

Article

An Efficient MAC Protocol for Blockchain-Enabled Patient Monitoring in a Vehicular Network

Muhammad Aman Ullah ¹, Ahmad Naseem Alvi ¹, Muhammad Awais Javed ¹,
Muhammad Badruddin Khan ^{2,*}, Mozaherul Hoque Abul Hasanat ², Abdul Khader Jilani Saudagar ²
and Mohammed Alkathami ²

¹ Department of Electrical and Computer Engineering, COMSATS University Islamabad, Islamabad 45550, Pakistan

² Information Systems Department, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11432, Saudi Arabia

* Correspondence: mbkhan@imamu.edu.sa

Abstract: Blockchain is an emerging computing platform that provides recording and tracking facilities to substantially increase the security issues in healthcare systems. The evolution of wireless body area networks requires the continuous monitoring of the health parameters of traveling patients while traveling on road. The health parameter data of each patient are sent to the Road Side Units (RSUs) for generating the blocks by computing the required hash functions. A major challenge in such a network is to efficiently exchange the data blocks between mining RSUs and vehicles using a medium access protocol with a reduced number of collisions. The medium access problem becomes more challenging due to the vehicle mobility, high vehicle density and the varying nature of the data generated by the vehicles. In this work, a TDMA-based MAC protocol to meet an Adaptive Patients Data traffic for Vehicular Network ($TAPD_{VN}$) is proposed. $TAPD_{VN}$ is specifically designed for patients in a vehicular network by considering the frequent entry and exit of vehicles in a mining node's coverage area. It allows mining nodes to adjust time slots according to the sensitive patient's data and allows the maximum number of patient vehicular nodes by considering their sensitivity to send their data in a session to compute their hash values accordingly. Simulation results verify that the proposed scheme accommodates the maximum number of high-risk patient data and improves bandwidth utilization by 20%.

Keywords: vehicular networks; blockchain; medium access protocol; patient monitoring



Citation: Ullah, M.A.; Alvi, A.N.; Javed, M.A.; Khan, M.B.; Abul Hasanat, M.H.; Saudagar, A.K.J.; Alkathami, M. An Efficient MAC Protocol for Blockchain-Enabled Patient Monitoring in a Vehicular Network. *Appl. Sci.* **2022**, *12*, 10957. <https://doi.org/10.3390/app122110957>

Academic Editors: Davide Careglio, Mirosław Klinkowski and Francesco Palmieri

Received: 4 September 2022

Accepted: 24 October 2022

Published: 28 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Future healthcare systems will provide many applications for smart and intelligent patient monitoring. By using the advancements in the sensor and wireless communication technologies, medical data can be efficiently collected and disseminated [1,2]. Moreover, advanced data analytic techniques will provide greater insights to the doctors and patients.

Security is a major challenge for healthcare systems due to the sensitivity of the shared data. Blockchain is an upcoming technology that can provide improved data security and data storage efficiency to the healthcare systems [3]. Blockchain is a cryptographically secured, decentralized, and immutable technology that comprises several blocks. Each block has its block ID and contains transaction data that comprises smart contracts with time stamps. These blocks are linked together in such a way that each block knows the encrypted hash value of its previous block, as shown in Figure 1.

Blockchain provides security features regarding the immutability of data, which means that data can not be easily tampered [4–6]. The security of blockchain relies on generating particular hash values based on a Secure Hash Algorithm (SHA-256). For this, large computational power is needed and hence, computing nodes miners can generate the

required hash functions and validate blocks in the [7,8]. In a healthcare system, a group of medical hospitals with their medical advisors can use decentralized consortium-based blockchain technology for transferring patients' data.

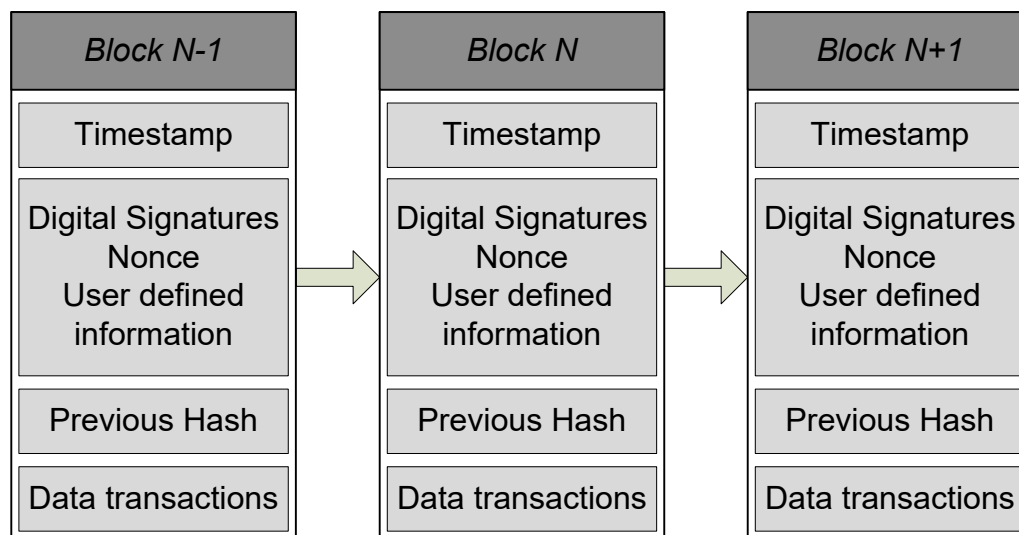


Figure 1. A standard blockchain structure.

In this paper, the focus is on the monitoring of patients who are traveling on the road. Blockchain-based data mining in such scenarios may utilize vehicular networks comprising vehicles, Road Side Units (RSUs) and a Traffic Command Center (TCC) [9–16]. Placing a mining computing node adjacent to each RSU as shown in Figure 2 provides the trustworthiness of data. Moreover, due to its proximity to vehicles, it provides quick data delivery to its mining node.

A major challenge in blockchain-enabled patient monitoring in a vehicular network is that at a higher data generation rate, the transmission of data from the vehicles to the mining nodes increases the chances of collision, thus resulting in poor Quality of Service (QoS). To avoid these collisions, dedicated time slots for each patient data vehicular node need to be used. As such patient data vary in its sensitivity in different time intervals, hence, data requests to RSUs vary in different time intervals. A classic Time Division Multiple Access (TDMA)-based MAC protocol does not fulfill these adaptive data traffic requirements. In addition, vehicle mobility and high vehicle density also add further complexity for efficient data sharing with the mining nodes.

In this work, a TDMA-based MAC protocol to meet an Adaptive Patients Data block in a vehicular network ($TAPD_{VN}$) between the patient vehicle and RSU nodes for consortium blockchain is proposed. $TAPD_{VN}$ allows RSU to adapt guaranteed time slots in a session according to the patients' data requirements within its session limits and prioritize the patients' data block to compute their Nonce value according to their sensitivity levels.

The salient features of $TAPD_{VN}$ are mentioned below:

1. The proposed MAC protocol prioritizes patient data for mining nodes to compute their valid nonce value by considering their sensitivity.
2. $TAPD_{VN}$ improves the Guaranteed Time Slot (GTS) utilization by reducing the size of data slots when data requests are less than the available data capacity in a session.
3. $TAPD_{VN}$ accommodates maximum patient data in a session by extending the number of slots to a maximum capacity of 255.
4. The network delay of data sending vehicles is reduced by adjusting the slot size according to the demand of data requesting vehicles.
5. Simulation results verify that the proposed protocol improves the successful block transmission percentage for high-risk patient data by 70%.

The rest of the paper is organized as: Section 2 describes different research works regarding mining nodes and MAC protocols for adaptive data requirements. Our proposed scheme is elaborated in Section 3. The performance of the proposed scheme along with its results is analyzed in Sections 4 and 5 concludes the paper.

