IEEE 802.11 based Medium Access Design for Wireless IoT-Blockchain Networks

Graduate Students,

Information and Communication Technologies (ICT)

Arezou Zamanyzadeh Abyaneh, Nizar Zorba

Department of Electrical Engineering, Qatar University, Doha, Qatar

Abstract

Communication is a very basic essence of the blockchain network and must be carefully planned while integrating with IoT, where an extremely large number of devices are interconnected. In this work, blockchain nodes are assumed to use wireless channels to communicate among themselves and other elements of the IoT setup. These communications can be in unicast and broadcast manner where transmission latency and throughput are significant metrics that might jeopardize the overall system. This work is proposing a Medium Access Control (MAC) mechanism addressing these performance metrics and best suitable for wireless IoT-Blockchain system. The proposed MAC protocol is based on the widely used IEEE 802.11 protocol, Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) basic access.

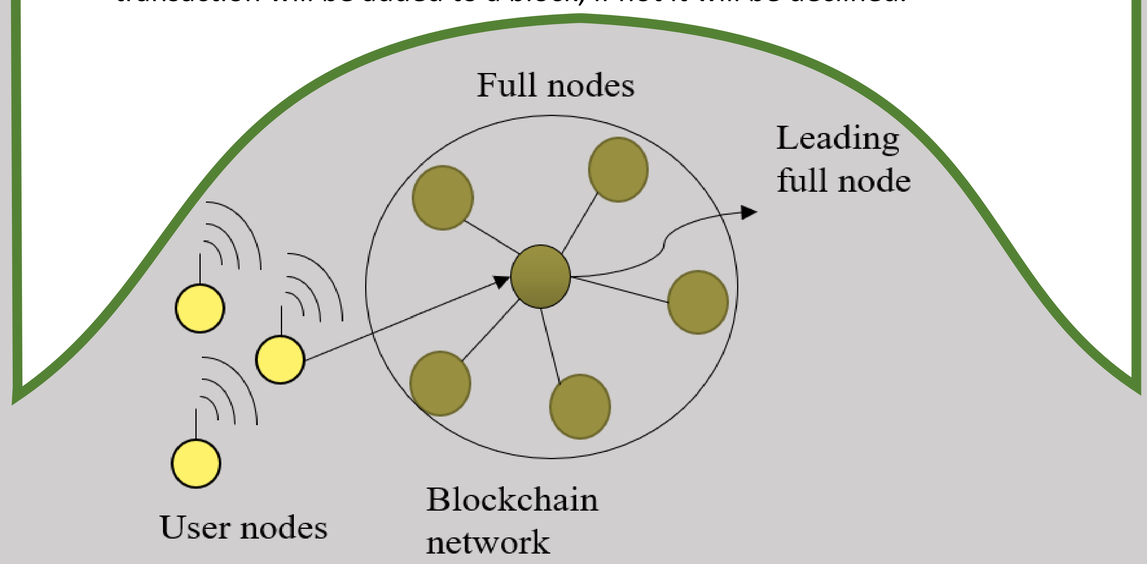
MAC for Wireless IoT-Blockchain

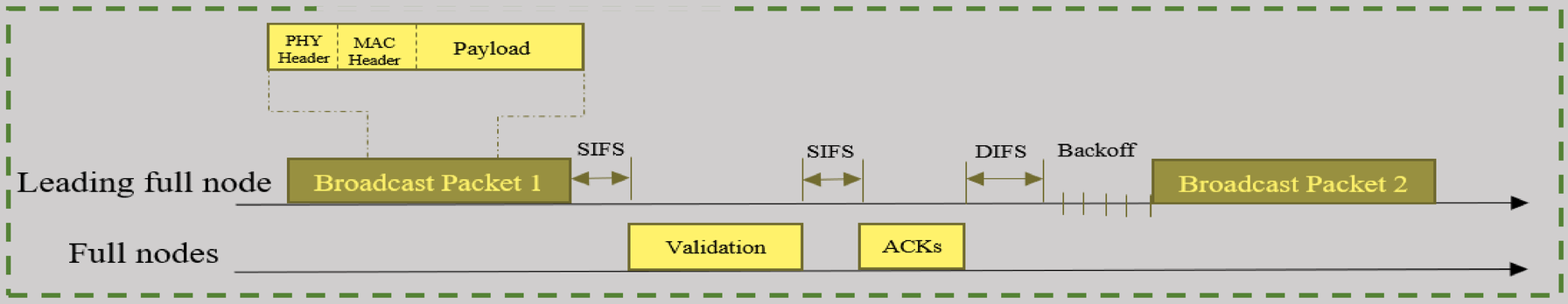
The setup in proposed MAC is controlled by the leading node that has a collection of transactions that it wishes to add to blockchain, and in this case, it will send the transaction through a wireless channel as a broadcast packet. Therefore, after a short interframe space (SIFS), and upon of successful transmission, the full nodes will start the validation process using the consensus protocol, and each node sends back acknowledgment (ACK) frames confirming the validity and safety of the transaction immediately after a SIFS. After successfully receiving all the ACK frames, the leading full node will wait for a period equal to distribute interframe space (DIFS), for guarantee the channel to be idle in order to start a new transmission [2].

