

Improving the performance of IoT devices that use Wi-Fi

Ali Ahmed Razzaq, Kunjam Nageswara Rao

Department of Computer Science and Systems Engineering, College of Engineering, Andhra University, Visakhapatnam, India

Article Info

Article history:

Received Nov 10, 2023

Revised May 26, 2024

Accepted Jul 3, 2024

Keywords:

Identity management system

Internet of things

Machine learning

Power consumption

Quality of service

ABSTRACT

Providing quality service to users of the internet of things (IoT) entails addressing two crucial aspects: one related to security and the other concerning the limited resources of IoT devices. We will face a challenge while using time-sensitive applications within a network that utilizes a high-performance Wi-Fi technology with exceeding energy consumption. Due to this research challenge, we propose a new algorithm, IoT-quality of service (QoS), designed to achieve a true balance between enhancing the security aspects of IoT devices and improving network-hardware performance. Thus, the algorithm efficiently manages the limited energy resources by monitoring energy levels, communication quality, and queuing delay at access points. This is accomplished by utilizing a streamlined identity management system capable of achieving authentication and access authorization with reduced loading for IoT devices. The research hypothesis underwent validation through a comparative analysis of its performance against the conventional model of a Wi-Fi-based IoT device. This evaluation was conducted utilizing the NS3 simulator and was based on a predetermined set of parameters influencing the examined performance metrics, including power consumption, throughput, delay, and response time. The findings exposed the superiority of the proposed algorithm.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ali Ahmed Razzaq

Department of Computer Science and Systems Engineering, College of Engineering, Andhra University

Visakhapatnam 530003, Andhra Pradesh, India

Email: taifali607@gmail.com

1. INTRODUCTION

The quality of service (QoS) is a parameter that assesses the overall performance of a service, particularly the performance observed (experienced) by service users. In light of the extensive utilization and implementation of internet of things (IoT) services in our day-to-day activities, it becomes essential to lower the expenses associated with IoT devices, all while ensuring that the level of provided QoS remains uncompromised. Also, Under the concept of the IoT, there are countless devices with different characteristics and capabilities. So to improve the QoS associated with IoT, two key elements should be ensured, namely: network security to achieve privacy and the security of network resources, and the efficient administration and allocation of network resources. Prominent research papers in IoT devices and QoS can be found in [1]-[6].

The concept of device isolation is crucial, as it prohibits direct access from the internet, ensuring prevention of unauthorized access and privacy violations. Both authentication and access authorization pose challenges for the IoT, given its divergence from traditional internet components, wherein IoT devices are predominantly purpose-specific and typically have limited resources. The identity management (IdM) system provides both authentication and access authorization for internet users (user identity information management) This system consists of four components, as illustrated in Figure 1, namely entities (users or devices), identifiers (entity Identities), identifier provider (IdP), and service provider (SP).