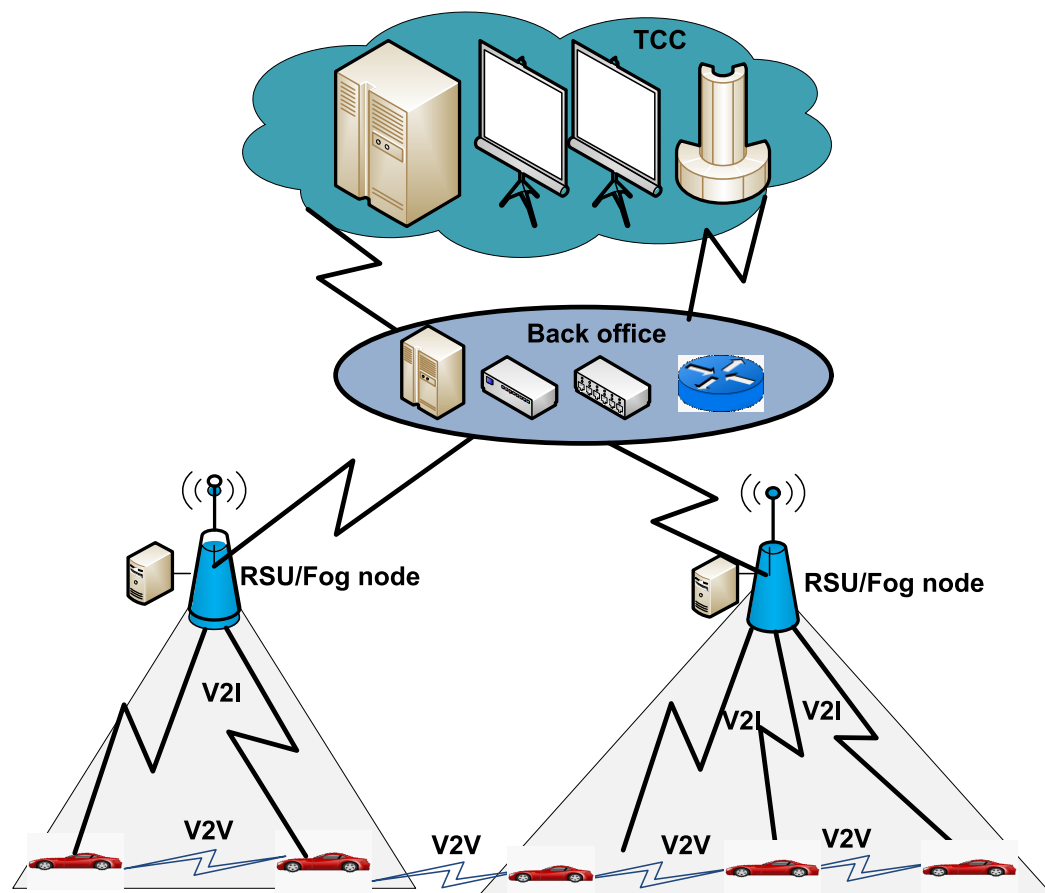


Figure 2. An architecture of vehicular networks (here, TCC: Traffic Command Centers).

2. Related Work

Secure and trusted data delivery are key challenges in vehicular networks. A blockchain-based contention-free MAC protocol is proposed in this work. This section is about previous studies about blockchain in vehicular networks and different MAC protocols that are used for wireless networks.

2.1. Blockchain Utility in Vehicular Networks

Trust management in transmitting data by a legitimate node is one of the prime requirements in vehicular networks. That is why the use of blockchain technology in provisioning security, privacy and trust in different prospects of the vehicular network is in high research demand.

In [17], the sharing of secured data for a scalable network based on consortium blockchain is proposed. The digital signature technique is used for data integrity. For the transaction of data, a practical Byzantine fault tolerance mechanism is used. In this work, the authors used smart contracts for pre-selected nodes to limit their triggering conditions. The authors claimed that their proposed scheme reduced data blocks about six times with an 83.33% increase in data transmission.

Refs. [18,19] introduced secure information sharing by introducing a regional blockchain environment for VANET. In [18], the authors proposed a local blockchain model by dividing the conventional blockchain into multiple geographic regions to ensure the scalability and timeliness of dissemination of message delivery trustworthiness of vehicular nodes. In [19],

the authors proposed four types of government-administered blockchains such as certificate blockchain, revocation, message and trust blockchains to improve the trust management among vehicles in a vehicular network. In this scheme, the malicious messages are rated with low values, and a predefined threshold value is proposed. In case the message value is less than the threshold value, it will be discarded from the network. The authors further claimed that their proposed technique improved the packet delivery ratio with reduced latency in the presence and absence of malicious attacks.

A blockchain-based secure mobility management scheme for the VANET environment is proposed in [20,21]. The proposed scheme in [20] improves the VANET environment in terms of handover latency, signal overheads and computational and communication overheads by allowing rights to the central and revocation authority, whereas RSUs have only read rights and the OBUs of vehicles have no rights. The scheme proposed in [21] comprises registration, initialization and handover phases. Blockchain technology is used for group authentication and to avoid Sybil attacks and replay attacks by introducing secure key negotiation in building up each communication session.

Most of the research regarding the use of blockchain in a vehicular network is in the light of providing security, and it focuses on malicious attacks and providing the validity of data delivery. However, according to our knowledge, there is no research on medium access techniques between mining and vehicular nodes in the blockchain environment for a vehicular network that is proposed.

2.2. MAC Protocols

MAC protocols are mainly categorized as contention-based and contention-free MAC protocols. In contention-based MAC protocols, there are chances of collision, and this probability increases with the rise in more data requesting nodes. In such scenarios, contention-free MAC protocols are preferred. Multiple MAC protocols are designed for different applications.

In [22,23], MAC protocols are proposed by adjusting duty cycles according to the adaptive data traffic. The authors in [22] proposed a Priority-based algorithm for Adaptive Superframe Adjustment and GTS Allocation (PASAGA) that allows the PAN coordinator to adjust its duty cycle according to the data priority of GTS requesting nodes on their data requests. In [23], an optimized GTS (OGTS) allocation algorithm is proposed that allocates GTS to data requesting nodes optimally to improve its GTS allocation.

TDMA-based MAC protocols to meet the adaptive data requirements of nodes are proposed in [24,25]. Both of these MAC protocols offered bit map-assisted TDMA-based MAC protocols and allocated the unused TDMA slots to those nodes, which required more data slots in a session to offer better link utilization. The authors in [25] proposed Bit map-assisted Shortest Job First (BS-MAC) and applied the Shortest Job First (SJF) algorithm [25]. The authors claimed that their proposed algorithm reduces network delay and offers better link utilization. In [24], Bit map assisted Efficient and Scalable TDMA-based MAC (BEST-MAC) protocol is proposed that offered a knapsack algorithm [26] to optimally allocate slots to GTS requesting nodes to improve the link utilization.

In [27], an adaptive collision avoidance scheduling is proposed for IoT networks. The proposed scheme is based on the traffic and priority of sensor nodes. The authors claimed that their proposed scheme improves the network performance as compared to a conventional scheme. In [28], an Efficient Superframe structure for adaptive Data requirement (ESAD) is proposed to meet the adaptive data requirement of wireless nodes. The authors proposed a superframe structure with an adaptive duty cycle for IEEE 802.15.4 standard. The authors claimed that their proposed scheme offers better bandwidth utilization by accommodating more GTS requesting nodes.

$TAPD_{VN}$ is designed to meet the adaptive data requirements between fog computing nodes and vehicles where the fog node acts as a cluster head and the vehicles node are attached with it. A brief comparison of all these MAC protocols is shown in Table 1.

A key weakness of the current techniques in the literature is the fixed slot sizes for data transmission, which will not be suitable for varying the frequency of data transmission scenarios such as for blockchain mining data transmission. Moreover, the priority of the data is also not considered to maximize the slot utilization for high-risk patients data.

Table 1. Comparative table between different MAC.

MAC Protocol	Delay	Link Utilization	Nodes Capacity Improved	Duty Cycle	Purpose/Procedure
PASAGA	Low	High	No	Conventional	Duty cycle adjustment by prioritizing GTS requests
OGTS	NA	High	Yes	Conventional	Optimal GTS allocation by considering their data requests
BEST-MAC	Low	High	No	Adaptive	Applied knapsack algorithm to optimally adjust GTS in a session
BS-MAC	Low	Low	No	Adaptive	Applied Shortest Job First algorithm
ESAD	Low	High	Yes	Adaptive	An algorithm to optimally adjust a duty cycle of the next superframe by considering data requests
TAPD _{VN}	Low	High	Yes	Adaptive	An algorithm to efficiently adjust the duty cycle of a TDMA session by considering data requests

3. Proposed Superframe Structures

In this work, a TDMA-based MAC protocol is proposed to prioritize adaptive patient data to compute their Nonce value for a valid hash value.

