International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 31, No. 3, March, 2026, pp. 773-780
Journal homepage: http://iieta.org/journals/isi

Energy-Aware Blockchain-Enabled Hybrid Protocol for Fast and Reliable Packet Delivery in Wireless Sensor Networks

Mohanad Ali Meteab Al-Obaidi[1*], Shajan Mohammed Mahdi[2], Zahraa Jawad Kadhim[3]

[1] Department of Computer Science College of Science, Mustansiriyah University, Baghdad 10045, Iraq
[2] Department of Computer, College of Education, Mustansiriyah University, Baghdad 10045, Iraq
[3] Information Technology Center, Mustansiriyah University, Baghdad 10045, Iraq

Corresponding Author Email: neros2210@uomustansiriyah.edu.iq

https://doi.org/10.18280/isi.310311

Received: 3 October 2025
Revised: 5 January 2026
Accepted: 16 March 2026
Available online: 31 March 2026

Keywords:
time division multiple access, code division multiple access, PoA/PBFT-lite, media access control, wireless sensor network, block chain

ABSTRACT

Wireless sensor network protocols with limited power resources seek access mechanisms to ensure network efficiency and scalability. Both time division multiple access (TDMA) and code division multiple access (CDMA) have provided partial solutions. While TDMA provides collision-free scheduling under dynamic traffic, it wastes power resources. While CDMA supports parallel transmissions, it ignores processing costs and interference, resulting in loss of access control for verification processes, exposing the network to channel fragmentation. In this paper, we leverage TDMA and CDMA to produce a hybrid protocol that combines the features of structured slots and parallel tokens, along with a lightweight blockchain framework (PoA/PBFT-lite) for verifying slot and token assignments. This ensures fast and secure packet access at the lowest possible cost, increasing network reliability and performance. 500 randomly distributed sensor nodes were used to conduct simulations over an area of 500 square meters. Simulation results showed that the proposed algorithm reduced the average access time to 110 ms, compared to 220 and 180 ms for both traditional TDMA and CDMA protocols, while increasing the packet delivery rate to 97.8% and the data transfer rate to 260 kbps. Simulation results also showed an improvement in energy reduction of 0.25 J per node, in addition to improving the network lifetime to 1280 and 2120 cycles for the first and last nodes, respectively. The results demonstrate the proposed approach as a promising method for sensor networks, demonstrating its scalability and robustness.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are a technological revolution in the world of modern spatially distributed applications that monitor physical conditions or the environment, healthcare, industrial and agricultural automation, and smart cities [1, 2]. Despite their wide application scope, they are limited by the limited computing power and energy of each sensor node. Designing strategies for dynamic traffic patterns and delivering them in a timely and reliable manner is a major concern in WSN research [3].

The media access control (MAC) layer plays a critical role in network performance by regulating the mechanisms for multiple network nodes to share the wireless channel. On the other hand, TDMA-based protocols provide collision-free scheduling of data transfer between nodes and improved energy efficiency, but suffer from resource waste when traffic is unpredictable. CDMA-based approaches offer the advantages of parallel transmission and more efficient channel utilization. Despite these distinct advantages, each mechanism suffers from high processing costs when data volume is large [4]. Neither protocol alone is sufficient to achieve network scalability, improved latency, and rapid deployment. Additional factors—such as security, trust, retransmission, and frequency of data collisions—add complexity to the design of WSNs. Traditional MAC protocols have difficulty verifying secure data access [5, 6].

Blockchain has recently been explored for IoT and WSN security, but most implementations target routing or application layers, leaving the MAC layer underexplored. Moreover, full-scale blockchain systems are unsuitable for energy-constrained nodes due to high computation and communication overhead [7-9].

This paper addresses latency, energy, throughput, and network reliability together by presenting the problem and solution within a common framework. Previous research has either studied TDMA-CDMA-based hybrid MAC protocols without considering blockchain integration [10, 11], or adopted blockchain-enabled MAC mechanisms without a hybrid TDMA-CDMA approach [12]. Furthermore, recent studies have demonstrated that blockchain integration with sensor networks within the IoT ecosystem has been extensively discussed at higher protocol layers, while MAC studies have rarely focused on blockchain-based integration [13, 14]. These reasons highlight a clear research gap, which this paper seeks to fill.

1.1 Problem statement

Current WSN deployments often experience high latency, reduced throughput, and premature energy depletion caused by inefficient medium access strategies and redundant retransmissions. Traditional TDMA-based systems lack flexibility in adapting to dynamic traffic loads, leading to idle slots and wasted resources, whereas CDMA-only systems suffer from processing overhead and interference when the number of simultaneous transmissions grows. Furthermore, the absence of a secure and verifiable mechanism for slot and code allocation makes the system vulnerable to misbehavior or malicious nodes that disrupt fair channel access. These challenges collectively degrade network reliability and hinder the ability of WSNs to support latency-sensitive applications.