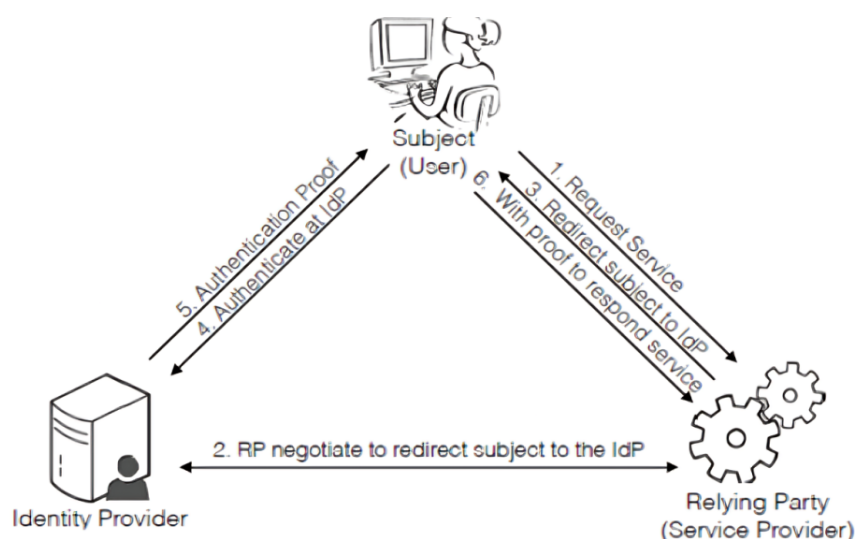


Figure 1. Components of the IdM system

Efforts and research have been directed towards proposing several approaches that could leverage IdM with IoT, specifically in the realms of authentication and access authorization schemes. A proposed authentication and access control framework for IoT devices considered devices as final entities in the internet architecture, communicating through unique IPv6 addresses. It utilized the OpenID protocol for authentication and the role-based access control (RBAC) protocol for access authorization. However, the proposal did not address single sign-on (SSO) issues and did not highlight any results that could validate the suggestion carried out by Liu *et al.* [7]. In Chibelushi *et al.* [8] studied an IdM system for IoT in the healthcare context, but it failed to provide secure communication, leaving IoT devices accessible directly from the internet. Later, Leo *et al.* [9] utilized web services between the internet and IoT to ensure confidentiality and security of transmitted information. This study, however, is not considered to be capable of securing end-to-end security interaction between the internet and IoT, secure communication channels, or even a SSO service. However, Witkovski *et al.* [10] suggested integrating IdM with IoT to maintain SSO and data encryption between communicating parties. However, the study did not provide any results related to power consumption, especially considering that the provision of SSO is based on encryption keys. Recently, Santos *et al.* [11] introduced the unified federated lightweight authentication of things (FLAT) authentication protocol, combining symmetric encryption systems and embedded certificates, bypassing the principles of asymmetric/symmetric encryption used in traditional federated IdM systems. Yet, it did not take into account access authorization processes and service discovery. Other studies about using IoT with IdM are found in [12]-[17].

This research aims at leveraging artificial intelligence (AI) techniques to accomplish this task, given their notable presence in addressing the challenges posed by the upcoming generations in the field of wireless communications. In this research, we use IoT devices employing Wi-Fi technology for network connectivity. This choice is based on the widespread use of wireless local area networks (WLAN) in the unlicensed spectrum, highlighting the increasing complexity in wireless networks. Quality of communication standards in the IoT must ensure stability and accuracy for the utilized learning technology. Sindjoun and Minet [18] distinguished between two types of communication quality standards, one is hardware-dependent and the other is software-dependent. Hardware-dependent standards directly collect data from the devices without preprocessing and include indicators such as received signal strength indicator (RSSI), link quality indicator (LQI), and signal-to-noise ratio (SNR). The precision provided by hardware-dependent standards is insufficient for two main reasons. Firstly, only successfully transmitted packets are considered, and secondly, the evaluation does not take into account the entire packet but only its initial symbols. However, acquiring its values requires undertaking computational operations, namely: packet delivery ratio, the required number of packet transmissions, and the degree.

As attaining performance quality for the IoT network is the primary objective, it is necessary to consider the allocated resources and attempt to utilize them optimally based on the outcomes of machine learning algorithms (i.e., channel state). Channel access is often congested simultaneously, particularly when a large

number of devices connect to the same wireless channel at the same time. Consequently, the channel becomes overloaded, So Ma *et al.* [19] proposed a deep learning-based channel allocation algorithm, applying time of wait (ToW) for selecting communication channels in massive cognitive IoT networks. Their results demonstrated significant improvement in interference detection compared to traditional methods not relying on deep learning. Energy allocation and interference management are crucial aspects affecting IoT networks. For this reason Lynggaard [20] proposed a dynamic system for interference detection and energy allocation, based on the interference level in radio channels. They applied the channel state information (CSI) algorithm to predict transmission energy levels (based on CSI). Considering that many IoT devices are small-sized with limited battery capacity, intelligent management and allocation of this scarce resource are essential. Hence, Zekić-Sušac *et al.* [21] suggested an AI based energy management system for smart cities relying on IoT. Neural networks, decision trees, and random learning methods were employed to predict energy consumption in those cities, demonstrating improved energy consumption predictions compared to non-AI-based approaches.

In Becvar *et al.* paper's [22], it was found that predicting channel quality using machine learning, leveraging network correlations, proved efficient in reducing overall expenses compared to the traditional pilot-based approach, exceeding 90%. It's noteworthy that the study network includes a large number of nodes that communicate with each other. Yet, another study Torres-Alvarado *et al.* [23] emphasized the importance of adopting machine learning algorithms to predict channel quality (low or high) for IoT networks, where authentication processes are affected by noise and radiation (associated with channel quality), especially when implemented in hardware (such as cognitive radio devices). According to their experiments, the random forest algorithm achieved the highest classification accuracy of 95.54%.

In our presented research, we seek to preserve service quality with both its key elements via a two fold strategy. Firstly, we utilize a modified IdM to enhance cybersecurity. Secondly, we adopt AI techniques to predict communication quality. This is coupled with monitoring energy levels and queuing delays at access points to efficiently manage the energy resource in IoT devices. This will be achieved without adversely impacting latency, recognizing it as a critical criterion for time-sensitive applications. This paper is structured as follows: the proposed algorithm presented in section 2, In section 3, discussion and results. Finally, section 4 concludes our paper.

2. THE PROPOSED ALGORITHM

In this section, it is essential to review the key points upon which our research proposal is based, aiming to achieve the research goal, before delving into the detailed operational mechanisms (as outlined in the flowchart review). The foundational aspects of the work are divided into two parts according to its objective.