3.1. Proposed Scheme

The proposed MAC is specifically designed to meet the adaptive data requirements of patients in vehicular networks. Vehicles are attached with RSU during their journey to form a cluster, and the RSU adjacent to Mining Node (MN) acts as a cluster head. All vehicles attached to this mining node are its member nodes.

RSU remains a cluster head throughout, and vehicles in its communication areas become its member nodes only for the time during which they are connected with this RSU. The proposed communication round comprises multiple sessions, and each session comprises a handshaking period and data transmission phase as shown in Figure 3.

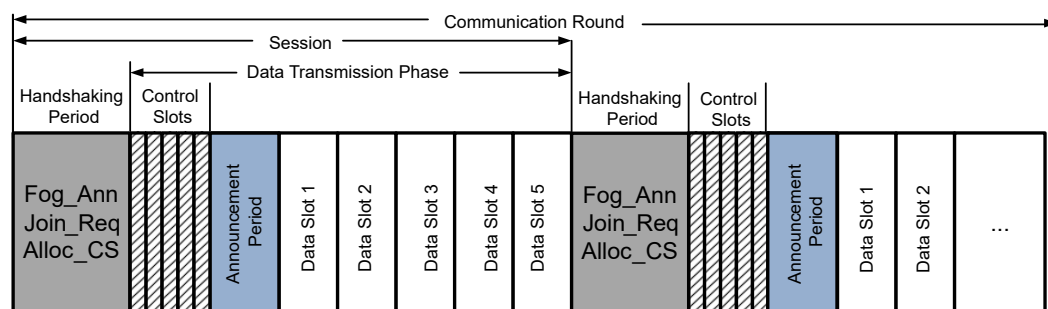


Figure 3. A communication round of the proposed MAC for mining nodes in vehicular networks.

3.1.1. Handshaking Period

Each session in a communication round starts with a handshaking period. During the handshaking period, the *RSU* broadcasts the announcement message (RSU_{Ann}) to all vehicles in its communication range. All vehicles must keep their radios ON to receive the announcement message. Vehicular nodes select the *RSU*, whose announcement message is heard with the largest signal strength. In the case of a tie, the next *RSU* is selected. After that, vehicles reply with a join request ($Join_{Req}$) message. This message consists of the control message, vehicle's address, *RSU* address and frame check sequence. After that, *MN* waits for some time to receive all the $Join_{Req}$ and then calculates the total number of vehicle requests. *RSU* computes a unique 1-byte short address for all the associated member nodes and for itself. Therefore, a maximum of 255 member nodes can be associated with a single *RSU*.

After receiving all the $Join_{Req}$, *RSU* assigns the separate control slot to each member node and sends the control slot allocation ($Alloc_{CS}$) message to all members nodes using CSMA. This message consists of the control byte, *RSU*'s short address, nodes' extended and short address, nodes' assigned control slot number, start time of data slot announcement period, and frame control sequence.

3.1.2. Data Transmission Phase

After the successful completion of the handshake period, the data transmission phase immediately starts. A data transmission phase comprises of control period, announcement period, and data transmission period.

Each patient's vehicular node is allocated a separate control slot to send their data slot requests. A data slot request comprises a number of data slots required by the patient's data block along with its nature of sensitivity. In this work, the data sensitivity is divided into eight different levels by assigning three bits in its frame structure. The sensitivity level increases from 0 to 7, where 0 means least sensitive and 7 means the most sensitive data. Each datum requesting patient's vehicles after computing its number of required slots along with its sensitivity level sends the control message to their attached *RSU* during the allocated control slot.

After the completion of the control period, the *MN* of the attached *RSU* has complete knowledge about the number of vehicles that want to send data and how many data slots are required by them. During the announcement period, *MN* disseminate information about slots allocation to all successful vehicles with their starting slot number and the number of slots assigned to each of them. In case there is no data slot request received from the vehicles, then there will be no data slot in that session. In addition, *MN* broadcasts about the start of the next session in its announcement period, so vehicles must be aware of the start of the upcoming session.

3.2. Proposed Algorithm

During the control period, each data-requesting node sends its required number of slots to the *MN*. If a data-requesting node n requires to transmit data (D_n), then the number of data slots required (S_n) by this node can be computed as:

$$\left[S_n = \frac{D_n}{Z} \right]$$

here, Z is the data slot capacity in a session.

At the end of the control period, the *MN* has the information of accumulating slots and their data sensitivities from the slot requests received from all patients' vehicle nodes.

In this proposed scheme, it is supposed that the number of time slots in a session is similar to the number of data requesting nodes. There are 8 bits reserved to determine the maximum number of slots in a session, allowing a maximum limit of 255 time slots in a session. There are three different data-requesting possibilities.

- Accumulating data slot requests are more than the initially available slots but less than the maximum limit.
- Accumulating data slots requests in a session are less than the initially available slots.
- Accumulating data slot requests are more than the maximum limit of 255.

3.2.1. Case 1

If the accumulating requests are more than the initially available slots and less than the maximum limit of 255, then slots are allocated to all data-requesting nodes in that session by increasing the extra slots in that session in such a way that the slots allocation to more sensitive patients' data is prioritized over less sensitive data.

3.2.2. Case 2

If accumulating data slot requests are less than the initially available slots, then the slot size needs to be shrunk by a factor of X to allow maximum slot utilization with reduced network delay. The reducing slot factor (X) is calculated as:

$$X = \frac{S_{Avail} - S_{total}}{S_{Avail}} \quad (1)$$

The new slot size (Z_{new}) is calculated as:

$$Z_{new} = Z \times (1 - X) \quad (2)$$

Now, MN has to compute the new slots requirements (S'_n) according to the Z_{new} as:

$$S'_n = \frac{(Z \times S_n)}{Z_{new}} \quad (3)$$

MN computes the divider (D) to divide each slot by that divider to efficiently assign the slots to vehicles to achieve high channel utilization. This D factor is achieved by dividing four bits maximum number 15 with the highest data-requesting vehicle as:

$$D = \frac{15}{S_{HJ}} \quad (4)$$

After the division of slots, the slot requirements will be changed, and MN updates that as per the new slot size after division.:

$$R_n = S'_n \times D \quad (5)$$

3.2.3. Case 3

In case the number of requesting slots by patients' vehicles is more than the maximum allowed limit of the proposed protocol, then the TDMA session cannot accommodate all data-requesting patients' vehicles. In this case, the data-requesting vehicles are optimally assigned data slots by applying the knapsack optimization algorithm. A complete flow chart of the proposed scheme is shown in Figure 4.

The proposed scheme assists MN to receive the sensitive data within the maximum session capacity to compute the nonce value of the patient's data block. This is achieved by optimally allocating data slots to vehicle patient nodes by applying the 0/1 knapsack algorithm as described in Section 3.2.4.