1.2 Contribution statement

This paper introduces an integrated MAC-layer approach to combine hybrid TDMA-CDMA scheduling with a low-weight blockchain based verification of WSNs. The proposed system combines two areas of research, which have previously been treated independently; namely, performance and security in order to provide both secure and reliable MAC layer access within one framework.

The main contributions include:

1. A hybrid TDMA/CDMA scheduling method that increases the efficiency of the use of the communication channels and decreases the latency using CDMA transmission, because it allows for multiple transmissions at once during defined time slots.
2. An extremely light weight version of a PoA/PBFT validation (PBFT-lite) is provided to validate slot allocations fairly and securely while minimizing overhead.
3. Adaptive selection of CDMA codes for scalable allocation and reduced power consumption.
4. Simulation examples show significantly better performance regarding latency, throughput, reliability and network lifetime than other conventional MAC layer protocols.

2. RELATED WORK

Existing research related to MAC protocols for WSNs, has focused primarily on three general categories of approaches; namely, (1) Optimization of TDMA / CDMA based MAC protocols, (2) Hybrid MAC Schemes, and (3) Blockchain enabled solutions.

Although each category addresses some network performance issues, none of them have addressed all the potential limitations of wireless sensor networks simultaneously.

TDMA based approaches [15, 16], allow for collision free communication by structuring the schedule for communications. These types of approaches suffer from poor channel utilization when the network is experiencing dynamic changes in traffic patterns as many nodes will often have idle time slots. On the other hand, CDMA based techniques [17], allow multiple nodes to transmit in parallel and thus increase throughput. However, they also result in increased computational requirements and interference under high network loads. The two above described approaches highlight a basic trade off between structured access efficiency and ability to support multiple simultaneous transmissions.

Hybrid MAC protocols were developed to help bridge this trade off. Examples of such hybrid MAC protocols include those proposed by Utama et al. [18], which are designed to be adaptable and capable of providing Quality of Service. However, both of these approaches continue to have significant residual collision problems and no mechanism for securely validating node access to the network at the MAC Layer.

There have been recent explorations of using block chain technology to increase trust and security in WSNs and Internet of Things (IoT) Systems [19-23]. These technologies offer a number of advantages including enhanced data integrity and reliability. They typically operate at higher levels than the MAC Layer in the Network Protocol Stack and therefore may introduce additional processing and communication overhead which could limit their utility in resource constrained environments where operating efficiently at the MAC Layer is critical.

The major reason that there are few methods currently available to support efficient use of channels in large-scale WSN systems is because current methods do not provide a method to efficiently utilize all channels, provide low latency or be scalable. Therefore, given the shortcomings of existing solutions it would be beneficial to develop a hybrid TDMA-CDMA protocol with an associated lightweight blockchain validation mechanism, as summarized in Table 1.

Table 1. Comparison of related work and proposed protocol

Ref.	Main Idea	Limitations	Proposed Hybrid Protocol
[15]	TDMA slot scheduling for collision-free access	Idle slots under low traffic, limited adaptability	Structured slots combined with adaptive CDMA codes
[16]	CDMA-based parallel transmissions	Processing overhead and interference under heavy load	Parallelism maintained with blockchain validation
[17, 22]	CSMA/CA and hybrid MAC with adaptive duty cycle	Collisions persist, QoS not fully ensured	Collision-free scheduling with secure validation
[18, 21]	Blockchain integration for MAC/IoT security	High computational and communication overhead	Lightweight PoA/PBFT-lite with minimal energy cost
Proposed	TDMA + CDMA + Lightweight Blockchain		Reduced latency, higher throughput, extended lifetime

3. PROPOSED METHODOLOGY

The proposed methodology introduces a hybrid medium access strategy that combines the advantages of TDMA and CDMA with a lightweight blockchain framework to improve packet delivery speed, reliability, and energy efficiency in large-scale WSNs. The design is structured into four main components: the network model, hybrid MAC scheduling, blockchain integration, and the operational workflow. To summarize the operational details of the proposed design, the complete hybrid procedure is expressed in algorithmic form. The algorithm outlines how node reports are collected, how TDMA slots and CDMA codes are assigned, how validators confirm allocations through a lightweight blockchain consensus, and how trust values are updated adaptively. This representation provides a clear step-by-step workflow that connects the conceptual design to its practical execution. The algorithmic steps are presented in Algorithm 1.

