Journal of Basics and Applied Sciences Research (JOBASR)
ISSN (print):3026-9091, ISSN (online): 1597-9962
Volume 3(4) July 2025
DOI: https://dx.doi.org/10.4314/jobasr.v3i4.4

# Machine Learning-Based Dynamic Queuing Model for Heterogeneous Traffic in Smart Home Networks

Zainab Abdulrazaq Tijjani[1*], Umar Illiyasu[2] & Yusuf Surajo[3]
[1,3]Computer Science Department, Umaru Musa Yar'adua University, Katsina State, Nigeria
[2]Computer Science Department, Federal University Dutsin-Ma, Katsina State, Nigeria
[*]Corresponding Author Email: zeeab93@gmail.com

**ABSTRACT**
Smart equipment in a house that allows remote automation, control, and monitoring a system that links and unifies differences is called smart home network. Devices can control and accessed via a central hub and can connect with one another, i.e., smart phone app or voice assistant. Sensors, smart appliances, and other gadgets that can interact with one another and react to user or system provider commands are the elements that make up a smart home network. In order to accommodate a high number of smart devices with different distributions and heterogeneous physical access (wired and wireless), smart home networks are expanding quickly. This leads to a variety of traffic patterns. To classify heterogeneous traffic flows in smart home networks by developing a dynamic queuing model based on machine learning and utilizing the Semi-Supervised Support Vector Machine (S3VM) is the goal of the work. We evaluate the performance of the QoS-level Pair Heterogeneous-sourced traffic model (QP-SH) against that of the proposed dynamic queuing system. Higher priority traffic might not need a smaller delay than lower priority traffic, because many advance QoS-aware scheduling techniques merely use the traditional IP type of service (ToS) information to determine priority metrics for deciding how to divide bandwidth. For instance, traffic from streaming devices needs a shorter maximum latency than traffic from medical sensors, although the former has a higher priority. Proposed network was evaluated using the MATLAB simulator, which was used to conduct simulation tests to verify the suggested model's performance. The MAL-DQ algorithm was compared with an existing queuing model, QP-SH, across metrics such as classification accuracy, throughput, and delay. The results shows that MAL-DQ outperformed QP-SH by achieving higher accuracy (average of 90.57% vs. 82.27%), better throughput (8.95 kbps vs. 7.02 kbps), and lower average delay (6.62 ms vs. 15.98 ms), confirming its suitability for smart home environments.

**Keywords:**
Smart Home Networks,
Heterogeneous Traffic,
Dynamic Queuing Model,
Machine Learning,
Semi Supervised Support Vector Machine,
Quality of Service,
Machine Learning-Based Dynamic Queuing Model.

## INTRODUCTION

Smart home network components including sensors, smart appliances, and other devices may interact with one another and respond to commands from the user or system provider. A smart home network is a platform that connects and integrates various smart appliances and device within a home to enable remote automation, control, and monitoring. These devices can be linked to one another and accessed and managed from a single location using a voice assistant or smartphone app.

Smart devices that need both wired and wireless heterogeneous physical access have led to the rapid expansion of smart home networks, which can handle a wide range of traffic types with different distributions.

In addition to the standard Quality of Service (QoS) metrics, traffic scheduling in a smart home network should take into account specific Quality of Experience (QoE) metrics. The most difficult problem that smart home gateways face when figuring out how to automatically schedule packets from multiple sources is determining their degree of criticality and fulfilling their maximum required delay. This is particularly true for delay-sensitive applications that demand QoS and QoE satisfaction from both home customers and ISPs.

Several scheduling algorithms have been developed in the past to handle different kinds of network traffic, with a focus on highcapacity hybrid priority queuing (HPQ) for high-speed network devices (Benacer et al.,

2018). The packet inserting order which took priority queuing (PQ) into account, was used to build the fixed priority approach.

A queuing mechanism that optimized bandwidth allocation in homes by using user-defined profile priorities networks. This solution is based on Software Defined Network (SDN) technology, which computes user profiles in a cloud-based central controller and pushes the resulting rules on a home gateway (Bakhshi and Ghita, 2016).

Several research works have been conducted to improve the traffic management in Smart Home Network such as (Zheng et al., 2017), (Butt et al., 2018), (Fan and Zhao, 2018) and (Chaabnia and Meddeb, 2018). The primary focus of these efforts is traffic control in smart home technologies. The term "traffic management" describes strategies and tactics for controlling and optimizing data flow within a smart home network. Numerous factors, such as the critical nature of application traffic and its maximum permitted delay, network congestion, quality of service (QoS), security threats, user experience, and network latency, make it challenging to implement a dynamic model for packet scheduling optimization in the smart home network.