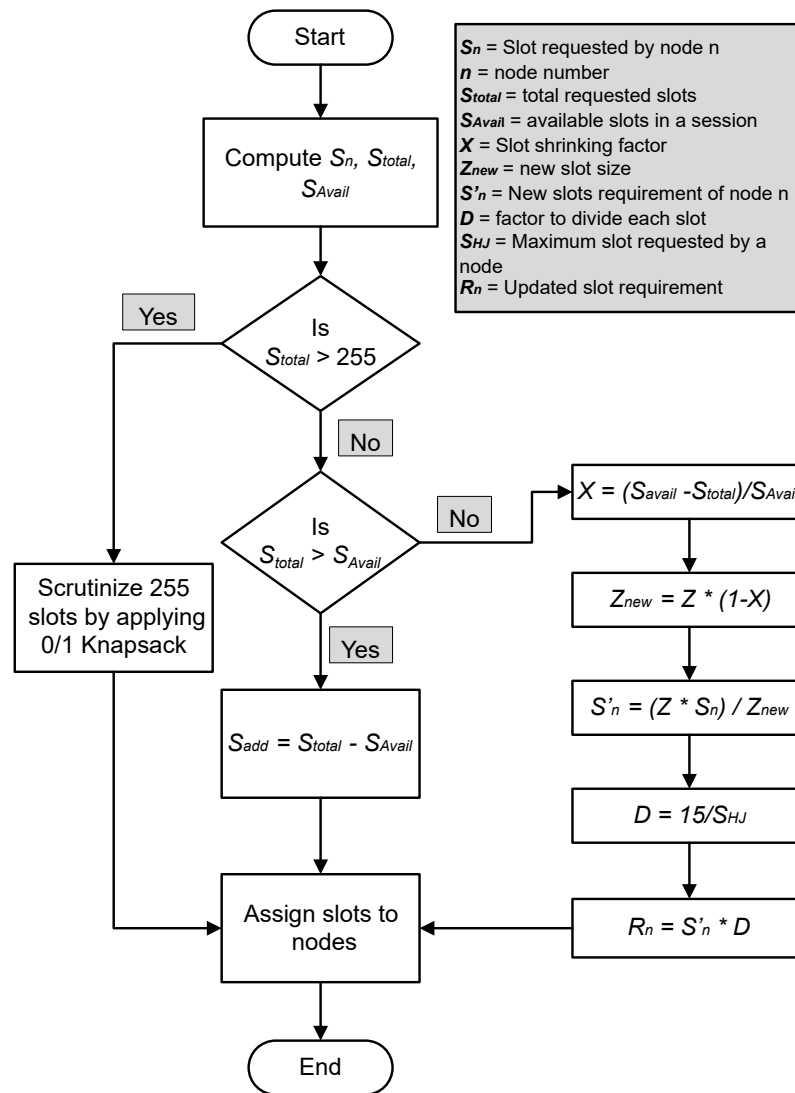


Figure 4. Proposed algorithm for adaptive data requirements in vehicular networks.

3.2.4. 0/1 Knapsack Algorithm

The 0/1 Knapsack algorithm allows utilizing the limited capacity with the most valuable items of different weights within its carrying capacity. Our proposed algorithm can have a maximum of 255 slots to restrict the control overhead. In case slot requirements are more than 255, then the knapsack algorithm selects the slots of vehicle nodes that have sensitive data requirements so that data can be transmitted on priority. All nodes have pre-configured sensitivity values: the higher the sensitivity level, the higher will be the value.

Our designed problem maps with the knapsack problem, as mentioned in Table 2.

Table 2. knapsack mapping.

Knapsack Problem	Slots Selection Problem
Knapsack capacity	Maximum slot capacity in a session (255)
Weight of item	Slot requested by vehicle
Value of item	Sensitivity level of requested data

The knapsack algorithm optimally scrutinizes items by filling a knapsack table by following the below-mentioned two steps:

1. Creating and filling knapsack table;
2. Selection of patients' vehicles that have sensitive data.

The knapsack algorithm starts with creating the knapsack table that has $N + 1$ rows and $S_{max} + 1$ columns, where N is the total number of vehicles and S_{max} is the maximum number of slots, i.e., 255. After the creation of the table, the knapsack algorithm starts filling the table. A complete algorithm for filling the 0/1 knapsack table in $TAPD_{VN}$ is shown in Figure 5. After creating and filling the knapsack table, the most sensitive data-requesting vehicles that have accumulative slots equal to or less than S_{max} is selected. Successful data-requesting vehicular node selection is shown in Figure 6.

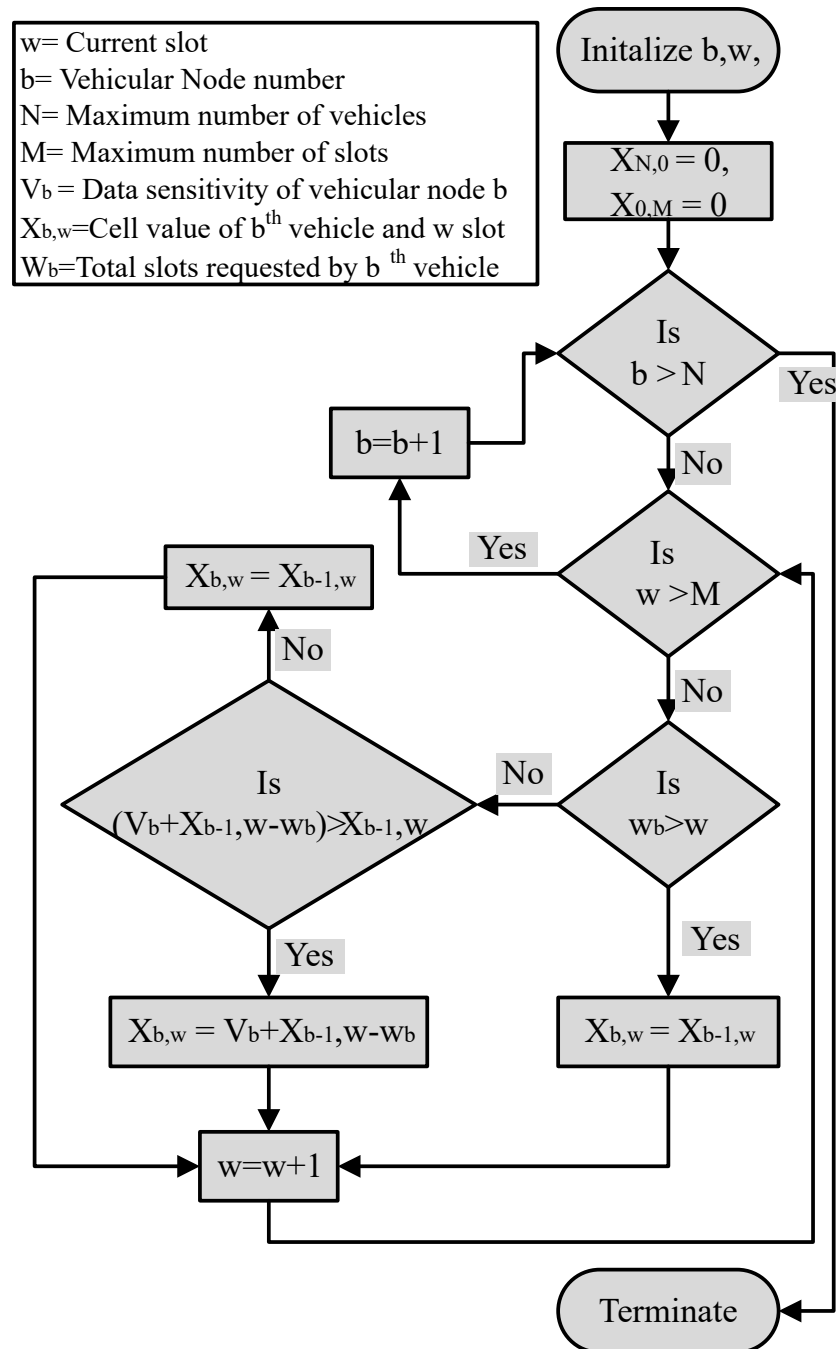


Figure 5. The 0/1 knapsack algorithm.