Algorithm 1. Hybrid TDMA–CDMA scheduling and blockchain-based verification procedure

Input: N nodes, S TDMA slots, K max CDMA codes per slot, validator set V
Output: Verified allocation map M: Node → (s, k)
1. Each node reports residual energy and traffic demand to its cluster head.
2. Scheduler aggregates reports and assigns TDMA slots to clusters.
3. Within each slot, allocate up to K CDMA codes to active nodes.
4. Broadcast allocation map M to validators.
5. Validators run lightweight consensus (PoA / PBFT-lite).
 • If accepted → record M on blockchain.
 • Else → request re-scheduling.
6. Nodes transmit packets in assigned slots and codes.
7. Receivers verify timing and code against blockchain record.
8. Update node trust values and adjust K adaptively.

The operational sequence of the proposed scheme is further illustrated in Figure 1, which provides a visual flow of the steps summarized in Algorithm 1.

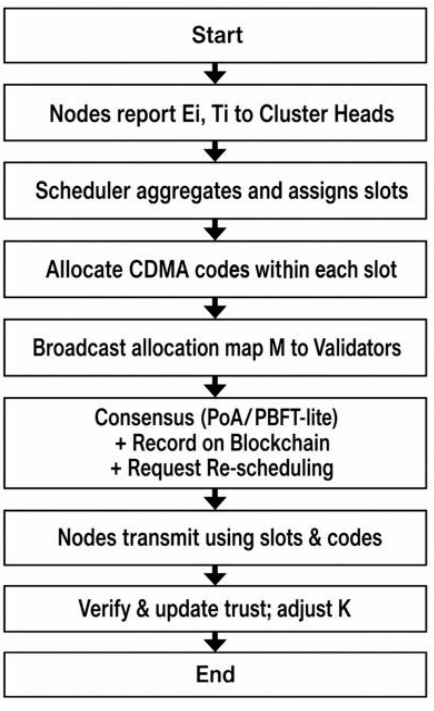

Figure 1. Algorithm steps

4. NETWORK MODEL

The network under consideration consists of 500 sensor nodes randomly deployed within a 500 × 500 m² area. Each node is initially equipped with limited energy resources and has identical communication and sensing capabilities. A centralized base station is positioned to collect aggregated data from the nodes. The adopted radio energy model follows the conventional parameters in WSN research, where the energy required for transmission and reception depends on packet size, distance, and channel conditions. Dynamic deployment is assumed, meaning that the load distribution and activity patterns of nodes vary across simulation rounds.

4.1 Hybrid media access control scheduling (TDMA + CDMA)

The proposed media access scheme relies on TDMA technology to divide the super-frame into multiple time slots, each allocated to a different sensor group. Within each time slot, CDMA spreading codes transmit simultaneously to multiple nodes without collisions. This two-layer mechanism leverages the orderly scheduling of TDMA for orderly access and the parallelism of CDMA, which increases throughput. It is especially effective when the number of distribution codes per time slot (k) is adjusted based on the network density and traffic congestion between nodes. The hybrid design enhances the time intervals, reduces idle periods and overall access time.

4.2 Lightweight blockchain integration

The blockchain layer was incorporated at the MAC layer to enable verifiable and secured Medium Access Control in a very low-cost manner. Cluster heads serve as validators that verify slot and CDMA Code assignments. When the super-frame begins, the scheduling map M, which contains node ID's, slot ID's, and CDMA code, is sent to the validator set.

Once an agreement has been made through a lightweight consensus algorithm such as Proof of Authority or PBFT-Lite, a new block is created.

This block will contain all verified allocation records. Each node in the network can use this block as a trusted reference when verifying whether they have a right to transmit on their assigned slots. As such, this method ensures there are no unauthorized slot occupations, and each node has fair access.

In order to be energy efficient, the blockchain layer uses a minimum number of bytes for each Block, and only generates blocks for events related to scheduling. Therefore, the computational overhead, and communication overhead associated with the blockchain layer are both reduced.

Cluster heads are used instead of every sensor Node in the network because it is assumed that cluster head nodes will have enough resources (computational power, storage space etc.) to handle the increased workload. Also, since consensus is achieved within two rounds, it is efficient even in resource constrained wireless sensor networks.

4.3 Operational workflow

The hybrid algorithm proposes a sequential approach. Wireless sensor nodes broadcast their available power and access path to cluster heads, and slots and tokens are allocated using a scheduled hybrid TDMA/CDMA protocol. The allocation is then authenticated and stored on lightweight blockchain blocks. Data is then transferred in parallel, and packet size is verified after each round to ensure secure and efficient access. Trust metric records are updated after each round. This hybrid protocol is characterized by its efficiency in improving energy consumption, scalability, and increased reliability.

4.4 Algorithmic workflow

The proposed hybrid TDMA-CDMA protocol, integrated with a lightweight blockchain framework, regulates the arrival of data packets while ensuring continuous reliable verification after each round. The workflow is divided into six stages, as follows:

• Network Sensing and Status Collection

All sensor nodes monitor transmission requests, the remaining energy, and periodically check the efficiency of the communication channel, and inform the cluster head.