2.1. Fundamentals of resource management mechanism

In this research, we rely on several key points to accomplish our work. Due to the limited resources of IoT devices, effective resource management translates to enhancing the quality of service provided to network users. In our proposed algorithm, the focus is directed towards the limited energy resource and how to efficiently utilize it while employing Wi-Fi as a means of data exchange. This includes considering the potential delays introduced by energy-saving measures and mitigating their impact on time-sensitive applications. In the following argument, we will review the mathematical models employed to check both parameters. Moreover, we will identify the machine learning algorithm that will contribute to enhancing energy efficiency by encouraging the wireless card to enter a sleep mode when the channel quality is poor.

2.1.1. Power consumption model

The proposed approach depends on predicting connection quality while concurrently monitoring network load directed towards the activated IoT device in power-saving mode (i.e., when it is in sleep mode) facilitated by Wi-Fi. However, such prediction and monitoring are contingent on the device remaining power capacity. It is crucial to emphasize that the algorithm necessitates dependence on a mathematical model to compute the wireless card's power consumption, as defined by (1) [24].

$$P_{avg} = \frac{P_{Tx} * T_{Tx} + P_{Rx} * T_{Rx} + P_I * T_I + P_S * T_S}{T} \quad (1)$$

As it is revealed by the former equation, the lifetime of the wireless card stays in each of its operating modes (transmitting T_{Tx}), receiving T_{Rx} , idle T_I , and sleeping T_S) is multiplied by the basic power consumption value of the mode (transmitting mode P_{Tx} , receiving mode P_{Rx} , idle mode P_I , and Sleeping mode P_S),

gives a simplified model for calculating consumption, noting that the symbol T indicates the simulation time (the sum of the presence times in the operating modes).

2.1.2. Average delay

The proposal did not overlook the nature of the transmitted data, taking into consideration the existence of two types or classifications of data, one of which requires calculating the delay standard, given that it is time-sensitive (as in critical industrial applications). Therefore, the average delay experienced by a data packet destined for an IoT device depends on the power-saving mode provided by Wi-Fi communication technology, with consideration of two factors, one of which is the probability of the packet arriving while the wireless card of the IoT device is in sleep mode Pr_{sleep} , and this leads to a delay in the queue of the access point, considering that notification of its existence (in order to be recovered by the device) will be made only at the beginning of the next beacon period. Not only that, but there is another waiting(delay) that the stored packet suffers from, with the beginning of the beacon period, namely the serving time of the packets that precede it in the queue of the access point $\bar{d}_{|sleep_n}$. Another factor contributing to the calculation of the average delay criterion is the average recovery time of packets stored at the access point by the IoT device, after waking up d_{avg} . Based on the above, the average is given according to (2) (see [25], [26]):

$$DSI_n = Pr_{sleep} * \bar{d}_{|sleep_n} + d_{avg} \quad (2)$$

2.1.3. Communication quality prediction

Machine learning enables systems to offer dynamically learning and enhance performance without being explicitly programmed. There exist both linear and non-linear models for machine learning techniques (see [12]). The random forest classifier was used as part of the proposed algorithm for assessing the quality of network communication, based on two standards. These are: the RSSI by the IoT device, which is a simple hardware standard that can provide an accurate and fast estimate of the quality of communication (see [22]). The RSSI average of an IoT device retrieving data packets from the access point (AP) (which is numbered n packets during the beacon period) is given according to (4) (see [18]):

$$RSSI_{avg} = \frac{\sum_{i=1}^n RSSI_i}{n} \quad (3)$$

Furthermore, there is the standard called packet delivery ratio (PDR), which is a software standard equal to the ratio of the number of packets successfully received by an IoT device (successful receipt necessarily means the recipient sending an acki notification to the sender (which is the access point here)) to the number of packets. Packet j sent by the access point at the beginning of each beacon period and is given according to the relationship as in (4) (see [18]):

$$PDR = \frac{\sum_{i=1}^n ack_i}{\sum_{j=1}^m packet_j} \quad (4)$$

2.2. Fundamentals of security-related operational mechanism

The research objective is to achieve service quality in IoT networks, and true service quality cannot be attained without considering the security aspect of the network. The proposed algorithm relies on the concept of IdM system to execute authentication and access authorization operations, yet the adopted system is a modified one.

2.2.1. The used identity management system

The modified IdM system adopted in the proposed algorithm depends basically on two fundamental points. Firstly: using contextual parameters that distinguish the user (such as its identity, role, activities, location, whether physical (global positioning system (GPS)) or virtual (internet protocol (IP) address) and the social networks it utilizes, in addition to the type of data that determines the sensitivity of the data), within the user identifiers, in which they will participate in the access control mechanism. Secondly: encryption of the transmitted data at two levels using two encryption keys key encryption key (KEK) (encrypts the content of messages exchanged during the session), and MKK (key encryption KEK), where the ANSI X.9.17 standard is used to manage the distribution of keys (see [10]). In accordance with what have been discussed, an IoT device should implement two programmed modules (see [8]): i) the context unit, composed of two sub-modules. One sub-module deals with identifiers and utilizes them within an algorithm that filters response content to serve the

request. The other sub-module focuses on constructing identifiers based on requests from users or IoT device users; and ii) the privacy unit, responsible for sending requests and receiving responses subject to authentication and authorization processes through dedicated servers external to the IoT network (the crucial point here is the offloading of privacy policy burdens from the IoT device, contrary to the study), in addition to the required encryption and decryption operations.