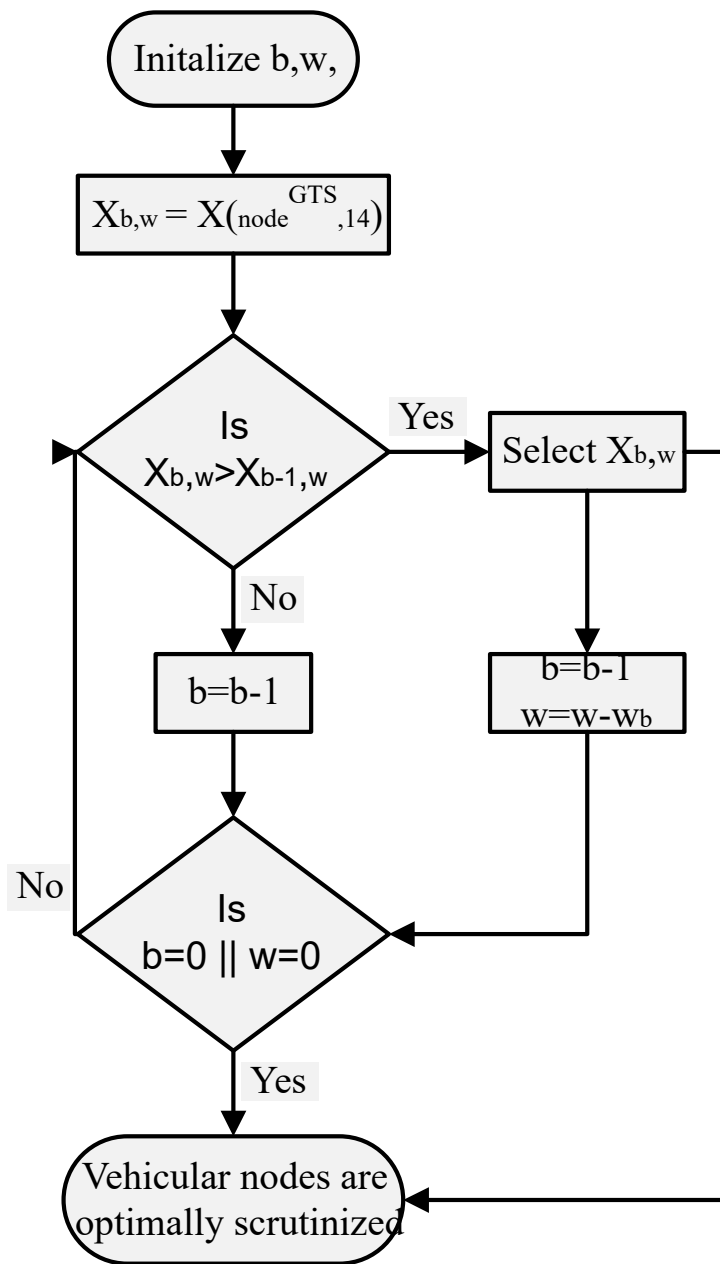


Figure 6. Optimal vehicular node selection criteria.

4. Results and Analysis

To evaluate the performance of our proposed scheme, a simulation environment is created, where vehicles are registered as a patient’s vehicle before the start of their journey. These vehicles remain in contact with RSUs throughout their journey. The mining node is placed adjacent to each RSU and acts as an *MN*, and all patients’ vehicles are connected with it in a star topology. Patient vehicles’ data are transmitted to its associated *MN* in a dedicated time slot.

A simulation environment is created in MATLAB that comprises 5 to 15 patients having adaptive data requests in each session of a round. The initial data slot duration is 83.3 ms with a data capacity of 2000 bits. This network is simulated for two different cases with varying data requests. Each case comprises a round of ten sessions. A complete set of simulation parameters are shown in Table 3. Simulations results are compared with state-of-the-art BS-MAC protocol and First Come First Serve (FCFS).

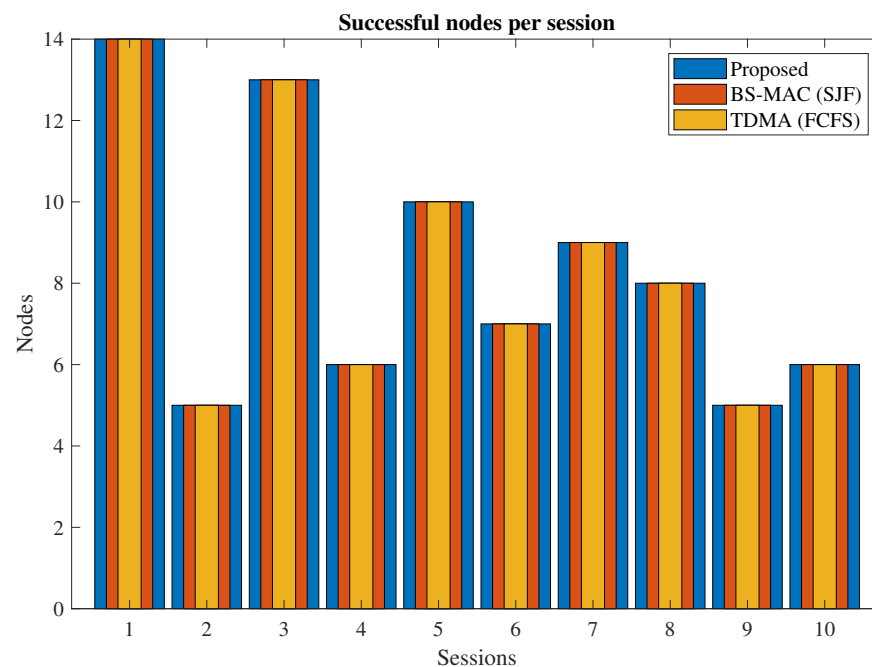
Table 3. Simulation Parameters.

Simulation Parameters	Values
Number of patient sensor nodes	5–15
Network size	100 m × 100 m
Data rate	250 kbps
Initial slot capacity (Bytes)	2000
Initial data slot duration (s)	0.0833
Data traffic per session for case 1 (KB)	6–70
Data traffic per session for case 2 (KB)	30–120
Number of sessions	10

4.1. Case 1

In this scenario, the total slots requirements are less than the available slots in each session. Our proposed protocol shrinks the session by reducing the slot size by following data requirements and then dividing each slot for the efficient allocation of slots to nodes in each session. The slot size will be different for every session.

In Figure 7, successful nodes per session of the proposed protocol and BS-MAC are compared. A successful node refers to the node which can transmit all the data successfully to the cluster head within a session. There is a total of 10 sessions simulated with a different number of nodes per session. All the nodes in each session succeeded in both protocols because the total slots requests are less than the available slots.

**Figure 7.** Successful vehicles in transmitting their data.

In Figure 8, the total amount of data transmitted in each session of the proposed protocol and BS-MAC is compared. There is a total of 10 sessions simulated with different numbers of nodes per session. Both BS-MAC and the proposed protocol allow all the nodes in each session to transmit all the data because all the nodes have less data than the session capacity.

In Figure 9, the channel utilization of proposed and BS-MAC protocols are compared for a session. There is a total of 10 sessions simulated with a different number of nodes per session. Results show that channel utilization of the proposed protocol is far better than BS-MAC because in this case, data are less than the total session capacity, and the proposed protocol reduced the session by shrinking the slot size by following data slots requests. The proposed protocol is more adaptable than BS-MAC because it divides the shrink slots by different numbers in every session according to slot requests. Whereas, in BS-MAC, data slots are divided by 10 in every session.

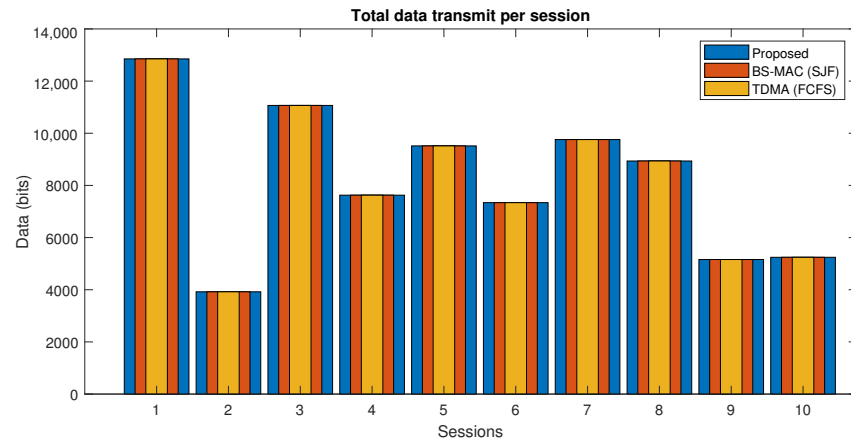


Figure 8. Data transmission in each session (Case I).