• Slot and Hybrid Code Scheduling

Based on the metrics collected within each slot, TDMA slot tables and CDMA code allocations are dynamically updated to ensure balanced usage and minimize idle periods.

• Blockchain Verification and Recording

To prevent slot misuse and maintain transparency of access control, the validity of slot schedules and token allocations is verified, and the verified results are stored in a blockchain ledger.

• Parallel Data Transfer

The active superframe handles the transmission of data packets in parallel, leveraging CDMA encoding and TDMA tables to prevent collisions and support multiple simultaneous transmissions.

• Trust Verification and Update

The cluster heads certify the integrity of packets, timing, and validity of tokens and blockchain records. This authentication improves transmissions.

• Adaptive Adjustment

At the end of each round, performance metrics—such as slot usage, token overlap, and power consumption—are evaluated to save energy, maintain throughput, and enhance security.

4.5 Mathematical power model

This section reviews the basic mathematical equations used for power consumption, latency, throughput, and trust in the proposed TDMA-CDMA-Blockchain hybrid protocol. Below is Table 2 of the symbols used in these equations.

1. Transmission Energy

In equation, L = packet length (Bits), d = transmission distance (Meters), E_{elec} = energy consumed in transmitter/receiver circuitry, ϵ_{fs} = amplifier energy for free space channel model ϵ_{mp} = amplifier energy for multipath channel model d_0 = threshold distance for using channel models to determine the channel model for a data packet.

$$E_{tx(L,d)} = \frac{L\left(E_{elec} + \varepsilon_{fs} \cdot d^2\right), d < d_0}{L\left(E_{elec} + \varepsilon_{mp} \cdot d^4\right), d \geq d_0} \tag{1}$$

2. Reception Energy

$$E_{rx(L)} = L \cdot E_{elec} \tag{2}$$

where, E_{rx} represents the energy consumed for receiving a packet of length L.

3. Latency

$$T_{delay} \approx \frac{T_{sf}}{S \cdot K} \tag{3}$$

where, T_{sf} is the super-frame duration, S is the number of TDMA slots, and K is the number of CDMA codes per slot.

4. Throughput

$$Th = \frac{S \cdot K \cdot L}{T_{sf}} \tag{4}$$

where, Th denotes the network throughput.

5. Trust Update

$$T_{i(t+1)} = \alpha \cdot T_{i(t)} + \beta \cdot S_{i(t)} - \gamma \cdot F_{i(t)} \tag{5}$$

where, T_i represents the trust value of node i, and S_i and F_i denote successful and failed transmissions, respectively.

Table 2. Notation summary

Symbol	Description
L	Packet length (bits)
d	Distance (m)
E_{elec}	Electronics energy (J/bit)
ε_{fs}	Free-space amplifier energy (J/bit/m²)
ε_{mp}	Multipath amplifier energy (J/bit/m⁴)
d_0	Threshold distance (m)
T_{sf}	Superframe duration (s)
S	Number of TDMA slots
K	Number of CDMA codes per slot

5. SIMULATION SETUP

The performance evaluation of the hybrid protocol was performed through simulations using MATLAB and NS-3 for randomly distributed network nodes. The simulation parameters are summarized in Table 3.

Table 3. Simulation parameters

Parameter	Value/Description
Simulator	MATLAB / NS-3
Number of Nodes	500
Network Area	500 × 500 m²
Initial Energy	0.5 – 1.5 J per node
Packet Size	2000 bits
Transmission Range	Adjustable
Superframe Structure	TDMA slots with CDMA codes per slot (k)
Evaluation Metrics	Latency, PDR, Throughput, Energy Consumption, Network Lifetime (FND/HND/LND), Blockchain Overhead

Additional simulation scenarios are being considered in order to evaluate this study as completely as possible. A number of variables that affect the network have been tested; the numbers of sensors are being varied for different network densities (for example, 200, 350, and 500 sensors); different traffic scenarios have been used to simulate low, medium, and high traffic conditions; and, the numbers of CDMA codes per TDMA time slot (K) have been varied to examine their effects upon performance and scalability.

To enhance the quality of results of the simulation, several runs were performed under the same conditions, and the reported values are the average results.

