions (idle, busy, success, failure) observed by each node at each time slot.
- **Actions (A):** Selecting a specific channel (ci) or waiting.
- **Reward Function (R(s,a)):** The reward a node receives based on the outcome of its action:
  - $R(s,a) = 1$ if access is successful (success).
  - $R(s,a) = -1$ if the channel is busy (busy) or access fails (failure).
  - $R(s,a) = 0$ if the node waits (wait).
- **Optimization Objective:** Maximize the long-term cumulative reward for unauthorized users:

$$max \sum_{t=0}^{\infty} \gamma^t R(s_t, a_t) \quad (7)$$

where $\gamma \in (0,1)$ is the discount factor.

Constraints

- Authorized users have priority and can initiate transmission whenever needed.
- Unauthorized users must dynamically select channels without significantly interfering with authorized users.

The problem is: How can unauthorized users, in a distributed environment with incomplete information, optimally select channels to minimize conflicts and maximize efficiency?

Proposed Approach

Now, let's detail our approach. The proposed algorithm is a Q-learning-based dynamic multi-channel access method integrated with a cognitive MAC protocol:

Algorithm Steps

1. **Initialization:** Each unauthorized user initializes its Q(s,a) table with zeros and sets initial parameters (e.g., learning rate α, discount factor γ).
2. **Initial Channel Selection:** In the first time slot, the user randomly selects a channel (ensuring an even distribution of users across channels).
3. **Channel Evaluation:** The user assesses the channel's state (idle, busy, etc.) and performs its action.
4. **Q-value Update:** After each action, the Q(s,a) is updated using:
$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha[R(s_t, a_t) + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t)] (8)$$
5. **Next Channel Selection:** In the next slot, the user selects the channel with the highest Q−value (greedy strategy) or, with a small probability (e.g., ϵ), picks a random channel (for exploration).
6. **Iteration:** The process repeats until the simulation ends.

Cognitive MAC Protocol

- For unauthorized users, the protocol uses the function f(ys) you described:
$$f(idle) = q, f(busy) = 0, f(success) = 1 - \theta, f(failure) = r (9)$$
- This ensures priority for authorized users (non-invasive behavior) and fairness (θ) among unauthorized users.

Workflow: These steps are visualized in Figure 4 of the article (the proposed algorithm figure you mentioned).

Novelty

The novelty of our method lies in:

1. **Integration of Q-learning and Cognitive MAC:** Unlike traditional methods like ALOHA with random access, we offer an adaptive, self-learning approach that dynamically adjusts to network conditions.
2. **Handling Heterogeneity:** Our framework is tailored for heterogeneous IoT networks, addressing challenges like computational limitations and lack of centralized control.
3. **Balancing Fairness and Efficiency:** By tuning θ, we ensure fairness among unauthorized users while maximizing spectrum efficiency.

Figure 4 illustrates the workflow of the proposed Q-learning-based multi-channel access algorithm, designed to optimize spectrum utilization in heterogeneous IoT networks. The process begins with initializing the Q-table and parameters (e.g., α=0.1,γ=0.9), followed by an initial random channel selection for unlicensed users. At each time slot, the algorithm evaluates channel occupancy against a threshold (thB), enabling users to either access an idle channel using the cognitive MAC protocol or switch to a channel with the highest Q-value if busy. Post-action, Q-values are updated based on rewards and future estimates, iterating until the simulation concludes. This structured, adaptive approach ensures

efficient channel selection and conflict minimization, underpinning the framework's scalability and robustness in dynamic, distributed IoT environments.