In this paper, we proposes a machine learning-based dynamic queuing model for heterogeneous traffic that classifies traffic flows using certain header bits from a packet's traffic class field using the Semi-Supervised Support Vector Machine (S3VM).

This research project aims to classify heterogeneous traffic flows by creating a machine-learning-based dynamic queuing model for smart home networks utilizing S3VM. There are several different scheduling algorithms that have been created to handle different kinds of network traffic. They havesignificantly improved the high-capacity hybrid Priority Queuing (HPQ) device for high-speed networks (Benacer et al., 2018). The fixed priority HPQ algorithm is based on the Priority Queuing (PQ) technique, which considers the priority order of inserted packets.

Due to the ability to integrate the real and virtual worlds and the exchange of personal data generated by sensors, security is becoming increasingly crucial for Internet of Things systems. Internet of Things technology uses embedded devices, unlike PCs, laptops, and mobile devices. Low-level encryption techniques are also necessary for IoT. The goal of the article by Azrour et al. (2021) is to highlight security challenges and significant issues that are expected to arise in the IoT ecosystem with the aim of guiding authentication methods and create a secure IoT service.

Additionally, IoT nodes will be subjected to excessive, if not unacceptable, demands due to a complex computing paradigm (Jine Tang et al., 2022). After temporal correlation data has been analyzed using the data prediction approach, data is further minimized by modifying the appropriate spatial sample rate based on the spatial correlation of sensory data.

Moreover, a two-level queuing model that considers the theoretical delay to meet QoS requirements in LTE networks was contributed by Shakir and Rajesh (2017). First layer queuing sorts packets according to size, predicted departure time, and service time. A weighted fair queuing algorithm (WFQ) is used to schedule the packets into calendar discs after the calendar discs have been sorted by their frequency bands in the second layer of queuing. The corresponding packets are then selected using the weighted round-robin algorithm (WRR), a generated version of Fair Queuing (FQ) that allows the en/de queuing of a predetermined number of packets (weights) from each queue at each scheduling round.

Using a weighted Gittins index scheduler, Anand and de Veciana (2017) also suggested a multi-class scheduler that maximizes end-user quality of experience (QoE) in wireless networks by optimizing resource allocation based on the mean latency sensitivity of different application classes using mean flow delay.

In order to overcome the aforementioned limitations, Butt et al. (2018) created an across-layer scheduling system across fading channels. In terms of loss tolerance for loss-tolerant applications in the 5G wireless network, this framework satisfies QoE criteria while guaranteeing the lowest energy consumption requirements for QoS. The writers used stochastic optimization approaches to address the scheduling problem after characterizing it with the Markov decision process.

A routing table including the deployed nodes is produced by the suggested approach. The base station verifies the keys of the nodes that will communicate and exchange information. Once the nodes receive the signal from the base station, data is transmitted between them. Jlassi et al. (2021) proposed a novel and precise technique for identifying and averting attacks. When compared to RPC, the message authentication mechanism will increase throughput and speed up data transfer through the network. In the future, a unique approach for identifying Sybil assaults with a guarantee of network energy consumption will be required.

Additionally, by considering user-defined priority, Bakhshi and Ghita (2016) created a queuing model that optimizes bandwidth allocation in a home network. In their method, user profiles are calculated in a cloud-based central controller using Software Defined Network (SDN) technology, and the rules are then sent to a residential gateway. The authors use streaming video and multimedia apps to test their solution. Only a small percentage of users with high priority have demonstrated good packet loss and delay performance

using this strategy.

Abuteir et al. (2016) developed a Wireless Network Assisted Video Streaming (WNAVS) framework that uses SDN technologies. But unlike real home network traffic, their approach only addresses a single kind of home application.

Additionally**,** they compared time and memory usage across various protocols and found that their method has several advantages (Gupta et al., 2021). However, they also noted that their strategy remains susceptible to offline password guessing attacks. Their revised protocol addresses these issues and has been verified as secure through both formal and informal evaluation.

Zheng et al. (2017), Butt et al. (2018), Fan and Zhao (2018), and Chaabnia and Meddeb (2018) conducted studies to improve traffic management in smart home networks. These works mainly concentrate on traffic control in smart environments. Traffic management is a component of smart home networks that uses techniques and strategies to regulate and enhance data flow witin a network. Considering the critical nature of application traffic, along with its maximum allowed delay, quality of service (QoS), security risks, user experience, and latency, it is challenging to implement a dynamic model for packet scheduling optimization in the smart home network due to network congestion.

The concept by Yaseen et al. 2022) uses a 1D-CNN model to prioritize traffic flows based on precedence levels, and SDN offers great control to provide the required flow priority to Security, Health, and Emergency (SHE) data traffic. However, there are obstacles toclassifying arriving packets at the SDN gateway using a 1D Convolutional Neural Network (1D CNN) model.