6. RESULTS AND ANALYSIS

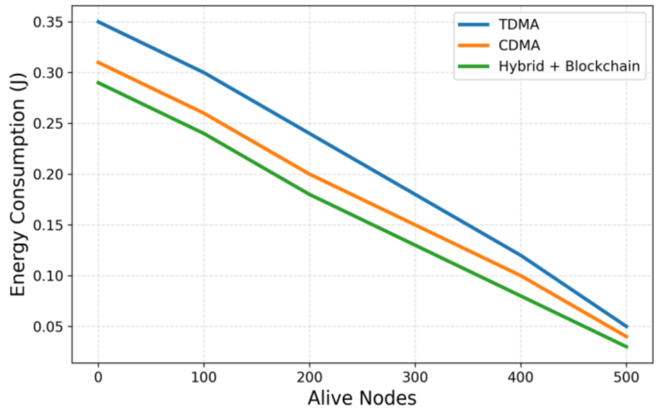

Figure 2. Energy consumption vs. alive nodes

Table 4. Performance comparison of media access control (MAC) protocols

Metric	TDMA	CDMA	Hybrid (No BC)	Hybrid + BC
Avg. Latency (ms)	220	180	120	110
PDR (%)	91.2	93.5	95.0	97.8
Throughput (kbps)	145	172	210	260
Energy (J)	0.34	0.31	0.27	0.29
FND (rounds)	980	1020	1150	1280
HND (rounds)	1450	1510	1650	1780
LND (rounds)	1890	1930	2000	2120

As can be seen from Figure 2, there is a direct correlation between the amount of energy consumed in the system, and the number of functioning nodes present within it. With the advancement of time in terms of the network's operational life cycle, as nodes begin to fail, they place greater amounts of burden upon their neighbors through increased communications. These findings are supported by the data provided in Table 4. The hybrid method that does not include the use of blockchain was found to have utilized less power than both methods (hybrid - blockchain; hybrid). Therefore, the hybrid - blockchain method utilized approximately 8% more power than the hybrid method. However, the increase in the amount of power required for the hybrid and blockchain approach is minimal when compared to the performance advantages realized through its implementation. Additionally, this can be explained because in addition to the existing overhead from validating transactions, the consensus process also consumes additional resources. Although the implementation of PBFT-Lite or Proof-of-Authority (PoA) provides lower computational requirements than other blockchains, these implementations provide less complex operations that support the resource-constrained nature of WSNs. Thus, it has been determined that the proposed lightweight consensus mechanism is suitable for WSN systems that operate under extremely limited resources. Hence, the hybrid and blockchain methodology presents a viable balance between achieving improved system performance while maintaining energy conservation.

The results given are all average simulation results, which give a consistent performance comparison of the tested protocols.

6.1 Latency comparison

The Hybrid TDMA-CDMA using Blockchain consistently achieves the lowest latency compared to TDMA and CDMA (as illustrated by Figure 3) due to the combination of structured TDMA scheduling and parallel CDMA transmissions that reduce wait times and minimize channel contention.

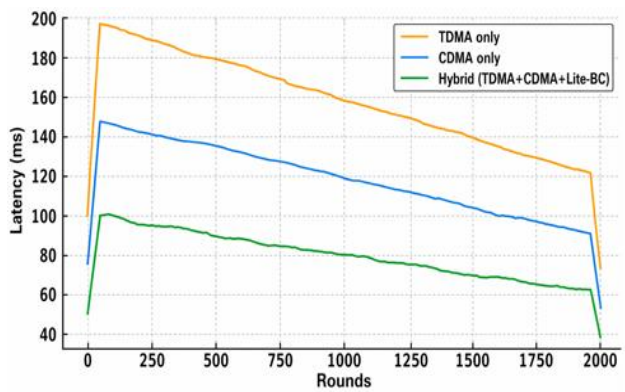

Figure 3. Latency of hybrid TDMA–CDMA -blockchain
Note: TDMA= time division multiple access; CDMA = code division multiple access.

Furthermore, the use of blockchain for validating transactions reduces the chance of transmission collisions and unauthorized access; therefore, it decreases retransmission opportunities, leading to additional reduction in delay. Overall, this provides an even faster and more dependable method for delivering data when the network environment is constantly changing.

6.2 Packet delivery ratio

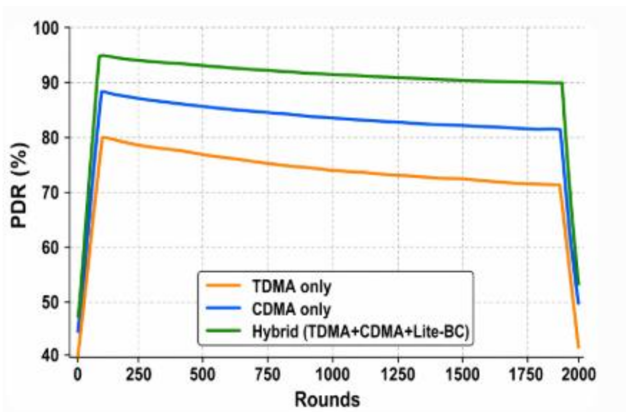

Figure 4. Packet delivery ratio

The hybrid TDMA-CDMA with blockchain shows the best performance in terms of packet delivery ratio (PDR) as depicted in Figure 4. The improvement in terms of PDR was due to the combination of the structured TDMA schedule and the use of multiple CDMA code channels for parallel transmission. With these two mechanisms combined, the number of competing packets for access to the wireless channel is reduced. Consequently, the probability of packet collision during reception is also decreased. In addition, the verification mechanism based on blockchain technology prevents unauthorized nodes from accessing their designated time slot or using their allocated code. Therefore, the amount of packet loss resulting from an uncooperative node intentionally interfering with other nodes' receptions is minimized. Ultimately, the proposed system achieves a PDR near 98% with improved robustness and reliability when operating in a highly dynamic environment.