2.3. The proposed algorithm internet of things-quality of service

The energy of the IoT device is considered a vital and crucial resource in the network. It should not be compromised, as preserving it without neglecting service quality is essential to meet the users' expectations. Therefore, we proposed the IoT-QoS algorithm, which operates as follows:

- The algorithm is invoked at the beginning of each Beacon Frame guidance period when the wireless card of the IoT device wakes up and receives the guidance frame. The device utilizes a power-saving mode supported by Wi-Fi technology.
- The algorithm first looks at the device's battery power as the threshold for decision-making in maintaining service quality. Predicting poor connection quality is done using the random forest classifier, relying on the RSSI and PDR metrics or a drop in the IoT device's energy level (P_{IoT}) below the threshold (P_{Thre}). In such cases, the Wi-Fi radio is turned off (transitioning the wireless card to sleep mode), and entering sleep mode for the longest possible period ($Sleep_{max}$) helps extend the device's operational lifespan due to low power consumption in this state. Furthermore, there is a need for packet aggregation for uplink data. The wireless card transitions from sleep mode to an active state when data packets are available in the transmission queue. Failure to aggregate data would result in transmission operations at a low transfer rate (due to poor channel conditions), increasing power consumption.
- If the prediction indicates good connection quality and the device's energy level is higher or equal to the threshold level (P_{Thre}), and there are no stored packets awaiting transmission, the card is put into sleep mode for a duration equal to twice the previous sleep period. This is because data movement on the internet occurs in the form of bursts (see [27]).
- If the IoT device possesses stored data packets at the access point, it will perform the required network transmission and reception operations. Here, a distinction is made based on whether the stored data is a data request (external query) accepted in terms of authentication and authorization (subject to the modified IdM system). In this case, an algorithm is invoked to provide packet fragmentation to reduce the amount of data to be sent according to the request context, relying on contextual information used to isolate users. Yet, if the transferred data is time-sensitive, the average delay of the retrieved packets must be calculated, and the duration of the wireless card's stay in sleep mode is reduced to the minimum value assigned if the imposed time constraint is not met. This condition serves as a real constraint for any delay caused by both data aggregation and entering sleep mode operation.

It is worth noting that the network transmission and reception operations for the mentioned data types are conducted according to a higher access priority to the wireless medium, compared to traditional IoT user data. This is achieved by granting IoT devices applying the proposed algorithm a shorter back-off time than those not using it (traditional devices). The latter applies the binary exponential increase for back-off time (distributed coordination function (DCF) access pattern), while our algorithm relies on linear increase. The proposed algorithm IoT-QoS diagram shown in Figure 2.

3. DISCUSSION AND RESULTS

In this section, we explained the results by using the NS3 simulator [28] to complete the evaluation process according to the parameters shown in Table 1, noting that the training data set is collected from the trace file, which is used to train the random forest classifier, which in turn generates a training model that is used to complete the classification process. According to Figure 3, devices using the proposed IoT-QoS algorithm were able to achieve lower energy consumption than their counterparts relying solely on the standard power-saving mode (IoT), with an increase in both the primary sleep interval and the number of network users. This is a direct result of the algorithm monitoring three parameters: energy levels, the presence of stored packets at the access point, and connection quality. The algorithm utilizes these parameters to achieve energy savings in devices. Additionally, it prioritizes access to the medium, reducing the wireless card's idle time during network contention. This positively affects the device's battery energy.