Wireless IoT-Blockchain SYSTEM MODEL

The main process to convert a raw data originated from user node (IoT device) into a confirmed block through a full node (blockchain node) is denoted as:

(i) A user node acquires new unsigned transactions
(ii) User node send the transaction to multiple full nodes.
(iii) A full node claims the transactions following the Ethereum protocol
(iv) The leading full node broadcasts the transaction using CSMA/CA to all blockchain nodes to confirm its legitimacy.
(v) If most full nodes validate the transaction following PoS consensus, the transaction will be added to a block, if not it will be declined.





Simulation Parameters

Parameters	Values
Number of nodes	5-100
Packet Payload	[1024,2048,4096,8192]bits
MAC Header	272 bits
Phy Header	128 bits
ACK length	112 bits + PHY header
Transaction Length	64 bits
Verification Time	100 ms
Air Propagation Delay	1 μs
SIFS	28 μs
DIFS	128 μs
Slot Time	50 μs

Mathematical Modeling

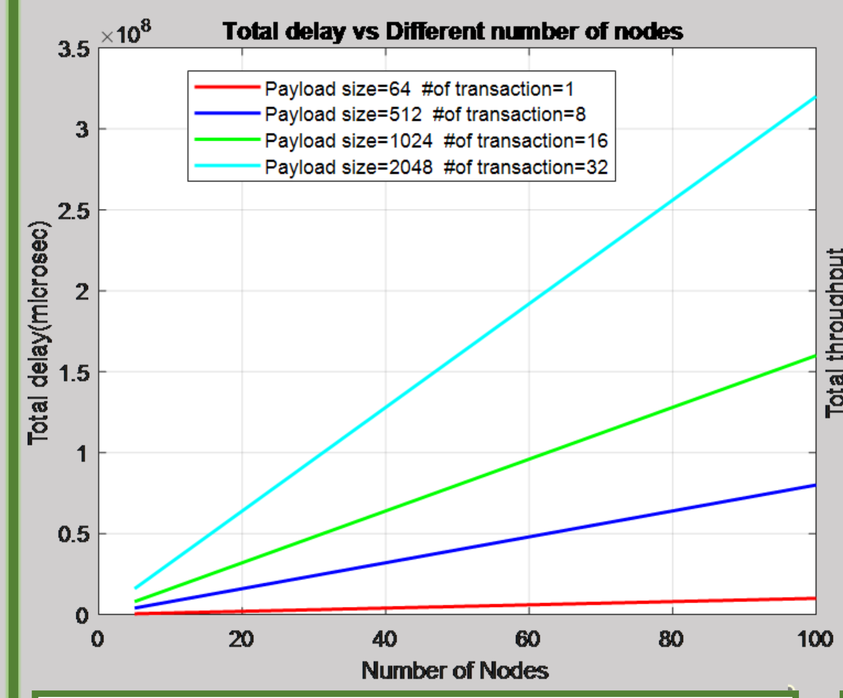
$$Total\ delay, T_s^t = E[P] + PHY_{header} + MAC_{header} + SIFS + N \times \frac{E[P]}{E[T]} T_d + SIFs + N \times ACKs + DIFS + \delta$$

$$Collision\ delay, T_c = E[P] + PHY_{header} + MAC_{header} + DIFS + \delta$$

$$Throughput = \frac{P_S E[P]}{P_S T_S + (1 - P_c) T_c}$$

Note: P_S is the probability that a packet is successfully transmitted and P_c the probability that a transmitted packet collides which is defined in detail in [1].