6.3 Throughput analysis

The Hybrid TDMA-CDMA with Blockchain reaches throughputs greater than 250 Kbps, far out performing both TDMA and CDMA protocols as shown in Figure 5. The improvement comes from the use of CDMA based multi-node (simultaneous) transmission within every TDMA slot.

Further, the validation process implemented using blockchain reduces re-transmission caused by unauthorized node access or conflicting transmission. Thus, increasing the effective data delivery rates. In conclusion, this proposed protocol can achieve increased throughput and increase resource usage efficiency for networks operating at different levels of traffic.

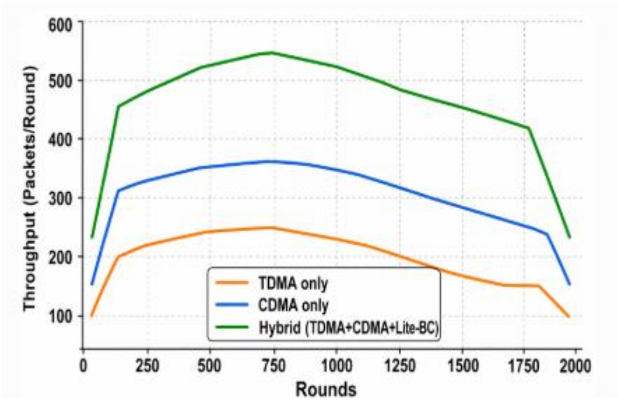

Figure 5. Throughput analysis

6.4 Energy consumption

A hybrid scheme requires less energy than both TDMA and CDMA (per transmission), since it allows for lower retransmission counts and has better slot utilization. In Figure 6, we compare the total amount of energy consumed by each protocol across multiple rounds in a simulated scenario.

From our experimentations, it is evident that the Hybrid TDMA-CDMA with Blockchain consumes the least amount of energy when comparing all of the other schemes. Even though an added overhead from the Blockchain is introduced through validations and consensus mechanisms, the cost savings from reduced retransmissions, and increased efficiency due to coordinated medium access control significantly offsets this. Therefore, the proposed mechanism is able to improve network performance while at the same time maintain low-energy consumption.

The results show that there was an increased in energy usage of the hybrid protocol from using blockchain compared to not having blockchain; nonetheless, it still is acceptable when you consider the increase in the level of reliability and security. The comparison indicates that the energy consumption after implementing blockchain has slightly increased because of the extra validation operations.

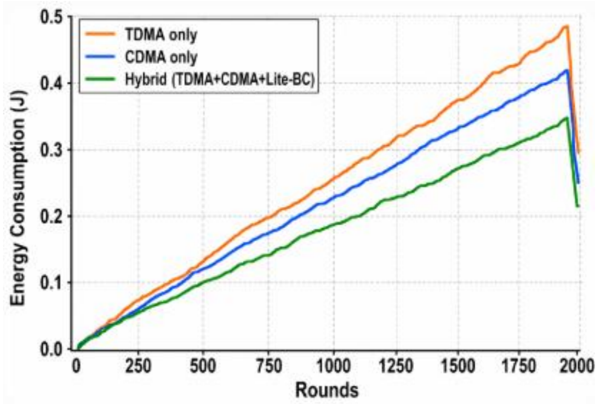

Figure 6. Energy consumption

6.5 Network lifetime

The hybrid TDMA-CDMA using Blockchain has an increased number of rounds that network can live for, i.e. it is significantly longer than TDMA and CDMA. For example, the time at which the first node died was after round 1280 whereas the last surviving node survived until round 2120 as demonstrated by the data presented in Figure 7.

These extended lifetimes are due to the fact that all nodes have equal power consumptions (i.e., are evenly powered), and this is accomplished by means of effective TDMA scheduling and parallel use of CDMA transmission schemes; both of these approaches reduce the overhead of communication operations, thus preventing premature energy exhaustion on overloaded nodes. Additionally, the validation mechanism based upon blockchain reduces the amount of unnecessary retransmission that would be needed if there were no such mechanisms in place. This validation mechanism also prevents unfair competition amongst nodes for limited access to the network's resources, allowing the network to operate for longer periods of time.