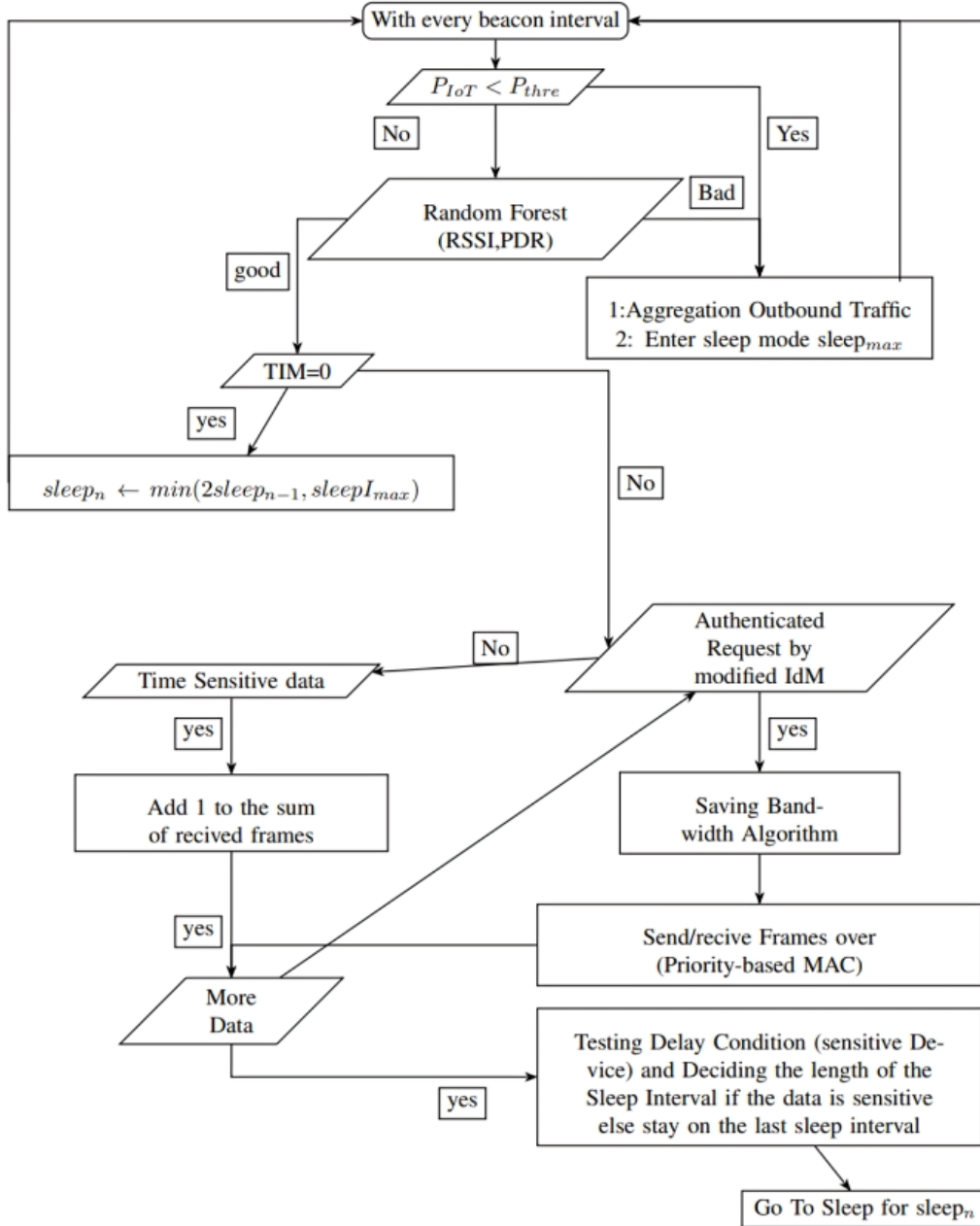


Figure 2. The proposed algorithm IoT-QoS diagram

Table 1. The parameters used in the simulator (NS3)

Parameter	Value
P_{Thre}	0.5 mJ
Transmitting power	1400 mW
Receiving Power	900 mW
Idle power	700 mW
Sleeping power	60 mW
CW_{min}	32
CW_{max}	1024
PSM timeout	25 msec
Max sleep interval	1,000 msec
Simulation time	200 Sec

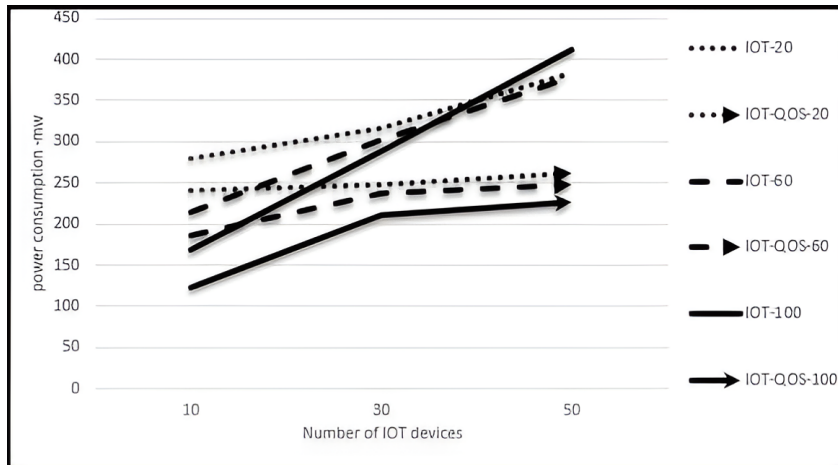


Figure 3. Energy consumption as a function of increasing IoT devices and primary sleep duration (insert link image)

Also, the proposed algorithm distinguishes between two types of data, one of these was subjected to modified authentication processes. The critical network standard for this data type is response time, considering that the additional security system load will affect data transfer time. According to our study, devices implementing the proposed algorithm achieved lower response times than those not using it, even with increased network data traffic, as depicted in Figure 4. This can be justified as the priority access scheme, which plays a crucial role in faster access to the wireless medium. Moreover, the algorithm for providing packet width had a significant impact on adjusting the transmitted information in response to the request context.