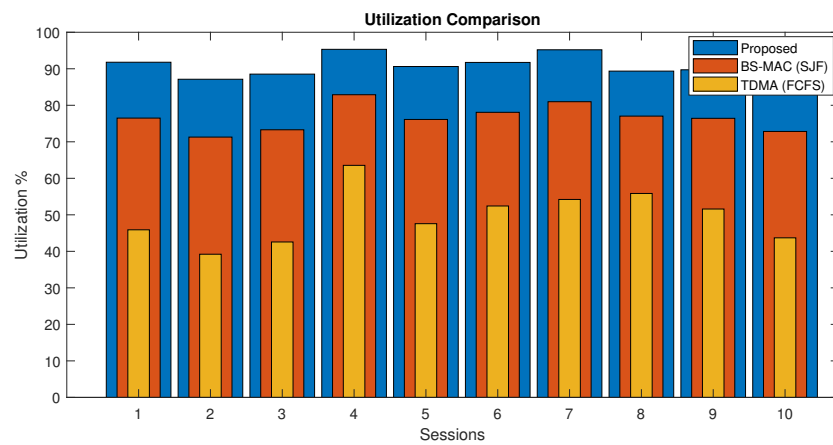


Figure 9. Channel utilization comparison of proposed protocol (Case I).

In Figure 10, the data transmission time of both proposed and BS-MAC protocols is compared in the case when the slots requests are less than the available slots. There are a total of 10 sessions simulated with a different number of nodes per session. Results show that the data transmission time for each session in the proposed protocol is far less than the BS-MAC protocol, because in this case, data are less than the total session capacity, and the proposed protocol reduced the session by shrinking the slot size by following data slots requests.

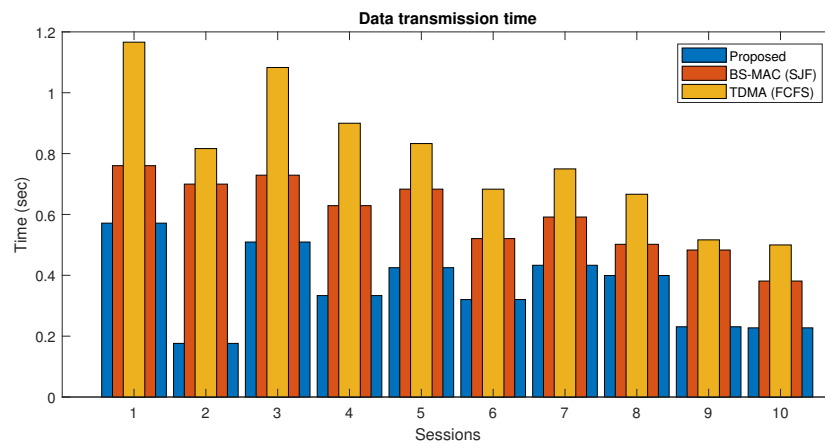


Figure 10. Data transmission time comparison of proposed protocol (Case I).

4.2. Case 2

In this case, the total slot requirements are more than the total available slots in all ten sessions. Our proposed algorithm added additional slots of the same slot size and extended each session to entertain all the source nodes.

In Figure 11, successful nodes per session of the proposed protocol and BS-MAC for case II are compared. A successful node refers to the node which can transmit all the data successfully to the cluster head in the current session. There are a total of 10 sessions simulated with a different number of nodes per session. Results show that the proposed protocol entertained all the nodes of each session whereas, in BS-MAC, only a few nodes can transmit data successfully.

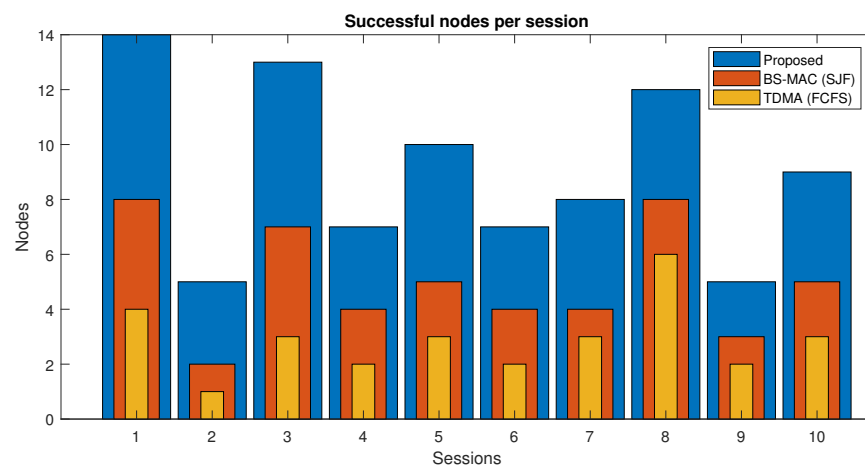


Figure 11. Successful vehicles in transmitting their data (Case 2).

In Figure 12, the total amount of data transmitted in each session of the proposed protocol and BS-MAC is compared. There are a total of 10 sessions simulated with a different number of nodes per session. Results show that more data are transmitted in the proposed protocol as compared to BS-MAC. The proposed protocol extended each session by following the data requirements of nodes and allowing the nodes to transmit all the data in the current session.

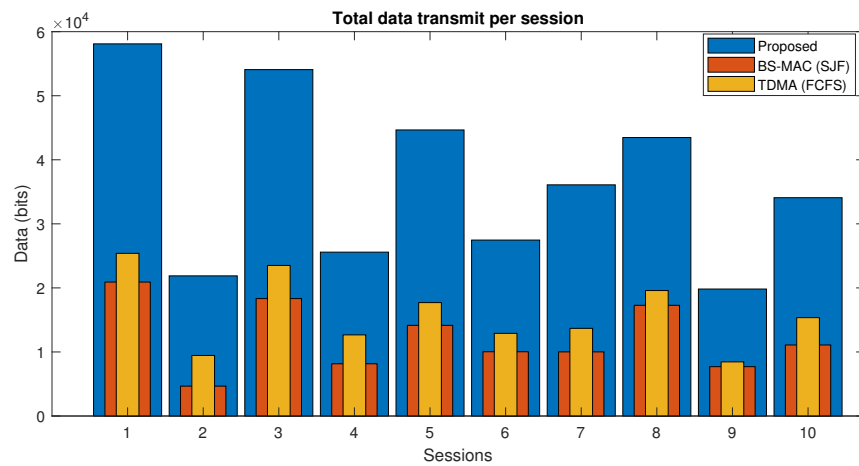


Figure 12. Data transmit per session of proposed protocol (Case 2).

In Figure 13, the channel utilization of proposed and BS-MAC protocols are compared for each session in the case when the total requested slots is more than the available slots. There are a total of 10 sessions simulated with a different number of nodes per session. Results show that channel utilization of the proposed protocol is far better than BS-MAC.

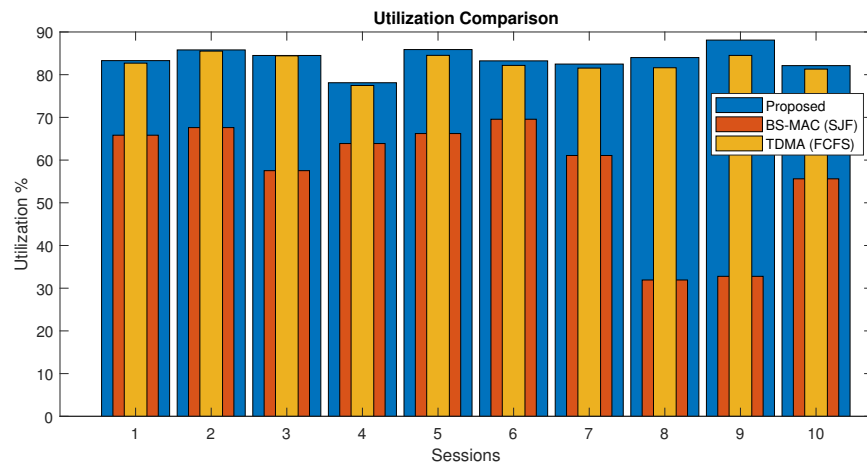


Figure 13. Channel utilization comparison of the proposed protocol (Case 2).

In Figure 14, the data transmission time of the proposed scheme is compared with the other two schemes when the slots requests are less than the available slots. Results show that the data transmission time for each session in the proposed protocol is more than the other two competitors. This is due to the increased slots offered in the proposed scheme to accommodate more data-requesting vehicular nodes. An increase in time slots results in increased session duration and hence results in more data-transmitting time of nodes. In comparison, BS-MAC and FCFS have a fixed session duration and do not accommodate more data-requesting nodes and consequently have fewer data-transmitting times, as non-accommodating nodes are not included in the results.