It can be difficult to collect a large amount of labeled data in network traffic situations, which is typically necessary for training 1D-CNNs successfully. On the other hand, S3VMs may utilize both labeled and unlabeled data, they are more suited for situations where there is a shortage of labeled data. For low-resource smart home gateways, 1D-CNN may not be the ideal choice because it requires large amounts of memory and processing power. Higher latency and power consumption can negatively impact the network's overall performance.

1D-CNNs feature more intricate hyperparameter tuning than S3VMs, which may requires more expertise and effort during the model-development phase. To address the aforementioned problems, this research proposes an enhanced dynamic queuing model for smart home networks accurately classify traffic using a Semi-Supervised Support Vector Machine (S3VM) classifier to examine the traffic patterns of various applications. Furthermore, QoS policies based on the S3VM paradigm are used to control the classified traffic flows for every application.

Despite advancements in smart home traffic management, existing solutions exhibit critical limitations that hinder optimal performance in heterogeneous environments. Traditional queuing mechanisms such as Priority Queuing (PQ), Weighted Fair Queuing (WFQ), and Hybrid Priority Queuing (HPQ) often rely on static packet classification methods that do not account for dynamic traffic behaviors or Quality of Experience (QoE) requirements. Moreover, models utilizing deep learning algorithms, particularly 1D-Convolutional Neural Networks (1D-CNNs), demand extensive labeled datasets and significant computational resources. This poses a challenge for real-time deployment in resource-constrained smart home gateways.

Furthermore, most prior models do not effectively differentiate between traffic types based on criticality and latency sensitivity, leading to inefficient bandwidth allocation and increased delay for high-priority applications such as emergency health monitoring. The reliance on static precedence values, such as those derived from IP Type of Service (ToS), often results in misaligned traffic prioritization, particularly when latency-sensitive traffic receives lower practical priority due to fixed classification schemes.

These gaps highlight the need for a lightweight, adaptive, and efficient traffic classification and queuing model that:

- Can learn from limited labeled data
- Is computationally feasible for smart home environments
- Accounts for QoS and QoE simultaneously
- And dynamically prioritizes heterogeneous traffic.

This research addresses these challenges by introducing a Machine Learning-Based Dynamic Queuing (MAL-DQ) model that leverages a Semi-Supervised Support Vector Machine (S3VM) to enhance traffic classification and scheduling, thereby improving smart home network performance across accuracy, delay, and throughput metrics.

## MATERIALS AND METHODS

### MODEL OF DYNAMIC QUEUING BASED ON MACHINE LEARNING (MAL-DQ)

Through the smart home gateway, different Quality of Service (QoS) levels of traffic are managed. Every home network includes a variety of things, including sensors, electronics, appliances, and entertainment devices like tablets, smartphones, and linked TVs.

Sensors are devices that can capture data about circumstances (open windows, temperature, shattered glass, energy use, doors, and motion etc.) determine the location of persons and objects. Examples of electronic devices include phones, televisions, and laptops. Examples of electrical gadgets include light bulbs, kettles, and toasters. Washing machines, refrigerators are examples of appliances. Health support, safety, energy efficiency, and monitoring can be used for variety of purposes.

Figure 1 depicts the three modules that comprise the home gateway are Classifier, Scheduler, and Service. In this study, a semi-supervised support vector machine (S3VM) classifier is employed to categorize network packets according to their priorities. The proposed smart home gateway is implemented using the Machine Learning-Based Dynamic Queuing Model (MAL-DQ).

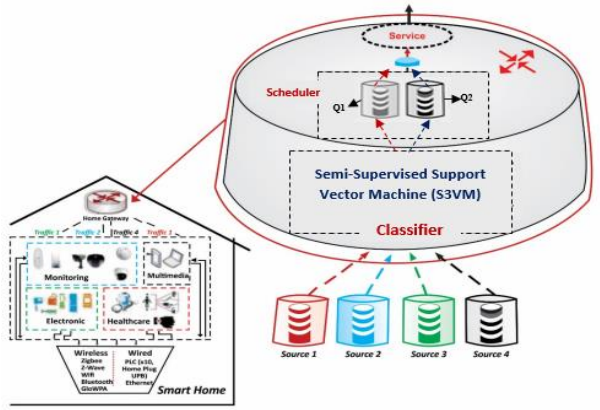


**Figure 1: MAL-DQ Model in Smart home gateway**

When incoming packets from various sources reach the gateway, the S3VM classifier will categorize them according to the attributes that were extracted from the packets. The categorized packets will then be sent to the scheduler. The scheduler divides classified packets into two queues according to their level priority. Q1 receives packets with a priority of 1, and Q2 receives packets with a priority of 2.