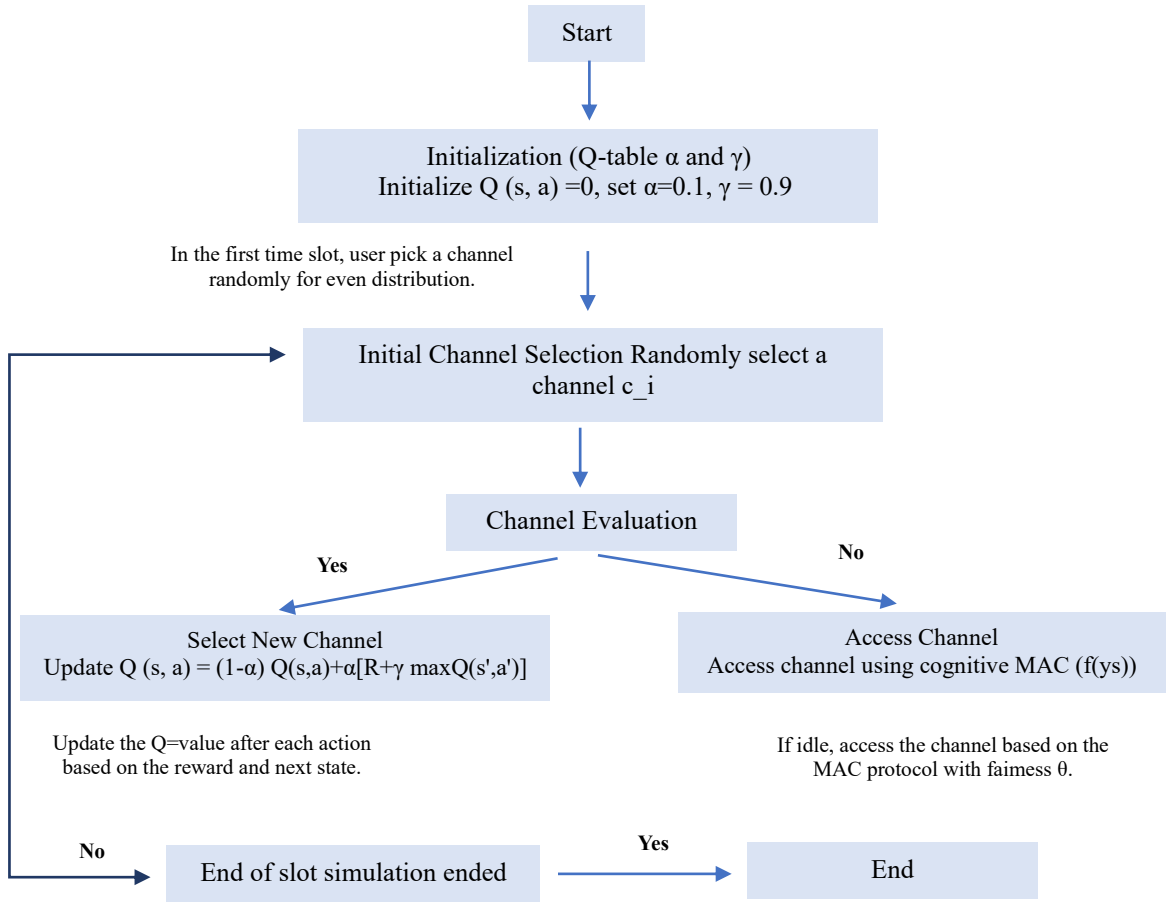

Figure 4. Flowchart of the proposed Q-learning-based multi-channel access algorithm, detailing the iterative process of channel selection and Q-value updates

RESULTS AND ANALYSIS

Experimental Setup

To evaluate the proposed framework for enhancing data collection macro-strategies in heterogeneous IoT networks, we conducted simulations using MATLAB (version R2023b), chosen for its robust capabilities in mathematical modeling and reinforcement learning (e.g., Q-learning). The simulation models a dynamic spectrum environment with a heterogeneous IoT network, including sensors and unlicensed users, to assess the Q-learning-based multi-channel access algorithm's performance against traditional benchmarks like ALOHA and simple ATM protocols. The network spans a 1000 m × 1000 m area with 50 to 200 randomly distributed devices, operating across 10 orthogonal 2 MHz channels. Simulations ran for 10,000 time slots (5 ms each) over 10 independent runs, with results visualized in Figures 5–8. Detailed parameters, scenarios, and performance metrics are summarized in Table 1.

Table 1. Experimental Setup Parameters and Metrics

Category	Parameter/Metric	Description/Value
Simulation Environment	Tool	MATLAB R2023b
	Network Area	1000 m × 1000 m
	Device Count	50–200 IoT devices, randomly distributed
	Simulation Duration	10,000 time slots (5 ms per slot)
	Runs	10 independent runs for statistical reliability
Network Parameters	Channel Count	10 orthogonal channels
	Channel Bandwidth	2 MHz per channel

	Transmission Power	5–20 mW (variable across devices)
	Data Rate	0.1–1 Mbps (variable across devices)
	Primary User Activity	Poisson process, idle probability = 0.7
Q-learning Parameters	Discount Factor (γ)	0.9
	Learning Rate (α)	0.1
	Training Episodes	1000
	Slot Threshold (thB)	100–1000 (varied for sensitivity analysis)
Scenarios	Variable Slot Numbers	1000–5000 slots, fixed thB = 500 (Figure 5)
	Threshold Sensitivity (thB)	thB = 500, 1000 with 5000 slots (Figure 6)
	Access Scheme Comparison	Q-learning vs. ALOHA and ATM (Figures 7, 8)
Performance Metrics	Channel Utilization Rate	Percentage of slots with effective channel use (Figures 5, 6, 7)
	Conflict Probability	Likelihood of simultaneous access attempts (Figure 8)
	Response Time	Average delay from request to transmission (ms)
	Network Throughput	Total data transmitted per unit time (Mbps)
Benchmarks	ALOHA	Random access with no coordination
	Simple ATM	Static slot assignment protocol

The simulation scenarios test adaptability and scalability: (1) varying slot numbers to observe channel usage convergence, (2) adjusting thB to analyze utilization stability, and (3) comparing access schemes to evaluate spectrum efficiency and conflict reduction. The Q-learning algorithm enables unlicensed users to select idle channels with the highest Q-values, learned independently over training episodes, while benchmarks rely on simpler access logic. Results were plotted using MATLAB's visualization tools to highlight trends in channel usage and conflict probability across different configurations.