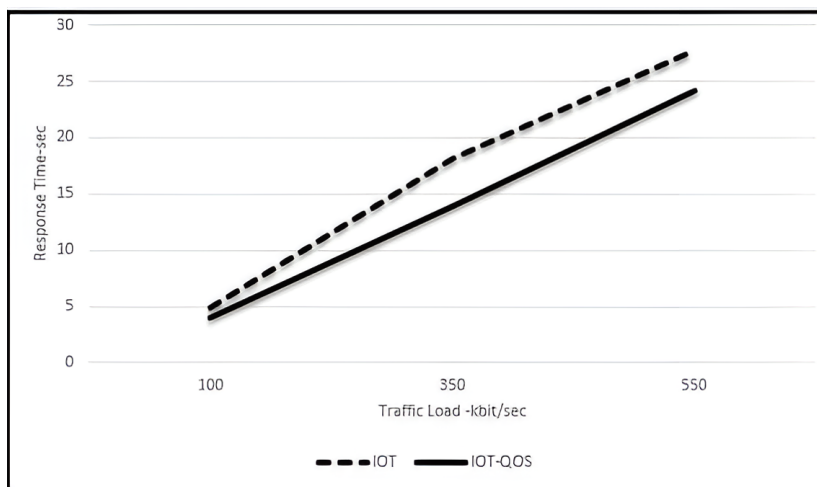


Figure 4. Response time as a function of increasing network load

Hence, the proposed algorithm managed to mitigate the impact of increasing the number of devices in the wireless network on latency, a crucial performance metric for time-sensitive applications. This data type, distinguished as the second type by the IoT-QoS algorithm, is illustrated in Figure 5, where the superiority of the proposal becomes evident, especially under network congestion. This action can be considered a natural outcome of the IoT-QoS algorithm's ability to indirectly reduce congestion levels compared to IoT. This reduction is achieved by predicting the wireless link state through random forest, which forces the wireless card into a sleep state when devices are not in proximity to the access point. In such cases, the card can enter transmission and reception operations at a higher rate with the beginning of each beacon frame period. This effectively reduces both contention time for the wireless medium and the time required for reception operations, resulting in faster data retrieval.

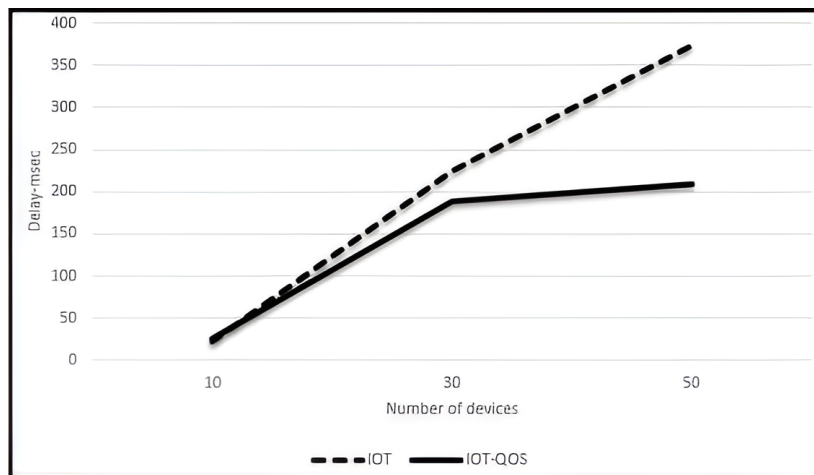


Figure 5. Delay as a function of increasing the number of IoT devices

The results depicted in Figure 6 indicate that the behavior of the proposed IoT-QoS algorithm has an impact on the round trip time (RTT) between an IoT device and the server, especially in the presence of a small number of devices in the network. This led to a decrease in productivity compared to traditional devices. However, the performance of the IoT-QoS algorithm surpasses that of traditional devices under network congestion. This improvement can be attributed to the algorithm's ability to reduce contention time for the wireless medium through the linear access scheme. It allows for transmission operations with improved channel conditions, avoiding the need for retransmission and enabling data transfer at a higher rate. Naturally, putting the wireless card to sleep under poor channel conditions reduces congestion levels, and impacting congestion in one way or another.