When classifying incoming packets, the S3VM classifier in the proposed MAL-DQ paradigm chooses the relevant header bits from the traffic class field rather than analyzing all 320-bit header bits. The service module will give the higher priority queue (Q1) precedence over the lower priority queue (Q2) after processing the packets from the queues.

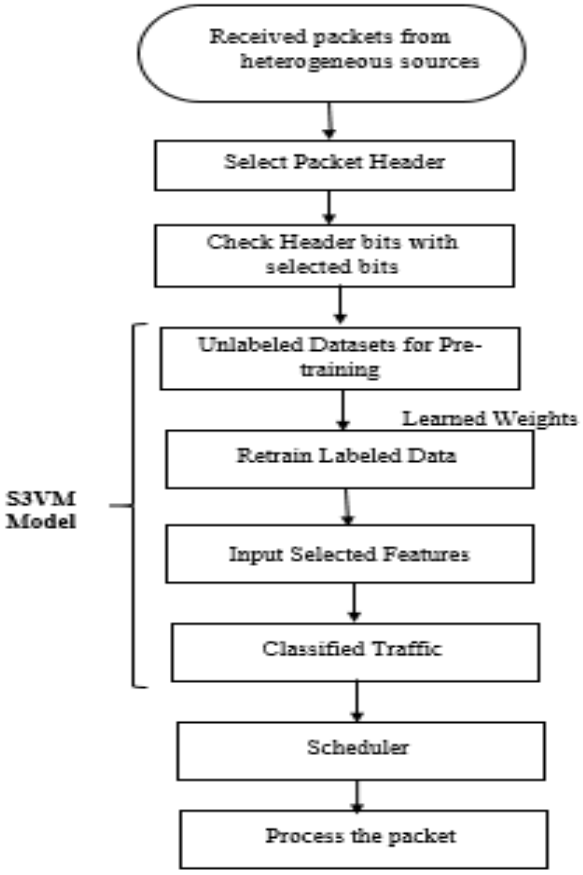


**Figure 2: The MAL-DQ Model**

Using S3VM, the process of identifying the most representative characteristics of traffic flow classes is automated by the MAL-DQ model. The learning information for the semi-supervised support vector machine (S3VM) is obtained from datasets with and without labels. A few categorized datasets are combined with a lot of unlabeled data to feed the machine learning system and categorize the data flow.

As the data flow enters the classifier sequentially, the machine learning classifies the three columns of the matrix-bit position, packet number, and packet direction. To enable the S3VM to extract learned weights during pre-training, different portions of the unlabeled dataset were sampled several times. To extract certain flow elements, these weights are used for re-training on labeled datasets. The header bits are used by the S3VM model to extract flow characteristics. Figure 3.4 show that the IPv6 header bits are 320. The inferred features of the data flow based on the selected bits are specified by the header bits' location and arrangement. In order words, the traffic flow's characteristics are determined by the order in which the header bits are chosen.

The S3VM at this point, classifies traffic based on the header bits that were selected. Figure 2 shows that the scheduler has received the categorized traffic and will queue it up for either Q1 or Q2. The service module will process the highest priority queue (Q1) before moving on to the lowest priority queue (Q2).

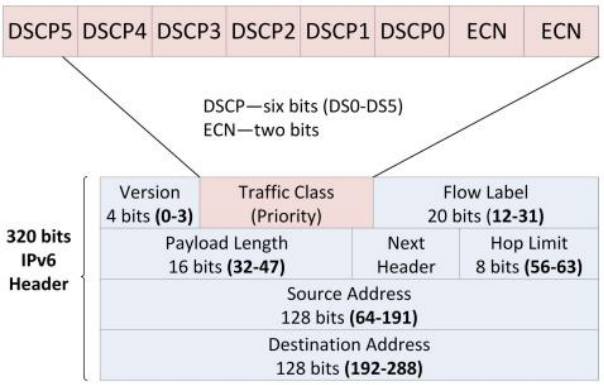


**Figure 3: IPv6 packet header fields and bits order**

**DIFFERENTIATED SERVICES BASED ON S3VM**

S3VM controls the Differentiated Services Code Point (DSCP) bits to give priority levels to classified traffic using network administrator policies. In the proposed system, packets are prioritized by the MAL-DQ algorithm according to the drop probability bits (DS2-DS1) and DSCP bits (DS5-DS3). In the DSCP, which employs precedence bits as shown in Table 3.1, the three most important bits (DS5, DS4, and DS3) establish the priority and "low" drop probability. According to Yaseen et al. (2019), the traffic class (8-bit) field of an IPv6 packet indicates its priority. It enables traffic flow control by gateways according to packet priority. In cases where network equipment is overloaded, the lowest priority packets are either dropped or classified as "routine traffic."