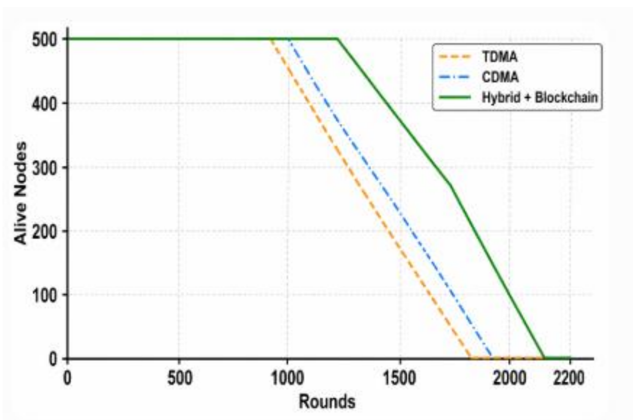

Figure 7. TDMA, CDMA and hybrid network lifetime

Note: TDMA= time division multiple access; CDMA = code division multiple access.

7. DISCUSSION AND CONCLUSION

This section presents the major outcomes from combining an innovative TDMA/CDMA hybrid wireless access protocol with a simple blockchain. A comparison of the various aspects of the performance (i.e., latency, reliability, throughput, energy consumption and network life) will be performed to provide evidence that the combination of both technologies has improved upon existing protocols. Finally, this section will describe the practical applications of the proposed solution as well as the conclusions obtained from the study and possible paths for further research.

7.1 Discussion

As summarized in Table 4, the proposed hybrid TDMA–CDMA scheme supported by a lightweight blockchain achieves consistent improvements over conventional MAC protocols. The integration of slot-based scheduling with code-based parallelism reduces delay and enhances throughput, while blockchain validation ensures fairness and prevents unauthorized access. These combined features result in lower energy consumption and a longer operational lifetime, confirming the practical advantage of the design for large-scale WSN deployments.

7.2 Conclusion and future work

This work presented a blockchain-enabled hybrid MAC protocol that unifies the strengths of TDMA and CDMA to meet the challenges of latency, reliability, and energy efficiency in sensor networks. Simulation results demonstrated notable gains across all major performance indicators, with extended network lifetime and improved communication reliability. Although a minor computational overhead is introduced, the trade-off is justified by the achieved efficiency and robustness. Future research will investigate adaptive scheduling using machine learning, explore ultra-lightweight consensus mechanisms to further reduce blockchain cost, and validate the protocol in heterogeneous IoT/WSN testbeds under real-world conditions.

ACKNOWLEDGMENT

The authors acknowledge the support of Mustansiriyah University (www.uomustansiriyah.edu.iq), Baghdad, Iraq, in facilitating this research.

REFERENCES

[1] Kaur, K., Kaur, A., Sarita, K., Saini, K., Kour, S., Kaur, S. (2024). Emerging applications and ongoing challenges in WSN assisted IoT networks. World Journal of Advanced Engineering Technology and Sciences, 11(2): 501-507. https://doi.org/10.30574/wjaets.2024.11.2.0143

[2] Ali, E., Ashraf, H., Shah, S.S., Abdullah, M., Waseem, Q., Faizan, M., Aleem, M., Adil, M. (2025). Enabling smart and sustainable solutions: Applications of wireless sensor networks in the era of IoT. International Journal of Computational Thinking and Data Science, 5(1): 50-59. https://doi.org/10.37934/ctds.5.1.5059a

[3] Bouazzi, I., Zaidi, M., Usman, M., Shamim, M.Z.M. (2021). A new medium access control mechanism for energy optimization in WSN: Traffic control and data priority scheme. Eurasip Journal on Wireless Communications and Networking, 2021(1): 1-23. https://doi.org/10.1186/S13638-021-01924-4

[4] Jaber, Z.H., Kadhim, D.J. (2022). Medium access control protocol design for wireless communications and networks: Review. International Journal of Electrical and Computer Engineering, 12(2): 1711-1723. https://doi.org/10.11591/ijece.v12i2.pp1711-1723

[5] Obaid, L., Alhashmiy, R., Alsulami, S., Majed, A.N. (2024). Challenges of wireless sensor networks and their solutions. Al-Majllah al-Dawliyah Lil-Hasibat Wa-al-Ma'lumatīyah, 3(10): 102-129. https://doi.org/10.59992/ijci.2024.v3n10p3

[6] Alocious, C., Xiao, H., Christianson, B., Spring, J. (2025). Embedding trust in the media access control protocol for wireless networks. Sensors, 25(2): 354. https://doi.org/10.3390/s25020354

[7] Draz, U., Ali, T., Yasin, S., Hijji, M., Ayaz, M., Aggoune, E.H.M. (2025). Decentralized energy swapping for sustainable wireless sensor networks using blockchain technology. Mathematics, 13(3): 395. https://doi.org/10.3390/math13030395