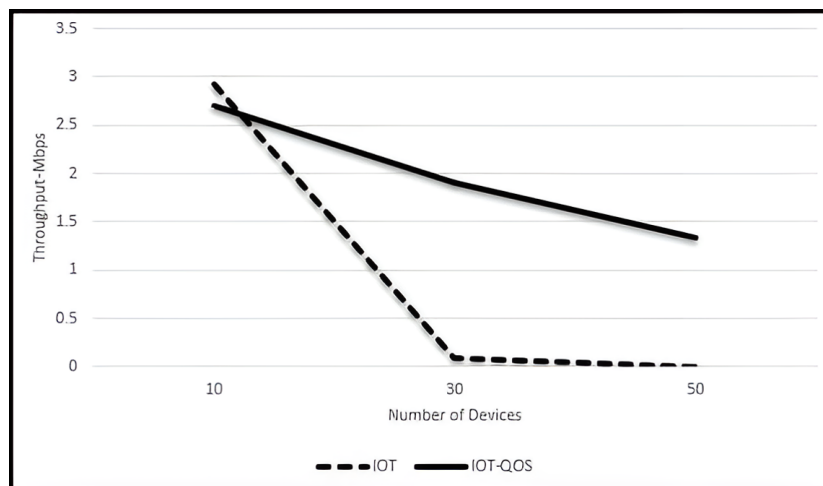


Figure 6. Throughput as a function of increasing the number of IoT devices

4. CONCLUSION

In light of the findings, it is evident that the IoT-QoS algorithm has demonstrated a capacity to enhance the performance of IoT devices utilizing Wi-Fi as their communication medium, all while ensuring the pivotal aspect of security is not compromised. Consequently, a strong recommendation emerges for the adoption of the proposed IoT-QoS algorithm, particularly for IoT devices characterized by constrained resources, notably in power. The algorithm showcases its efficacy by successfully upholding QoS standards while notably diminishing power consumption within the wireless cards of IoT devices operating in congested network environments, thereby outperforming traditional devices in similar conditions. In the future, we seek to enhance the security

aspect of the IoT network. Several research directions may be explored in this regard, including the adoption of blockchain technology for authentication processes. Additionally, there is a growing interest in leveraging AI and software defined networks to detect attacks and make informed decisions to mitigate their impact.





REFERENCES

- [1] D. Bandyopadhyay and J. Sen, "Internet of things: applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, May 2011, doi: 10.1007/s11277-011-0288-5.
- [2] L. Mathy, C. Edwards, and D. Hutchison, "Principles of QoS in group communications," *Telecommunication Systems*, vol. 11, pp. 59–84, 1999, doi: 10.1023/A:1019132914996.
- [3] M. Singh and G. Baranwal, "Quality of service (QoS) in internet of things," in *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, IEEE, Feb. 2018, pp. 1–6. doi: 10.1109/IoT-SIU.2018.8519862.
- [4] R. Duan, X. Chen, and T. Xing, "A QoS architecture for IOT," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, IEEE, Oct. 2011, pp. 717–720. doi: 10.1109/IThings/CPSCoM.2011.125.
- [5] M. S. Bernard, T. Pei, and K. Nasser, "QoS strategies for wireless multimedia sensor networks in the context of IoT at the MAC layer, application layer, and cross-layer algorithms," *Journal of Computer Networks and Communications*, vol. 2019, pp. 1–33, Dec. 2019, doi: 10.1155/2019/9651915.
- [6] S. Pawar *et al.*, "Security and QoS (quality of service) related current challenges in IoT," *International Journal of Electronics and Communication Engineering*, vol. 10, no. 4, pp. 9–20, Apr. 2023, doi: 10.14445/23488549/IJECE-V10I4P102.
- [7] J. Liu, Y. Xiao, and C. L. P. Chen, "Authentication and access control in the internet of things," in *2012 32nd International Conference on Distributed Computing Systems Workshops*, IEEE, Jun. 2012, pp. 588–592. doi: 10.1109/ICDCSW.2012.23.
- [8] C. Chibelushi, A. Eardley, and A. Arabo, "Identity management in the internet of things: the role of MANETs for healthcare applications," *Computer Science and Information Technology*, vol. 1, no. 2, pp. 73–81, Sep. 2013, doi: 10.13189/csit.2013.010201.
- [9] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for internet of things security," in *2014 Euro Med Telco Conference (EMTC)*, IEEE, Nov. 2014, pp. 1–5. doi: 10.1109/EMTC.2014.6996632.
- [10] A. Witkovski, A. Santin, V. Abreu, and J. Marynowski, "An IdM and key-based authentication method for providing single sign-on in IoT," in *2015 IEEE Global Communications Conference (GLOBECOM)*, IEEE, Dec. 2015, pp. 1–6. doi: 10.1109/GLOCOM.2015.7417597.
- [11] M. L. B. A. Santos, J. C. Carneiro, A. M. R. Franco, F. A. Teixeira, M. A. A. Henriques, and L. B. Oliveira, "FLAT: federated lightweight authentication for the internet of things," *Ad Hoc Networks*, vol. 107, p. 102253, Oct. 2020, doi: 10.1016/j.adhoc.2020.102253.
- [12] M. J. M. Al-Saadi and M. Ilyas, "Identity management approach in internet of things (IoT)," in *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, IEEE, Oct. 2020, pp. 1–6. doi: 10.1109/ISMSIT50672.2020.9254470.
- [13] M. A. Bouras, B. Xia, A. O. Abuassba, H. Ning, and Q. Lu, "IoT-CCAC: a blockchain-based consortium capability access control approach for IoT," *PeerJ Computer Science*, vol. 7, p. e455, Apr. 2021, doi: 10.7717/peerj-cs.455.
- [14] V. Dehalwar, M. L. Kolhe, S. Deoli, and M. K. Jhariya, "Blockchain-based trust management and authentication of devices in smart grid," *Cleaner Engineering and Technology*, vol. 8, p. 100481, Jun. 2022, doi: 10.1016/j.clet.2022.100481.
- [15] X. Zhu and Y. Badr, "Identity management systems for the internet of things: a survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, Dec. 2018, doi: 10.3390/s18124215.
- [16] K. M. Sadique, R. Rahmani, and P. Johannesson, "DiDM-EIoT: distributed identity management for edge internet of things (IoT) devices," *Sensors*, vol. 23, no. 8, p. 4046, Apr. 2023, doi: 10.3390/s23084046.
- [17] J. Chen, Y. Liu, and Y. Chai, "An identity management framework for internet of things," in *2015 IEEE 12th International Conference on e-Business Engineering*, IEEE, Oct. 2015, pp. 360–364. doi: 10.1109/ICEBE.2015.67.
- [18] M. L. F. Sindjoun and P. Minet, "Wireless link quality prediction in IoT networks," in *2019 8th International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, IEEE, Nov. 2019, pp. 1–6. doi: 10.23919/PEMWN47208.2019.8986920.
- [19] J. Ma, T. Nagatsuma, S.-J. Kim, and M. Hasegawa, "A machine-learning-based channel assignment algorithm for IoT," in *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC)*, IEEE, Feb. 2019, pp. 1–6. doi: 10.1109/ICAIIIC.2019.8669028.
- [20] P. Lynggaard, "Using machine learning for adaptive interference suppression in wireless sensor networks," *IEEE Sensors Journal*, vol. 18, no. 21, pp. 8820–8826, Nov. 2018, doi: 10.1109/JSEN.2018.2867068.
- [21] M. Zekić-Sušac, S. Mitrović, and A. Has, "Machine learning based system for managing energy efficiency of public sector as an approach towards smart cities," *International Journal of Information Management*, vol. 58, p. 102074, Jun. 2021, doi: 10.1016/j.ijinfomgt.2020.102074.
- [22] Z. Becvar, D. Gesbert, P. Mach, and M. Najla, "Machine learning-based channel quality prediction in 6G mobile networks," *IEEE Communications Magazine*, vol. 61, no. 7, pp. 106–112, Jul. 2023, doi: 10.1109/MCOM.001.2200305.
- [23] A. Torres-Alvarado, L. A. Morales-Rosales, and I. Algreto-Badillo, "A channel-quality classification analysis for IoT communication based on machine learning," in *2021 Mexican International Conference on Computer Science (ENC)*, IEEE, Aug. 2021, pp. 1–4. doi: 10.1109/ENC53357.2021.9534815.
- [24] J. Li, J. Xiao, J. W.-K. Hong, and R. Boutaba, "FSM-based Wi-Fi power estimation method for smart devices," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, IEEE, May 2015, pp. 147–155. doi: 10.1109/INM.2015.7140287.
- [25] D. Jung, R. Kim, and H. Lim, "Power-saving strategy for balancing energy and delay performance in WLANs," *Computer Communications*, vol. 50, pp. 3–9, Sep. 2014, doi: 10.1016/j.comcom.2014.02.005.
- [26] R. Zheng, J. Hou, and L. Sha, "Performance analysis of the IEEE 802.11 power saving mode," in *Proc. CNDS*, 2004, pp. 1–9.