The performance of the proposed MAC is further analyzed by following its successful transmission of critical patient data as compared to the normal patient data. For a fair comparison, the session duration of both BS-MAC and FCFS is fixed. The results shown in Figure 15 verify that for a fixed session length, our proposed scheme accommodates more high-risk patients’ data blocks as compared to the other two schemes by compromising the medium-risk and low-risk patients’ data.

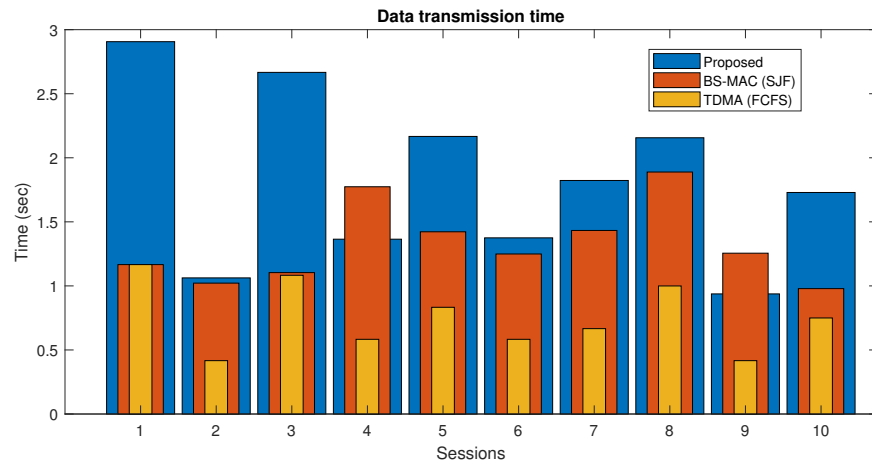


Figure 14. Data transmission time comparison of proposed protocol (Case 2).

The results shown in Figure 16 elaborate the same results in terms of percentage with a varying number of the patients’ data blocks in each session. It is evident from the results that the proposed scheme accommodates the maximum of the high-risk patients’ data as compared to the other two schemes by compromising the medium-risk and low-risk patients’ data as compared to the other two schemes for fixed session length.

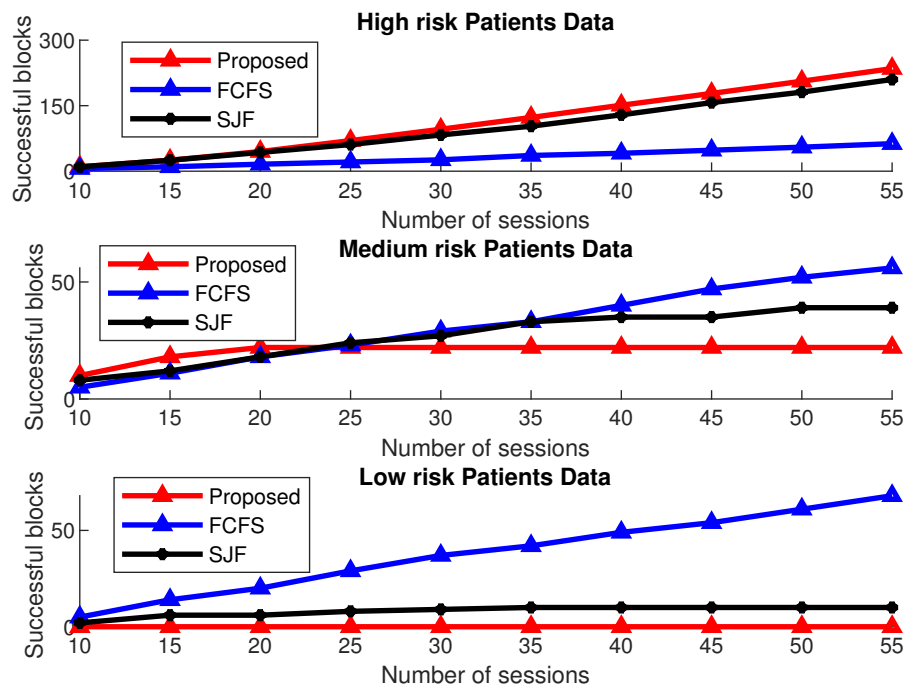


Figure 15. Successful transmission of priority data for a varying number of sessions.

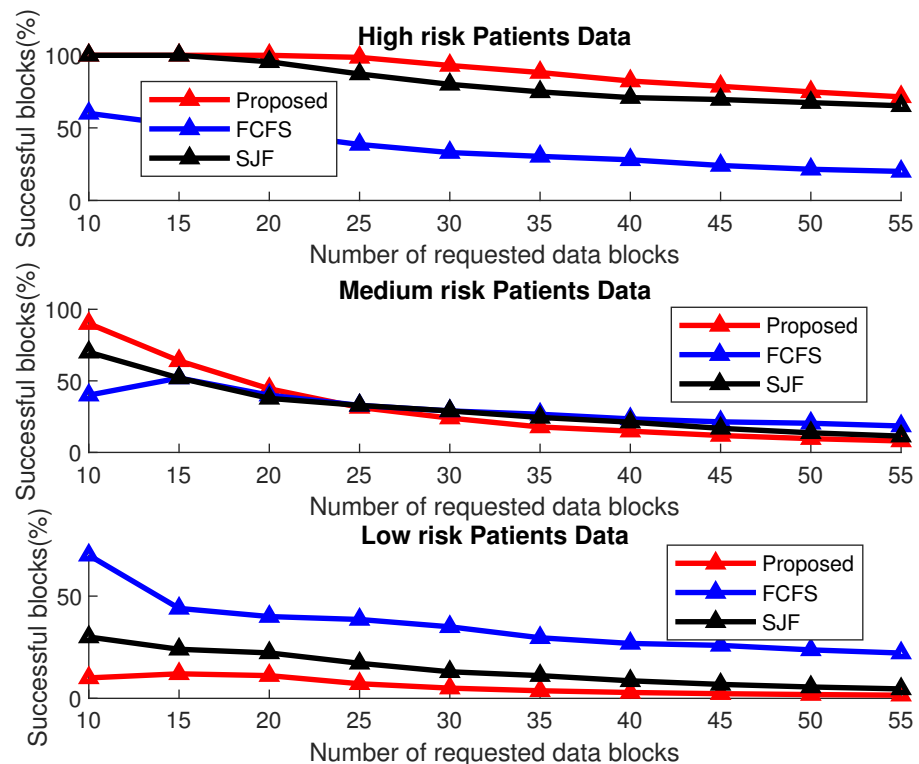


Figure 16. Successful transmission of priority data for a varying number of requested data blocks.

4.3. Discussion

From the results, it is clear that the proposed protocol outperforms the other two schemes in terms of the utilization and successful block transmission percentage. The major reason for this improvement is the adaptive nature of the protocol that adjusts the slot sizes as per the data requirements. Moreover, a priority is assigned to the high-risk patient data. As a result, the proposed technique has the highest successful block transmission percentage for high-risk patients' data. This improvement comes at the expense of lower successful percentage for the low-risk patient data. Since these data have low priority with low latency requirements, it does not impact the application performance. Therefore, the proposed technique is suited for the transmission of blockchain data to the mining nodes for high-risk patients.

5. Conclusions

This paper focuses on developing a novel protocol for blockchain-based health related data transmission between vehicular nodes and mining RSU nodes. A TDMA-based MAC protocol to meet the Adaptive Patients' Data requirement for blockchain-based vehicular Network ($TAPD_{VN}$) is proposed. $TAPD_{VN}$ is designed according to the diverse patients' vehicle density and assists the mining node to compute nonce according to the sensitivity level of the patient's data block. The proposed MAC protocol allocates guaranteed time slots in a session according to the data requirement by shrinking or expanding the data slots. The proposed MAC protocol allows new patient vehicles to become part of this network and transmit data in their guaranteed time slots. The performance of $TAPD_{VN}$ is comprehensively compared with FCFS and BS-MAC in multiple scenarios. The results show that $TAPD_{VN}$ accommodates better data transmission in a session with improved GTS utilization as compared to the other two schemes. In addition, it accommodates more patients' vehicles to send their data in a session with the maximum limit of 255 as compared to FCFS and BS-MAC.