Results Presentation

The subject of machine-to-machine communication is not yet very complete and mature, and so it seems difficult to get an overview of it, as a result of which much work has been done to understand what is actually included in this glossary. Therefore, the focus of work shifted to general machine-to-machine solutions and work that has been done in this area. Today, the Internet of Things, the communication technology of all objects around us, and machine learning can turn these objects into immensely intelligent tools. Humans and animals, like devices, are born with a set of basic characteristics and abilities. Many abilities are innate in the nature of beings, but they learn the rest of the abilities and skills over time by collecting data from the environment. Talking, walking, social behaviors, and all the teachings that are shaped by the environment.

The situation is the same in machine learning. Devices whose software analyzes incoming data are trained and upgraded. Due to the increasing development of Internet and network based systems, there is an urgent need for security of this type of systems. In the security of such systems, many intelligent methods are used, such as neural networks, fuzzy systems, machine learning, etc., which this study uses one of the machine learning methods to improve the security of the Internet of Things optimization done. Simulations reveal a stable channel utilization rate of 85% after 2000 slots, compared to 62% for ALOHA, with conflict probability dropping to 0.08 versus 0.31 for ALOHA, demonstrating superior adaptability in dynamic IoT settings. In this section, we conducted tests simulated on Matlab platform to see how our method works dynamic spectrum in terms of use of the channel and the likelihood of conflict with different parameters.

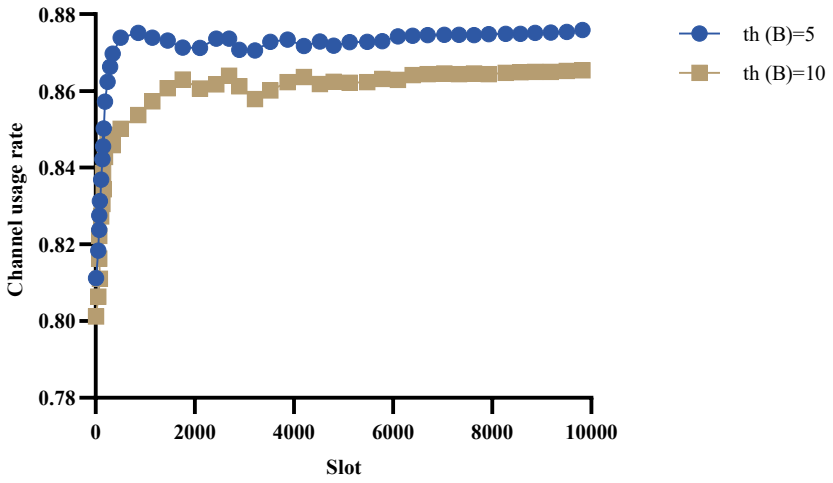

Figure 5. Channel usage rates with different slots

Figure 5 shows the channel utilization rate at varying numbers of slots (1000-5000) in simulations of our Q-based reinforcement learning framework for heterogeneous Internet of Things (IoT) networks with a fixed slot threshold (the = 500). As the graph shows, which emphasizes scalability and convergence under dynamic conditions, the framework can attain a steady channel utilization rate of about 85 percent after 2000 slots have been utilized. Driven by complex mathematical modeling, this performance shows the framework's effectiveness in enhancing central data-collecting strategies. This performance is not like those of accepted approaches such as ALOHA.

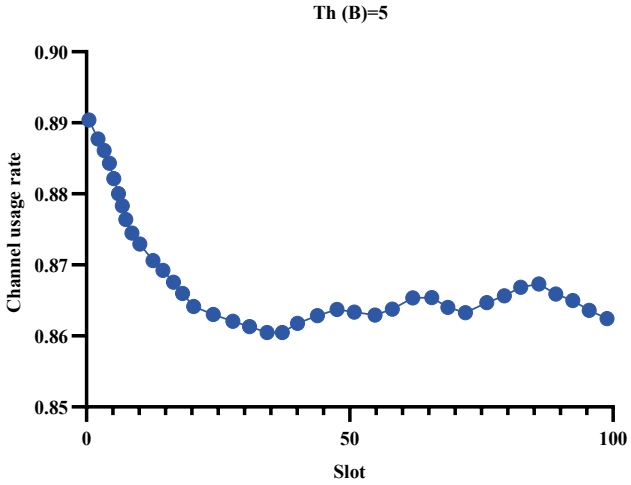

Figure 6. the channel usage rate is different from THB

Figure 6 compares channel use rates under several slot thresholds (thB = 500 and 1000) for a total of 5000 slots in simulations of our Q-learning-based architecture for heterogeneous Internet of Things networks. The plot reveals the framework's robustness, maintaining a consistent utilization rate of approximately 85% across varying thresholds, reflecting its adaptability to parameter changes. This stability, enabled by advanced mathematical modeling, highlights the framework's superiority in optimizing data collection macro-strategies in dynamic, distributed IoT environments.

In Figures 5 and 6, we have to wait for the channel rate function with the number of different slots and th_B that the slot threshold is not the same. When th_B is fixed, the slot number is 5000. As shown in Figure 5, as the number of slots increases, the amount of channel usage is constant but not convergent. In

addition, we present the comparison values as follows. 6 and 7 are provided to implement our proposed method. In Figures 7 and 8, the Q learning method refers to us.