**Table 1: DSCP precedence level**

| Precedence Level | Description |
|---|---|
| 0 | Best Effort |
| 1 | Class 1 |
| 2 | Class 2 |
| 3 | Class 3 |
| 4 | Class 4 |
| 5 | Express Forwarding (EF) |
| 6 | Apply common IP routing protocols |
| 7 | Link layer & network layer keep alive |

**MAL-DQ ALGORITHM**

The MAL-DQ model, which uses a Support Vector Machine (SVM) classifier, is introduced in Algorithm 1 for handling heterogeneous network traffic in a smart home network. The system uses particular header bits from a packet's traffic class field to classify and regulate traffic.

**Algorithm: MAL-DQ ALGORITHM**

**Input:** *IncomingPacket*
**Output:** *ProcessedPacket*
1: Initialization
2: WHILE network IS ACTIVE
3: HighPriorityQueue = [ ]
4: LowPriorityQueue = [ ]
5: **IF** NEW_PACKET_ARRIVED
6: packet = RECEIVE_PACKET(*IncomingPacket*)
7: headerBits = GET_HEADER(packet)
8: selectedBits = EXTRACT_HEADER_BITS(packet)
9: trafficClass = S3VMClassifier.CLASSIFY(selectedBits)
10: **IF**trafficClass == "HighPriority"
11: ENQUEUE packet INTO HighPriorityQueue[trafficClass]
12: **ELSE**
13: ENQUEUE packet INTO LowPriorityQueue[trafficClass]
14: **END IF**
15: **END IF**
16: **IF**HighPriorityQueueIS NOT EMPTY
17: packet = DEQUEUE(HighPriorityQueue)
18: **ELSE**
19: packet = DEQUEUE(LowPriorityQueue)
20: **END IF**
21: **END WHILE**

**EXPERIMENTS**

A sample setting showing how S3VM is implemented in the SHE in MATLAB with a number of IoT nodes is shown in figure 5. 5, 10, 15, 20, 25, and 30 mobile nodes were used to examine the results of the simulation.