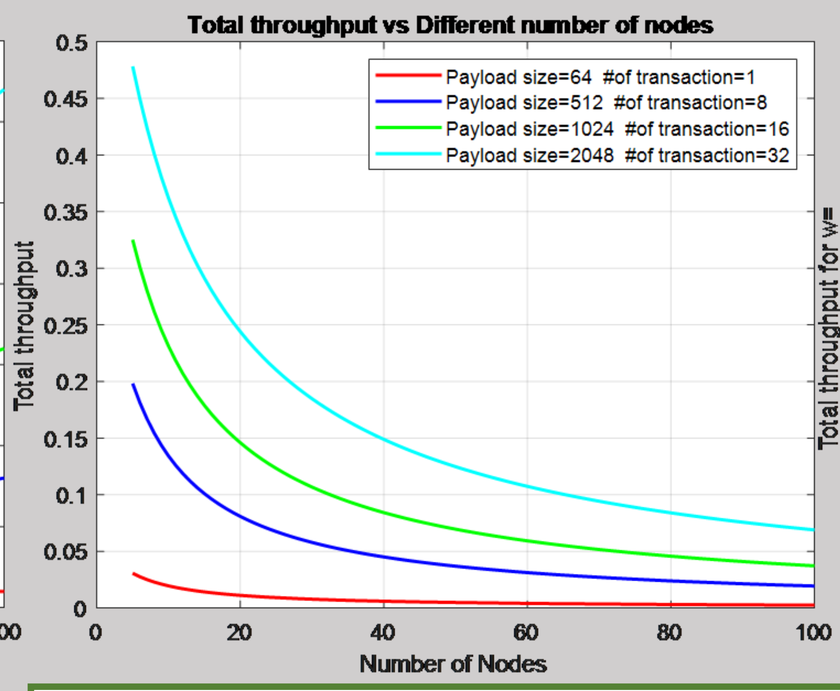
Evaluation and Simulation Results



Delay Vs #of Nodes

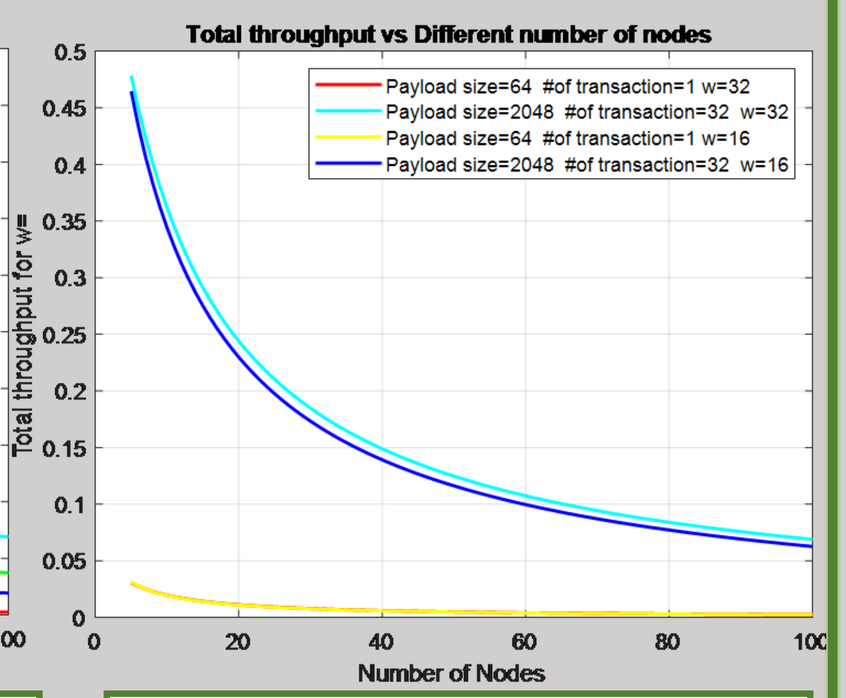
Delay increases for more #of Nodes
- Reasons: Validation Delay

However, more validating nodes means more security!



Throughput Vs #of Nodes with constant CW

Throughput decreases for more #of Nodes
- Meaning: lower percentage of successful transmission
- Reasons: increase #of consecutive ideal slots between two broadcasts



Throughput Vs #of Nodes for Variable CW

Throughput decreases as Decreasing the window size.
- Reasons: high probability of collision

effect will be more apparent with increasing the payload

Conclusion

The integration of blockchain and IoT promises a decentralized, scalable and fault resistant system. In current work, a MAC scheme was proposed to model the transmission between nodes in wireless IoT-Blockchain setup to see the variation in throughput and delay with respect to different number of nodes. We investigate the effect of blockchain on CSMA/CA built on top of Ethereum-based blockchain by building a MATLAB model and mathematical modeling. Blockchain promises more security in IoT as it uses all the nodes in the network to verify a new transaction before adding it to the chain, so more contributing nodes means more security and as we have seen in simulations done in this work, it means more delay and less throughput. This presents a trade-off which should be a real concern while integrating IoT network and Blockchain technology.

References

[1[G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE J. Sel. Areas Commun., vol. 18, no. 3, pp. 535–547, 2000.

[2] A. Abyaneh, N. Zorba and B. Hamdaoui, "IEEE 802.11ax based Medium Access Design for Wireless IoT-Blockchain Networks", IEEE Globecom, Taiwan, December 2020.