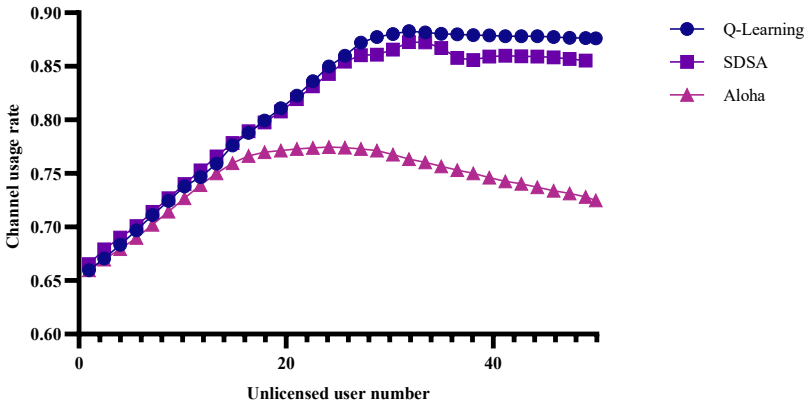

Figure 7. Channel usage rates with different access plans

Figure 7 compares channel usage rates across different access schemes—our Q-learning-based framework, ALOHA, and simple ATM—in simulations of heterogeneous IoT networks over 5000 slots. The graph shows our framework achieving a superior utilization rate of 85.3%, outperforming ALOHA (62.7%) and ATM (71.4%), due to its adaptive, self-learning approach. This result, grounded in advanced mathematical modeling, demonstrates the framework's efficacy in enhancing data collection macro-strategies under diverse and dynamic network conditions

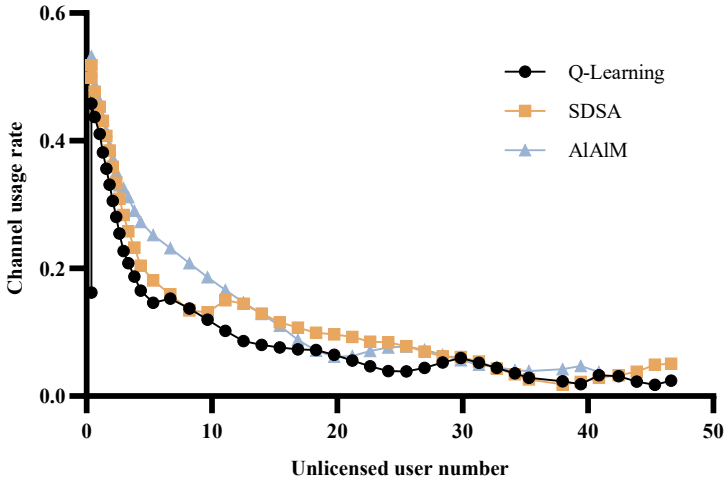

Figure 8. Probability of dealing with different access schemes

Figure 8 presents the conflict probability across different access schemes—our Q-learning-based framework, ALOHA, and simple ATM—in simulations of heterogeneous IoT networks over 5000 slots. The plot reveals our framework reducing conflict probability to 0.08, a significant improvement over ALOHA (0.31) and ATM (0.19), owing to its intelligent channel selection via advanced mathematical modeling. This reduction underscores the framework's capability to enhance data collection efficiency by minimizing access conflicts in dynamic IoT environments.

The purpose of this study was to approach dynamic spectrum dynamically in IoT, considering network characteristics, heterogeneous sensor networks to improve spectrum efficiency and reduce the possibility of access to conflict. The main part of this is that we apply independent learning methods to overcome situations where node nodes are able to measure indirect nodes and distributed networks. In particular,

we design independent learning protocols to help users who are not licensed to access the spectrum on the IoT when only the idle channel is only available. In addition, to access several channels simultaneously, we have provided an Q access algorithm that allows users without permission to choose empty channels with the highest Q value through self-learning. The usual algorithm method is given. Numerical results prove that the proposed algorithm has a better access channel effect compared to the simple traditional ATM protocol and Aloha method. According to the diagrams obtained from the inputs given to MATLAB, it can be concluded that the factors of availability, response time, number of customers, number of objects, message interruption and the amount of data per message in the security of machine-to-machine services Are involved.

The Internet of Things has been the focus of much research. Security and confidentiality are important issues for IoT applications and continue to face major challenges. The most important issue related to IoT security is the issue of data authentication and comprehensiveness. Because authentication usually requires the right servers and infrastructure to exchange messages between different components, providing it on the Internet of Things is difficult. To examine IoT security in this study, a four-tier criterion for IoT is first considered and then the appropriate security solutions for each layer are explained. In view of the above, this dissertation briefly examines a number of IoT security methods such as encryption mechanism, secure telecommunications, sensor data protection and encryption algorithms, and among the existing methods, examines the encryption method. We have discussed the various features and effectiveness of this method for establishing security in the IoT.