Author Contributions: This article was prepared through the collective efforts of all the authors. Conceptualization, M.A.U., A.N.A., M.A.J., M.B.K., M.H.A.H., A.K.J.S. and M.A.; Critical review, M.A.U., A.N.A., M.A.J., M.B.K., M.H.A.H., A.K.J.S. and M.A.; Writing—original draft, M.A.U., A.N.A. and M.A.J.; Writing—review and editing, M.B.K., M.H.A.H., A.K.J.S. and M.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University for funding this work through Research Group no. RG-21-07-07.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is available upon request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ahmed, J.; Nguyen, T.N.; Ali, B.; Javed, A.; Mirza, J. On the Physical Layer Security of Federated Learning based IoMT Networks. *IEEE J. Biomed. Health Inform.* **2022**, *1*. [[CrossRef](#)] [[PubMed](#)]
2. Malik, U.M.; Javed, M.A.; Zeadally, S.; Islam, S.U. Energy-Efficient Fog Computing for 6G-Enabled Massive IoT: Recent Trends and Future Opportunities. *IEEE Internet Things J.* **2022**, *9*, 14572–14594. [[CrossRef](#)]
3. Menon, S.; Jain, K. Blockchain Technology for Transparency in Agri-Food Supply Chain: Use Cases, Limitations, and Future Directions. *IEEE Trans. Eng. Manag.* **2021**, 1–15. [[CrossRef](#)]
4. Ahamed, N.N.; Thivakaran, T.K.; Karthikeyan, P. Perishable Food Products Contains Safe in Cold Supply Chain Management Using Blockchain Technology. In Proceedings of the 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 19–20 March 2021; Volume 1, pp. 167–172. [[CrossRef](#)]
5. Javed, M.A.; Nguyen, T.N.; Mirza, J.; Ahmed, J.; Ali, B. Reliable Communications for Cybertwin driven 6G IoVs using Intelligent Reflecting Surfaces. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7454–7462. [[CrossRef](#)]
6. Ahmad, R.W.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Omar, M.; Ellahham, S. Blockchain-Based Forward Supply Chain and Waste Management for COVID-19 Medical Equipment and Supplies. *IEEE Access* **2021**, *9*, 44905–44927. [[CrossRef](#)]
7. Malik, U.M.; Javed, M.A. Ambient Intelligence assisted fog computing for industrial IoT applications. *Comput. Commun.* **2022**. [[CrossRef](#)]
8. Malik, U.M.; Javed, M.A.; Frnda, J.; Rozhon, J.; Khan, W.U. Efficient Matching-Based Parallel Task Offloading in IoT Networks. *Sensors* **2022**, *22*, 6906. [[CrossRef](#)]
9. Javed, M.A.; Zeadally, S.; Hamida, E.B. Data analytics for Cooperative Intelligent Transport Systems. *Veh. Commun.* **2019**, *15*, 63–72. [[CrossRef](#)]
10. Khan, A.A.; Abolhasan, M.; Ni, W.; Lipman, J.; Jamalipour, A. A Hybrid-Fuzzy Logic Guided Genetic Algorithm (H-FLGA) Approach for Resource Optimization in 5G VANETs. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6964–6974. [[CrossRef](#)]
11. Janjevic, M.; Winkenbach, M. Characterizing urban last-mile distribution strategies in mature and emerging e-commerce markets. *Transp. Res. Part A Policy Pract.* **2020**, *133*, 164–196. [[CrossRef](#)]
12. Chen, B.; Imran, M.; Nasser, N.; Shoaib, M. Self-Aware Autonomous City: From Sensing to Planning. *IEEE Commun. Mag.* **2019**, *57*, 33–39. [[CrossRef](#)]
13. Ding, L.; Wang, Y.; Wu, P.; Li, L.; Zhang, J. Kinematic Information Aided User-Centric 5G Vehicular Networks in Support of Cooperative Perception for Automated Driving. *IEEE Access* **2019**, *7*, 40195–40209. [[CrossRef](#)]
14. Jameel, F.; Javed, M.A.; Ngo, D.T. Performance Analysis of Cooperative V2V and V2I Communications Under Correlated Fading. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 3476–3484 [[CrossRef](#)]
15. Ahmad, S.A.; Hajisami, A.; Krishnan, H.; Ahmed-Zaid, F.; Moradi-Pari, E. V2V System Congestion Control Validation and Performance. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2102–2110. [[CrossRef](#)]
16. Sheehan, B.; Murphy, F.; Mullins, M.; Ryan, C. Connected and autonomous vehicles: A cyber-risk classification framework. *Transp. Res. Part A Policy Pract.* **2019**, *124*, 523–536. [[CrossRef](#)]
17. Zhang, X.; Chen, X. Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network. *IEEE Access* **2019**, *7*, 58241–58254. [[CrossRef](#)]
18. Shrestha, R.; Nam, S.Y. Regional Blockchain for Vehicular Networks to Prevent 51% Attacks. *IEEE Access* **2019**, *7*, 95033–95045. [[CrossRef](#)]
19. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET. *Sensors* **2019**, *19*, 4954. [[CrossRef](#)]
20. Malik, N.; Nanda, P.; Arora, A.; He, X.; Puthal, D. Blockchain Based Secured Identity Authentication and Expeditious Revocation Framework for Vehicular Networks. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 674–679. [[CrossRef](#)]

21. Lai, C.; Ding, Y. A Secure Blockchain-Based Group Mobility Management Scheme in VANETs. In Proceedings of the 2019 IEEE/CIC International Conference on Communications in China (ICCC), Changchun, China, 11–13 August 2019; pp. 340–345. [[CrossRef](#)]
22. Lee, B.; Wu, H.; Yu, N. A priority based algorithm for adaptive superframe adjustment and GTS allocation (PASAGA) in IEEE 802.15.4 LR-WAN. In Proceedings of the 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 13–17 April 2018; pp. 318–320. [[CrossRef](#)]
23. Alvi, A.N.; Khan, S.; Javed, M.A.; Konstantin, K.; Almagrabi, A.O.; Bashir, A.K.; Nawaz, R. OGMAD: Optimal GTS-Allocation Mechanism for Adaptive Data Requirements in IEEE 802.15.4 Based Internet of Things. *IEEE Access* **2019**, *7*, 170629–170639. [[CrossRef](#)]
24. Alvi, A.N.; Bouk, S.H.; Ahmed, S.H.; Yaqub, M.A.; Sarkar, M.; Song, H. BEST-MAC: Bitmap-Assisted Efficient and Scalable TDMA-Based WSN MAC Protocol for Smart Cities. *IEEE Access* **2016**, *4*, 312–322. [[CrossRef](#)]
25. Alvi, A.N.; Bouk, S.H.; Ahmed, S.H.; Yaqub, M.A.; Javaid, N.; Kim, D. Enhanced TDMA based MAC protocol for adaptive data control in wireless sensor networks. *J. Commun. Netw.* **2015**, *17*, 247–255. [[CrossRef](#)]
26. Ezugwu, A.E.; Pillay, V.; Hirasen, D.; Sivanarain, K.; Govender, M. A Comparative Study of Meta-Heuristic Optimization Algorithms for 0–1 Knapsack Problem: Some Initial Results. *IEEE Access* **2019**, *7*, 43979–44001. [[CrossRef](#)]
27. Nguyen, L.T.; Nguyen, T.H.T.; Le, H.C.; Vinh Vu, T.; Trinh Nguyen, C. Adaptive Collision Avoidance Scheduling based on Traffic and Priority for IoT Sensor Networks. In Proceedings of the 2021 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 14–16 October 2021; pp. 73–78. [[CrossRef](#)]
28. Khan, S.; Alvi, A.N.; Javed, M.A.; Bouk, S.H. An enhanced superframe structure of IEEE 802.15.4 standard for adaptive data requirement. *Comput. Commun.* **2021**, *169*, 59–70. [[CrossRef](#)]