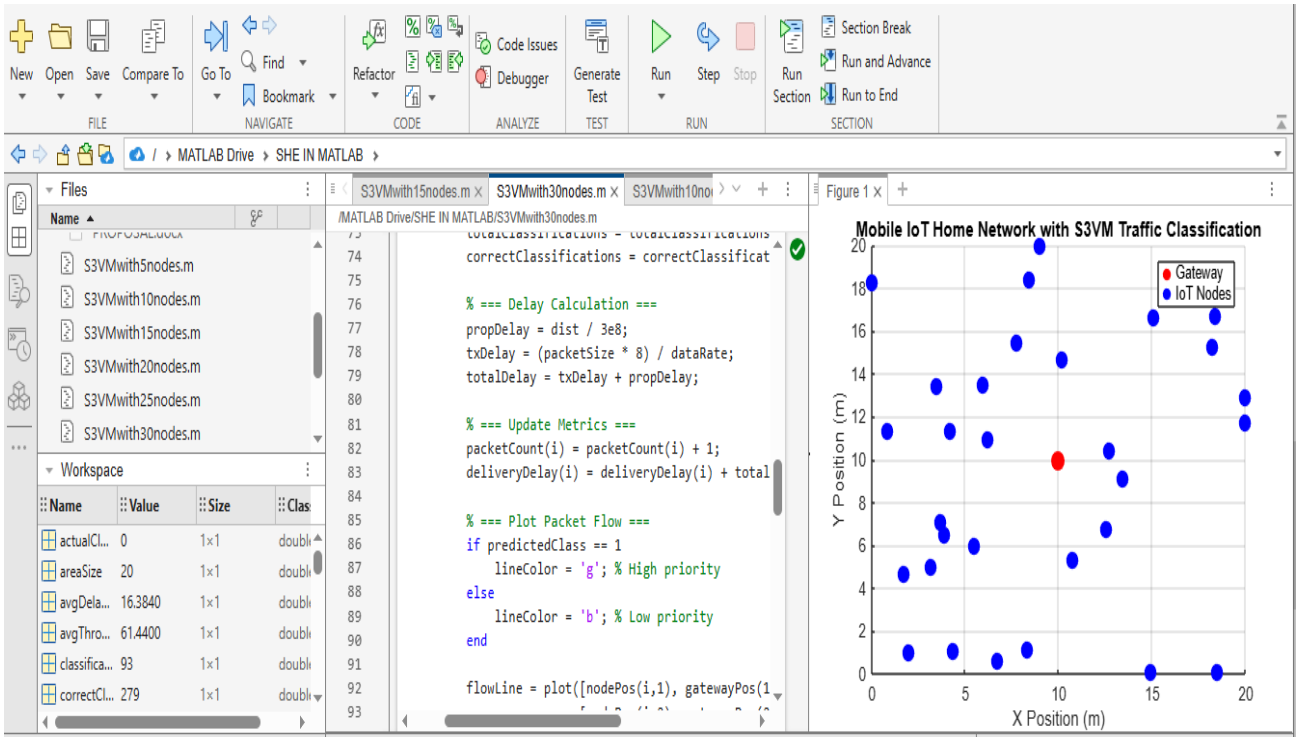


**Figure 4: Simulation Environment**

One of the most effective platforms for modeling, simulating, and analyzing complicated physical systems is the MATLAB simulation environment. PID controllers and state-space models are among the control schemes it implements. Here, MATLAB's interactive environment speeds up the research process to test and improve the idea and produces excellent plots, charts, and graphs to illustrate their data to integrate visualization capabilities. Based on the nodes used, it is easily shared and replicable, promoting collaboration and research result verification.

## RESULTS AND DISCUSSION

The simulation experiment conducted to confirm the effectiveness of the MAL-DQ algorithm. The aim of the study was to analyze the performance of the proposed Machine Learning-Based Dynamic Queuing Model (MAL-DQ) in smart homes. A 2019 study by Yaseen et al. found that gateways can allow traffic flow based on packet priority. In the proposed MAL-DQ algorithm, the following network performance indicators are considered. In the event of network device congestion, the packets with the lowest priority level are either dropped or considered "routine traffic".

The suggested IoT home network with S3VM was evaluated using the performance criteria listed below: **(1) Classification accuracy** is the proportion of correctly classified priority packets to total classifiedpriority packets. **(2) Throughput**: Indicates how many packets are successfully received within a given time. Bits per second (bps), kilobits per second (Kbps), megabits per second (Mbps), gigabits per second (Gbps), and so forth are the common units of measurement. **(3) Network delay** is the time it takes for a packet to travel between two communication endpoints. Measurements used are the milliseconds (ms), microseconds (µs), and other fractions of seconds. The parameters 5, 10, 15, 20, 25, and 30 mobile nodes were used to examine the results of the simulation for the accuracy and network performance of the mobile IoT home network with S3VM.

### Accuracy (AC) comparison between MAL-DQ and QP-SH

The accuracy of both QP-SH and MAL-DQ decreases slightly as the number of delays grows, according to the data shown in Figure 5. Due to packet collisions, this causes information loss and reduces accuracy. However, MAL-DQ outperforms QP-SH in detecting IoT nodes, maintaining higher accuracy rates even as the number of nodes increases. While QP-SH effectiveness diminishes more significantly with more nodes, MAL-DQ provides more consistent and reliable accuracy performance.

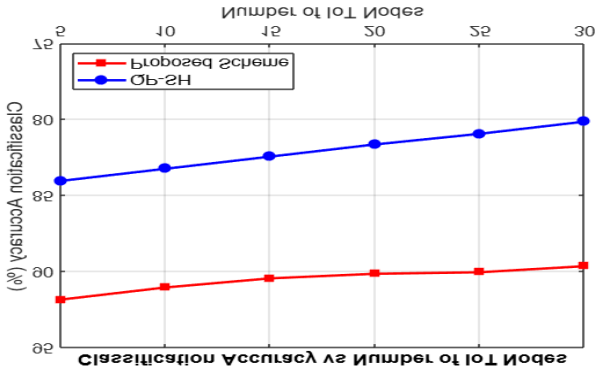

**Figure 5: Accuracy Comparison of QP-SH AND MAL-DQ**

**Table 2: Accuracy Comparison of QP-SH AND MAL-DQ**

| Number of IoT Nodes | Accuracy (%) | |
|---|---|---|
| | QP-SH | MAL-DQ |
| 5 | 84.2 | 92 |
| 10 | 83.7 | 91 |
| 15 | 82.9 | 90.5 |
| 20 | 82 | 90.2 |
| 25 | 80.8 | 90 |
| 30 | 80 | 89.7 |
| **Average** | **82.27%** | **90.57%** |

**Throughput Comparison of QP-SH and MAL-DQ**

Throughput is impacted by node speed, network topology changes, and scarce network resources. MAL-DQ is higher than QP-SH because of a malicious threat that causes communication to become unreliable as the number of IoT devices in the network increases. But in every studied case, MAL-DQ's throughput is still higher than QP-SH's, indicating that MAL-DQ may be better suited to managing network resources or handling larger node counts. MAL-DQ consistently provides higher throughput than QP-SH, both on average and at individual node count levels. Although both methods notice a decrease in throughput as the number of nodes rises, MAL-DQ maintains a superior performance throughout. This indicates that MAL-DQ might be more efficient in managing network resources and delivering better data transfer rates under varying traffic conditions.