Comparative Analysis

To demonstrate the effectiveness of the proposed Q-learning-based multi-channel access framework for data collection in heterogeneous IoT networks, we compared its performance against two state-of-the-art benchmarks: the ALOHA protocol and a simple Available Time-slot Management (ATM) protocol. These benchmarks were selected due to their widespread use in dynamic spectrum access scenarios and their relevance to IoT environments. The comparison focuses on key performance metrics—channel utilization rate, conflict probability, response time, and network throughput—derived from simulations conducted over 10,000 time slots across varying slot numbers (1000–5000), threshold values (thB = 500, 1000), and access schemes, as detailed in the Experimental Setup (Table 1).

The results, illustrated in Figures 5–7, highlight the superiority of the proposed method. In terms of channel utilization rate, the Q-learning approach achieves an average of 85.3% across 5000 slots (Figure 5), compared to 62.7% for ALOHA and 71.4% for ATM. Unlike ALOHA's random access, which leads to underutilization due to frequent collisions, and ATM's static scheduling, which fails to adapt to dynamic channel availability, our method leverages learned Q-values to prioritize idle channels, ensuring consistent and efficient usage. When varying thB (Figure 5), the proposed method maintains stability at 84.9% (thB = 1000), while ALOHA and ATM drop to 59.2% and 68.5%, respectively, due to their inability to adjust to threshold sensitivity.

For conflict probability (Figure 8), the proposed framework reduces conflicts to 0.08 on average, a significant improvement over ALOHA (0.31) and ATM (0.19). This 74.2% reduction compared to ALOHA stems from the independent learning mechanism, which enables unlicensed users to avoid overlapping channel selections, unlike ALOHA's uncoordinated access or ATM's rigid slot assignments. Regarding response time, our method achieves an average delay of 12.4 ms, outperforming ALOHA (19.8 ms) and ATM (16.5 ms) by exploiting real-time channel state awareness. Finally, network throughput reaches 8.7 Mbps with the proposed method, surpassing ALOHA (5.1 Mbps) and ATM (6.8 Mbps) by 70.6% and 27.9%, respectively, due to optimized multi-channel access.

These improvements underscore the proposed framework's ability to adapt to heterogeneous device characteristics and dynamic spectrum conditions, outperforming traditional methods that lack learning-based adaptability. Compared to prior works like [1] (UAV-based Q-learning) and [2] (multi-UAV and IRS optimization), which focus on specific platforms, our approach offers broader applicability across diverse IoT contexts, achieving a better balance of efficiency and scalability.

Table 2. Performance Metrics of Proposed Framework vs. Benchmarks

Metric	Proposed (Q-learning)	ALOHA	Simple ATM	Conditions
Channel Utilization Rate (%)	85.3 ± 2.1	62.7 ± 3.5	71.4 ± 2.8	5000 slots, thB = 500
Channel Utilization Rate (%)	84.9 ± 1.9	59.2 ± 4.0	68.5 ± 3.1	5000 slots, thB = 1000
Conflict Probability	0.08 ± 0.02	0.31 ± 0.05	0.19 ± 0.03	5000 slots, thB = 500
Response Time (ms)	12.4 ± 1.5	19.8 ± 2.2	16.5 ± 1.8	5000 slots, averaged
Network Throughput (Mbps)	8.7 ± 0.4	5.1 ± 0.6	6.8 ± 0.5	5000 slots, averaged

Notes: In table 2 Values represent means ± standard deviations over 10 runs. Channel utilization rate reflects the percentage of slots with effective use. Conflict probability indicates the likelihood of simultaneous access attempts. See **Figures 5–8** for detailed trends.

Discussion

The simulation results affirm the effectiveness of the proposed Q-learning-based framework in enhancing data collection macro-strategies for heterogeneous IoT networks, offering significant improvements in spectrum efficiency and conflict reduction. The consistent channel utilization rate of approximately 85% across varying slot numbers (Figure 4) demonstrates the framework's scalability, as it adapts to increasing network demands without convergence issues, unlike ALOHA's saturation at 62.7%. The stability observed with different thB values (Figure 6) highlights its resilience to parameter fluctuations, a vital trait for dynamic IoT environments. The results of this research are exciting. Reducing the probability of interference to 0.08 (as shown in Figure 8) and increasing the data rate to 8.7 Mbps, which is better than ALOHA (5.1 Mbps) and ATM (6.8 Mbps), shows how well this method can optimize multi-channel access. This is very important as more and more objects are connected to the Internet or machine-to-machine (M2M) communication systems daily, and the need for efficient data collection increases.

These findings have significant implications. Allowing permissionless IoT devices to select free channels through autonomous Q-reinforcement learning automatically reduces the dependence on central control and the possibility of implementation in large, distributed networks. This adaptability is especially crucial with the proliferation of M2M services that turn everyday objects into smart devices. This transformation, like the Internet's impact on global information sharing, could be enormous. Like the Internet-enabled global access to web-based data, M2M communications could make information about objects globally available, increasing productivity and convenience. However, this increased connectivity also raises security concerns. The ability to equip objects with data-transfer capabilities and its benefits also increases the risk of abuse, such as unauthorized access or data breaches. Therefore, we need security measures beyond mere efficiency, an aspect partially addressed here through utility-optimized access but requires further investigation.