- [27] Y. Xiao, P. Savolainen, A. Karppanen, M. Siekkinen, and A. Ylä-Jääski, "Practical power modeling of data transmission over 802.11g for wireless applications," in *Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking*, New York, NY, USA: ACM, Apr. 2010, pp. 75–84. doi: 10.1145/1791314.1791326.
- [28] K. Wehrle, M. Güneş, and J. Gross, Eds., *Modeling and tools for network simulation*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. doi: 10.1007/978-3-642-12331-3.

BIOGRAPHIES OF AUTHORS



Ali Ahmed Razzaq     had a master's degree in computer network engineering from Andhra University. Now I am a research scholar at Andhra University in the IoT specialty for the purpose of obtaining a Ph.D. He has several skills in the field of artificial intelligence and its programming in the field of networks and design websites by framework django in python. He currently works in the field of air navigation and its systems as a data entry for aviation transit (FDO) in the Iraqi Air Traffic Management Center in the Area Control Center (ACC) and now an air traffic controller at Baghdad International Airport (Iraq). He can be contacted at email: taifali607@gmail.com.



Prof. Kunjam Nageswara Rao     is a Professor in Department of Computer Science and Systems Engineering at Andhra University College of Engineering. He has more than 24 years of teaching experience. He has published 3 patents and more than 50 research papers so far in various highly reputed international journals. His research interest includes cloud computing, wireless networks, sensor networks, IoT, bioinformatics, medical image processing, network security, data mining and data analytics. He can be contacted at email: kunjamnag@gmail.com.