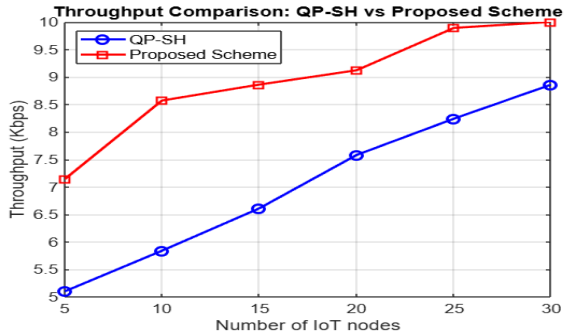


**Figure 6: Throughput Comparison of QP-SH AND MAL-DQ**

**Table 3: Accuracy Comparison of QP-SH AND MAL-DQ**

| Number of IoT Nodes | Throughput (kbps) | |
|---|---|---|
| | QP-SH | MAL-DQ |
| 5 | 5.0 | 7.1 |
| 10 | 5.8 | 8.6 |
| 15 | 6.6 | 8.9 |
| 20 | 7.6 | 9.2 |
| 25 | 8.2 | 9.9 |
| 30 | 8.9 | 10.0 |
| **Average** | **7.02** | **8.95** |

**Delay Comparison of QP-SH and MAL-DQ**

The delay of QP-SH and MAL-DQ is displayed below. The graph indicates that MAL-DQ has a higher delay than QP-SH because it requires more computation for estimate speed, which impacts the total delay experienced by the nodes. While the delay increases for both methods, QP-SH consistently provides higher delays compared to MAL-DQ, which is as a result of additional task of computing estimated speed. This suggests QP-SH may be more efficient in handling network traffic or managing communication protocols.

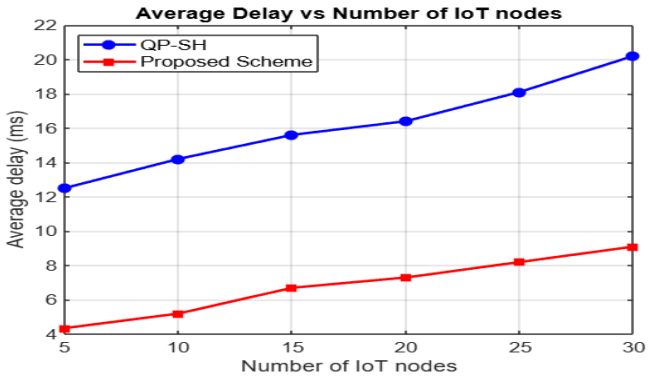


**Figure 7: Delay Comparison of QP-SH and MAL-DQ**

**Table 4: Delay Comparison of QP-SH and MAL-DQ**

| Number of IoT Nodes | Delay (ms) | |
|---|---|---|
| | QP-SH | MAL-DQ |
| 5 | 12.3 | 4.1 |
| 10 | 14.0 | 5.0 |
| 15 | 15.4 | 6.4 |
| 20 | 16.2 | 7.2 |
| 25 | 18.0 | 8.0 |
| 30 | 20.0 | 9.0 |
| **Average** | **15.98** | **6.62** |

## CONCLUSION

The S3VM model is the only method used to choose header bits from a packet's traffic class field in order to rank traffic flows based on precedence levels. It has not been applied to other supervised and unsupervised machine learning algorithms. For upcoming work, it is recommended that this be done. The results shows that MAL-DQ outperformed QP-SH by achieving higher accuracy (average of 90.57% vs. 82.27%), better throughput (8.95 kbps vs. 7.02 kbps), and lower average delay (6.62 ms vs. 15.98 ms), confirming its suitability for smart home environments. This significantly demonstrates how both labeled and unlabeled packet data can effectively utilized for traffic classification. This approach overcomes the limitation of requiring large labeled datasets, which is often a challenge in smart home environment. In order to achieve high classification accuracy, it shows that selecting specific bits from the IPv6 traffic field is sufficient and reduces computational overhead and allows the model to function efficiently on resource-constrained smart home gateways. Future work should focus on introducing adaptive features that allow the model to dynamically update packet priorities based on real-time network conditions or user-defined policies.