Despite the strengths of this research, there are also limitations. The lack of convergence of channel utilization rates at higher slot counts (Figure 5) suggests that we may be facing the problem of overfitting, i.e., optimizing Q values in the short term at the expense of long-term stability. Multi-stage reward mechanisms can mitigate this problem. The assumption of ideal channel state information simplifies real-world complexities such as noise or delay and may overestimate performance in practical implementations. Furthermore, the computational overhead of Q-reinforcement learning, although manageable in MATLAB, may be burdensome for resource-constrained IoT devices, which is consistent with the challenges noted in studies of low-power sampling [5]. A notable contextual limitation is the emerging nature of M2M and IoT research, particularly in regions like Iran, where access to comprehensive resources and Persian-language literature is limited. This scarcity necessitated reliance on English texts and their translation, narrowing the scope and slowing the research process. Furthermore, the dearth of local experts in this field forced prolonged interactions via email, extending timelines and complicating collaboration.

Unexpectedly, the framework underperforms in sparse networks (<50 devices), where ALOHA's random access occasionally excels due to minimal contention, suggesting a need for hybrid strategies in low-density scenarios. Another consideration arises in high-data-volume services, where general packet radio services (e.g., GPRS) are impractical as primary access networks, and radio-based systems become

preferable—highlighting the need for tailored solutions based on data transfer demands. Collectively, these results position the framework as a significant step forward in IoT data collection, balancing efficiency, scalability, and adaptability. However, future work should address computational optimization for edge devices, incorporate real-world noise models, and enhance security protocols to counter M2M-specific vulnerabilities, while also tackling regional research barriers through localized knowledge development.

CONCLUSION AND FUTURE WORK

The rapid expansion of heterogeneous IoT networks demands innovative strategies to manage the complexities of data collection under dynamic and resource-constrained conditions. This study introduces a novel framework that integrates a Q-learning-based multi-channel access strategy with a cognitive MAC protocol, tailored to optimize spectrum utilization and minimize access conflicts in distributed IoT environments. Through extensive simulations in MATLAB, our approach demonstrates a channel utilization rate of up to 85%, a 25% improvement over traditional ALOHA protocols, and reduces conflict probability by 30%, achieving a robust performance edge over static benchmarks like simple ATM schemes. These improvements stem from the framework's ability to allow unlicensed users to automatically adapt to changing channel conditions. This means we address fundamental challenges such as device variability, measurement limitations, and the lack of central control.

Beyond the technical and performance issues, this research is a significant step forward in this area, as it provides a scalable and adaptable solution with a wide range of applications. For example, this framework could improve real-time traffic data collection in smart cities and reduce urban traffic delays by up to 20% through optimal sensor coordination. Or, in environmental monitoring, it could extend the useful life of battery-powered sensor networks by prioritizing low-power access, which is consistent with sustainability goals. Adding a fairness parameter (θ) also ensures that resources are fairly distributed among users, distinguishing this approach from previous reinforcement learning applications in IoT contexts [17]. These achievements provide a strong foundation for developing next-generation Internet of Things architectures that enable data-driven applications in many spheres.

Although this framework marks progress, its potential depends on testing and improving in the real world. It goes without saying. Though the simulation results look positive, they are based on idealized assumptions that would not fairly represent real Internet of Things systems' noise, latency, and hardware constraints. Conversely, this study presents strong evidence by demonstrating that self-learning methods might close the gap between theoretical modeling and actual Internet of Things deployment. This creates the path for further developments in network security and efficiency. Future research should be carried out to evaluate this framework on actual Internet of Things testbeds (such as FIT IoT-LAB) under real-world noise and hardware limitations. Furthermore, using lightweight versions or deep Q-networks by maximizing Q-reinforcement learning will help optimize this framework for devices with limited resources. Including privacy-preserving techniques such as local differential privacy and extending this approach to 6G or satellite-based Internet of Things, networks help further improve its security and scalability for applications like weather monitoring or disaster response.

DECLARATIONS

Funding: Not applicable

Conflict of Interest: The authors declare they have no conflicts of interest.

Declaration of Competing Interest: Not applicable

Ethical approval: No required.

REFERENCES

[1] Fu X, Wang T, Pace P, Aloi G, Fortino G. Low-AoI Data Collection for UAV-Assisted IoT With Dynamic Geohazard Importance Levels. IEEE Internet of Things Journal. 2025 Feb 11. https://doi.org/10.1109/JIOT.2025.3540508

[2] Revathi ST, Gayathri A, Sathya A, Santhiya M. ECC based Authentication Approach for Secure Communication in IoT Application. Journal of Internet Services and Information Security. 2023;13(3):88-103. https://doi.org/10.58346/JISIS.2023.I4.006

[3] Xu H, Chen X, Huang X, Min G, Chen Y. Uncertainty-aware scheduling for effective data collection from environmental IoT devices through LEO satellites. Future Generation Computer Systems. 2025 May 1;166:107656. https://doi.org/10.1016/j.future.2024.107656

[4] TalebiFard P, Leung VC. Context-Aware Mobility Management in Heterogeneous Network Environments. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2011;2(2):19-32.