[8] Jadhav, S.B., Gade, P.S. (2024). Blockchain in IoT security. International Journal for Research in Applied Science and Engineering Technology, 12: 1074-1077. https://doi.org/10.22214/ijraset.2024.59962

[9] Ibibo, J.T. (2023). A systematic review of blockchain solutions for routing protocols in low power and lossy networks. International Journal of Science and Research, 12(9): 1243-1258. https://doi.org/10.21275/sr23910200613

[10] Iglesias-Suarez, F. (2023). TDMA-based MAC protocols designed or optimized using artificial intelligence for safety data dissemination in vehicular ad-hoc networks: A survey. Lecture Notes in Computer Science, 13767: 88-112. https://doi.org/10.1007/978-3-031-36183-8_7

[11] Lee, J., Lee, M. (2023). A blockchain system for tdma-based tactical wireless networks with constrained resources. IEEE Access, 11: 6857-6866. https://doi.org/10.1109/access.2023.3237828

[12] Abyaneh, A.Z., Zorba, N., Hamdaoui, B. (2020). IEEE 802.11ax based medium access design for wireless IoT-blockchain networks. In GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, pp. 1-6. https://doi.org/10.1109/GLOBECOM42002.2020.9348079

[13] Adhikari, N., Ramkumar, M. (2023). IoT and blockchain integration: Applications, opportunities, and challenges. Network Journal, 3(1): 115-141. https://doi.org/10.3390/network3010006

[14] Zainuddin, A.A., Rose Sidi, H.S.H., Shamsudin, M.D.A., Ahmad, K., Abu Bakar, N.A.M., Mohd Sukri, N.S.S., Mustapa, N.S., Mohd Sazali, M.N. (2023). Recent trends of integration of blockchain technology with IoT by analysing networking systems: Future research prospects. Journal of Knowledge Management Practice, 23(1): 46-66. https://doi.org/10.62477/jkmp.v23i1.4

[15] Benrebbouh, C., Louail, L. (2021). Dynamic TDMA for wireless sensor networks. In 2021 30th Wireless and Optical Communications Conference (WOCC), Taipei,

Taiwan, pp. 204-208. https://doi.org/10.1109/WOCC53213.2021.9602892
[16] Anwar, S., Ullah, A., Rocha, Á., Sousa, M.J. (2023). Cluster-based interference-aware TDMA scheduling in wireless sensor networks. In Proceedings of International Conference on Information Technology and Applications, Lecture Notes in Networks and Systems, Springer, Singapore, pp. 449-458. https://doi.org/10.1007/978-981-19-9331-2_38
[17] Mohan, N. (2020). Multi-bearer coordinate grouping-based code division multiple access for data communication in wireless network. The Journal of Supercomputing, 76(8): 6083-6093. https://doi.org/10.1007/S11227-019-03116-W
[18] Utama, S., Seger, I.S., Muhil, S., Din, R., Almaliki, A.J.Q., Almaliki, J.Q. (2024). Analytical and empirical insights into wireless sensor network longevity: The role of MAC protocols and adaptive strategies. Journal of Advanced Research in Computing and Applications, 36(1): 52-60. https://doi.org/10.37934/arca.36.1.5260
[19] Hanggoro, D., Windiatmaja, J.H., Muís, A., Sari, R.F., Pournaras, E. (2024). Energy-aware proof-of-authority: Blockchain consensus for clustered wireless sensor networks. Blockchain: Research and Applications, 5(3): 100211. https://doi.org/10.1016/j.bcra.2024.100211
[20] Vidhya, N., Meenakshi, C. (2025). Blockchain-enabled secure data aggregation routing protocol for IoT-integrated sensor networks. International Journal of Computational and Experimental Science and Engineering, 11(1): 181-194. https://doi.org/10.22399/ijcesen.722
[21] Oh, T. (2025). Blockchain-enabled security enhancement for IoT networks: Integrating LEACH algorithm and distributed ledger technology. Journal of Machine and Computing, 5(1): 483-495. https://doi.org/10.53759/7669/jmc202505038
[22] Asaithambi, S., Ravi, L., Kotb, H., Milyani, A.H., Azhari, A.A., Nallusamy, S., Varadarajan, V., Vairavasundaram, S. (2022). An energy-efficient and blockchain-integrated software defined network for the industrial IoT. Sensors, 22(20): 7917. https://doi.org/10.3390/s22207917
[23] Anand, S., Krishnamoorthy, R., Kumar, U.S., Kamalakkannan, D. (2022). An effective hybrid mobility aware energy efficient low latency protocol for wireless sensor networks. Cybernetics and Systems, 56(6): 1-16. https://doi.org/10.1080/01969722.2022.2157598