## REFERENCE

*Mehmat-AliM, Khabazian, M., & Aissa, S.* (2013). Performance model of safety message broadcasting in vehicular ad hoc networks. *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, ***14***(1), *380–387*. https://doi.org/10.1109/TITS.2012.2213595

A. Fladen Muller, O. Fourmaux, and R. M. Abuteir (2016). An SDN approach to adaptive video streaming in IEEE International Wireless Home Networks. 321–326, Wireless Communication. Mobile Computing. https://doi.org/Conf/(IWCMC).

J. He, Y. Zhang, S. Leng, and M. Zeng (2018). A matching-theoretic approach to QoE-aware power management in vehicle-to-grid networks. IEEE Transactions on Smart Grid, 9(4), 2468–2477.

Q. Huang, H. Chen, and QQ. Zhang (2020). Coordinated design of sensing and communication systems for smart homes. IEEE Transactions on Intelligent Transportation System, 34(6), 191-197.

F.-R. Boyer, Y. Savaria, and I. Benacer (2018). In the proceedings of the 16th IEEE International Conference on New Circuits and Switching (NEWCAS), HPQ: A hybrid priority queue architecture with large capacity for fast network switches was presented.

I.-H. Hou and P.-C. Hsieh (2018). QoE optimality for on-demand video streams over fading channels: a heavy-traffic analysis. IEEE/ACM Transaction on Intelligent Transportation Network., 26(4), 1768–1781.

S. S. H. Shakir and A. Rajesh (2017). The performance analysis of two-level calendar disc scheduling in an LTE advanced system with carrier aggregation. Wireless Pers. Commun., 95(3) 2855–2871. https://doi.org/10.1007/TITS.11277-017-3967

Fan S., Zhao H. (2018). Cross-layer delay-based QoS scheme for wireless ad hoc networks for streaming video. China Commun., 15(9) 215–234.

ShambelTseggaye Getaneh (2019). Enhanced Security Mechanism for VANET Sybil Attack Detection. The Paper Turned in to the Department of Information Technology to Comply with Part of the Master of Science in Computer Networks and Security Standards.

Zaidi, Taskeen, and Syed Mohd Faisal (2020), Time stamp-Based Sybil Attack Detection in VANET: International Journal of Network Security, https//doi.org/10.6633/IJNS.2020 0522(3).05.

Anand, A. and de Veciana, G. (2017). Measurement-based scheduler for multiclass QoE optimisation in wireless networks. IEEE INFO COM Conf. Comput. Commun., 1-9.

Ghita, B., and Bakhshi (2016). User-centric traffic optimization in residential software-defined networks. IEEE 23rd International Conference on Communications Technology (ICT), 1-6; T.

Bozkurt I-N. and Benson T. (2016). Contextual router: Bringing experience-oriented networking to the home, 15 Proc. ACM Symp. SDN Res.

Lukman Audah, Mustafa Maad Hamdi, Sameer Alani, and Sami Abduljabbar Rashid (2020). Prediction Based Efficient Multi-hop Clustering Approach with Adaptive Relay Node Selection for VANET. Journal of

Communications, 15(4). https://doi.org/10.12720/jcm.15.4.332-344

Kugali, Sandeep N. and Kadadevar, Sneha (2020). Vehicular ADHOC Network (VANET):- A Brief Knowledge. ISSN: 2278-0181 International Journal of Engineering Research & Technology (IJERT) Volume 9, Issue 06, June 2020 2020 ICASISET, May 16–17Chennai, India © 2021 eai.16-5-2020.2304038 EAIDOI10.4108.

A. Mohamed, E. A. Jorswieck, and M. M. Butt (2018). A system-level model for the trade-off between energy and bursty packet loss over fading channels. IEEE System Journal, Volume 12, Issue 1, pages 527–538.

H. Gao, J. Li, Z. Cai, and X. Zheng (2017). A study on wireless networks using application-aware scheduling. IEEE Trans. Mobile Comput., 16(7) 1787–1801.

Taoufik Yeferny and Sofian Hamad (2020). Vehicular Ad-hoc Networks: Architecture, Applications, and Challenges. International Journal of Computer Science and Network Security, 20(2). https://doi.org/10.48550/arXiv.2101.04539.

Hubaux J.P., Luo J., Capkun S. (2004). The security and privacy of smart vehicles, IEEE International Conference on Security & Privacy, 2(3) 49-55. https:/doi.org/10.1109/MSP.2004.26

Chaabnia S. and Meddeb A. (2018). Slicing aware QoS/QoE in software defined smart home network. Proc. NOMS IEEE/IFIP Netw.Oper.Manage. Symp., 1–5.

By Xiao L., Greenstein L.J., Mandayam N.B., and Trappe W. (2009). Channel-based detection of Sybil attacks in wireless networks. IEEE International Conference on Information Forensics and Security, 4(3) 492-503. https//doi.org/10.1109/TIFS.2009.2026454