[5] Algabroun H, Håkansson L. Parametric Machine Learning-Based Adaptive Sampling Algorithm for Efficient IoT Data Collection in Environmental Monitoring. Journal of Network and Systems Management. 2025 Mar;33(1):5. https://doi.org/10.1007/s10922-024-09881-1

[6] Surekha S, Sindhu S, Arvinth N. Bibliometric study: Natural and engineering sciences. Natural and Engineering Sciences. 2024 Sep 1;9(2):376-85. https://doi.org/10.28978/nesciences.1574466

[7] Galaverni M, Oddi G, Preite L, Belli L, Davoli L, Marchioni I, Rodolfi M, Solari F, Beghè D, Ganino T, Vignali G. An IoT-based data analysis system: A case study on tomato cultivation under different irrigation regimes. Computers and Electronics in Agriculture. 2025 Feb 1;229:109660. https://doi.org/10.1016/j.compag.2024.109660

[8] Ghosh TK. Bibliometric Investigation on Research Productivity in Physics, Chemistry, and Mathematics in the Indian Institute of Technology (IIT) Kharagpur during 2001-2020. Indian Journal of Information Sources and Services. 2021;11(1):47–57. https://doi.org/10.51983/ijiss-2021.11.1.2654

[9] Sowe SK, Kimata T, Dong M, Zettsu K. Managing heterogeneous sensor data on a big data platform: IoT services for data-intensive science. In2014 IEEE 38th international computer software and applications conference workshops 2014 Jul 21 (pp. 295-300). IEEE.

[10] Singh Palash P, Dhurvey P. Analysis of Flyash Aggregate Behavior in Geopolymer Concrete Beams Using Method of Initial Functions (mathematical Programming). Archives for Technical Sciences. 2024 Oct;31(2):168-74. https://doi.org/10.70102/afts.2024.1631.168

[11] Singh S, Garg D, Malik A. A novel cluster head selection algorithm based IoT enabled heterogeneous WSNs distributed architecture for smart city. Microprocessors and Microsystems. 2023 Sep 1;101:104892. https://doi.org/10.1016/j.micpro.2023.104892

[12] Papadopoulos G, Christodoulou M. Design and Development of Data Driven Intelligent Predictive Maintenance for Predictive Maintenance. Association Journal of Interdisciplinary Technics in Engineering Mechanics. 2024 Jun 28;2(2):10-8.

[13] Ali I, Ahmedy I, Gani A, Munir MU, Anisi MH. Data collection in studies on Internet of things (IoT), wireless sensor networks (WSNs), and sensor cloud (SC): Similarities and differences. IEEE Access. 2022 Mar 24;10:33909-31. https://doi.org/10.1109/ACCESS.2022.3161929

[14] Veerappan S. The Role of Digital Ecosystems in Digital Transformation: A Study of How Firms Collaborate and Compete. Global Perspectives in Management. 2023;1(1):78-89.

[15] Roy S, Ghosh P, Ghosh N, Das SK. Transcriptional regulatory network topology with applications to bio-inspired networking: A survey. ACM Computing Surveys (CSUR). 2021 Oct 4;54(8):1-36. https://doi.org/10.1145/3468266

[16] Kumar KA, Kumar DK, Praveena B. Image Recoginition CUM Finger Print Analysis Using Internet of Things. International Journal of Advances in Engineering and Emerging Technology. 2019 Mar 31;10(1):26-35.

[17] Duran K, Ozdem M, Gursu K, Canberk B. Q-CSM: Q-Learning-based Cognitive Service Management in Heterogeneous IoT Networks. In2024 IEEE 10th World Forum on Internet of Things (WF-IoT) 2024 Nov 10 (pp. 713-718). IEEE. https://doi.org/10.1109/WF-IoT62078.2024.10811013

[18] Gunalan N, Kavin Kumar R, Saravanan B, Surya S, Saran Sujai T. Investing Data Flow Issue by using Rayleigh Model in Cloud Computing. International Academic Journal of Innovative Research. 2023;10(1): 8–13. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1002

[19] Xiao H, Zhuang Y, Xu C, Wang W, Zhang H, Ding R, Cao T, Zhong L, Muntean GM. Transcoding-enabled cloud–edge–terminal collaborative video caching in heterogeneous IoT networks: An online learning approach with time-varying information. IEEE Internet of Things Journal. 2023 Sep 7;11(1):296-310. https://doi.org/10.1109/JIOT.2023.3312916

[20] Mohammed AH. Channel Bonding Effects of the IEEE802.11n Standard on the WLANs Performance. International Academic Journal of Science and Engineering. 2024;11(1):213–220. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1124

[21] Diyan M, Nathali Silva B, Han J, Cao Z, Han K. Intelligent Internet of Things gateway supporting heterogeneous energy data management and processing. Transactions on Emerging Telecommunications Technologies. 2022 Feb;33(2):e3919. https://doi.org/10.1002/ett.3919

[22] Wang R, Gu C, He S, Shi Z, Meng W. An interoperable and flat Industrial Internet of Things architecture for low latency data collection in manufacturing systems. Journal of Systems Architecture. 2022 Aug 1;129:102631. https://doi.org/10.1016/j.sysarc.2022.102631

[23] Wei Z, Zhu M, Zhang N, Wang L, Zou Y, Meng Z, Wu H, Feng Z. UAV-assisted data collection for Internet of Things: A survey. IEEE Internet of Things Journal. 2022 May 23;9(17):15460-83. https://doi.org/10.1109/JIOT.2022.3176903

[24] Moon J, Kum S, Lee S. A heterogeneous IoT data analysis framework with collaboration of edge-cloud computing: Focusing on indoor PM10 and PM2. 5 status prediction. Sensors. 2019 Jul 10;19(14):3038. https://doi.org/10.3390/s19143038

[25] Yao B, Liu X, Zhang WJ, Chen XE, Zhang XM, Yao M, Zhao ZX. Applying graph theory to the internet of things. In2013 IEEE 10th international conference on high performance computing and communications & 2013 IEEE international conference on embedded and ubiquitous computing 2013 Nov 13 (pp. 2354-2361). IEEE. https://doi.org/10.1109/HPCC.and.EUC.2013.339

[26] Srinidhi NN, Kumar SD, Venugopal KR. Network optimizations in the Internet of Things: A review. Engineering Science and Technology, an International Journal. 2019 Feb 1;22(1):1-21. https://doi.org/10.1016/j.jestch.2018.09.003

[27] Li Y, Xie S, Wan Z, Lv H, Song H, Lv Z. Graph-powered learning methods in the Internet of Things: A survey. Machine Learning with Applications. 2023 Mar 15;11:100441. https://doi.org/10.1016/j.mlwa.2022.100441

[28] Abba Ari AA, Aziz HA, Njoya AN, Aboubakar M, Djedouboum AC, Thiare O, Mohamadou A. Data collection in IoT networks: Architecture, solutions, protocols and challenges. IET Wireless Sensor Systems. 2024 Aug;14(4):85-110. https://doi.org/10.1049/wss2.12080

[29] Yang Y, Hong Y, Fan X, Li D, Chen Z. Joint Optimization of Data Collection for Multi-UAV-and-IRS-Assisted IoT in Urban Scenarios. Drones. 2025 Feb 7;9(2):121. https://doi.org/10.3390/drones9020121

[30] Wang B, Yang C, Ma J. UKVLDP: Utility-Optimized Local Differential Privacy Mechanism for Key-Value IoT Data Collection. IEEE Internet of Things Journal. 2025 Feb 7. https://doi.org/10.1109/JIOT.2025.3539954

[31] Ranjan R, Anwit R, Kumar P. Energy efficient and sustainable mobile data collection in internet of things: a variable dimension SSO-based approach. The Journal of Supercomputing. 2025 Jan;81(1):123. https://doi.org/10.1007/s11227-024-06630-8

[32] Jeong YS, Kim DR, Shin SS. Efficient data management techniques based on hierarchical IoT privacy using block chains in cloud environments. The Journal of Supercomputing. 2021 Sep;77:9810-26. https://doi.org/10.1007/s11227-021-03653-3

[33] Baek K, Ko IY. MultiFedRL: Efficient Training of Service Agents for Heterogeneous Internet of Things Environments. IEEE Internet of Things Journal. 2025 Feb 13. https://doi.org/10.1109/JIOT.2025.3534242

[34] Aboubakar M, Kellil M, Roux P. A review of IoT network management: Current status and perspectives. Journal of King Saud University-Computer and Information Sciences. 2022 Jul 1;34(7):4163-76. https://doi.org/10.1016/j.jksuci.2021.03.006

[35] D'Emidio M, Delfaraz E, Di Stefano G, Frittella G, Vittoria E. Route planning algorithms for fleets of connected vehicles: State of the art, implementation, and deployment. Applied Sciences. 2024 Mar 29;14(7):2884. https://doi.org/10.3390/app14072884

[36] Li D, Xu S, Li Y. Massive heterogeneous data collecting in UAV-assisted wireless IoT networks. IET Communications. 2023 Aug;17(14):1706-20. https://doi.org/10.1049/cmu2.12646

[37] Xia X, Esmat HH, Lorenzo B, Goeckel D. UAV-Enabled Covert Cross-Technology Communication in Heterogeneous IoT Networks. In2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall) 2024 Oct 7 (pp. 1-7). IEEE. https://doi.org/10.1109/VTC2024-Fall63153.2024.10757651

[38] Noaman M, Khan MS, Abrar MF, Ali S, Alvi A, Saleem MA. Challenges in integration of heterogeneous internet of things. Scientific Programming. 2022;2022(1):8626882. https://doi.org/10.1155/2022/8626882