My 'Smart' Fridge Slows Down Teams Calls: Exploring the Quality of Service in Domestic Properties with High Numbers of Internet of Things Devices

Thomas Boxall (up2108121)

15 December 2025

1635 words

Abstract

High Quality of Service between interconnected devices is a critical factor in ensuring smooth operation. With the rapid increase of numbers of Internet of Things devices seen within home networks and the amount of network traffic they generate, it has never been more important to automatically prioritise network traffic. This paper conducts a review into existing solutions to this problem and identifies a gap in the market. An Artificial Intelligence powered traffic prioritisation engine is proposed which automatically prioritises traffic based on attributes.

1 Introduction

The Internet of Things (IoT) is defined as "development of the internet in which many everyday objects are embedded with microchips giving them network connectivity, allowing them to send and receive data" (Oxford English Dictionary, 2025). The number of IoT devices have risen by approximately 10 trillion devices between 2019 and 2024, with this number predicted to grow to approximately 40 trillion by 2034 (Transforma Insights, 2025).

Smart home devices are a sub-category of IoT devices, providing technological function to non-technical devices. Some smart home devices are designed to communicate via WiFi or Ethernet protocols while others are designed to communicate using specialist protocols such as Zigbee or Z-Wave. Regardless of protocols the devices use to communicate - they will all generate some level of traffic on the Local Area Network (LAN) which they are connected to, whether this be for smart-phone control or receiving firmware updates. Smart home devices can often be combined together to create automations (Phillips Hue, n.d.-a), the software for which is designed to be end-user friendly allowing them to simply connect different appliances together (Phillips Hue, n.d.-b).

Within networking, an important requirement is Quality of Service (QoS). QoS is the idea of ensuring that the devices on the network are able to use enough bandwidth ensuring minimal functionality; and where the minimal bandwidth of the network is not enough, QoS prioritises high-priority over low-priority applications (Fortinet, n.d.). QoS is important in any network, especially within a domestic LAN where there are often high numbers of devices fighting for bandwidth, including IoT devices which can cause congestion on the network (Crissy Joshua, 2025).

This paper will first explore the background, gaining an understanding of the uprising of IoT. The underlying problem will be defined and a solution proposed utilising global usage data to construct an automated Artificial Intelligence (AI) traffic prioritisation model.

2 Background & Related Works

IoT devices are being seen more and more in the domestic setting. A survey (Stannard et al., 2020) found that approximately 140 out of 2000 people owned a smart kitchen appliance. This number is on the rise, with 40 of those claiming to have purchased their appliance within the previous five months (Stannard et al., 2020). These devices are often seen functioning in the paradigm of Machine-to-Machine (M2M) where the device is directly connected to another and the internet. While this can be a benefit to the automation of mundane daily tasks such as ordering more milk, IoT devices are often vulnerable and provide malicious actors easy targets to compromise whole networks (Kebande et al., 2017). Proofpoint (2014) discovered that over two weeks, approximately one million spam emails were sent from IoT devices. This type of attack is not uncommon (Bitdefender, 2025) with IoT devices attempting to be compromised on average 30 times a day. Each attack can use a significant amount of network bandwidth with one attack causing 3.7GB to be transmitted from one device in one day (Mark Tyson, 2024). According to Ofcom (2024) the average household daily data usage in the UK is approximately 17GB. Therefore an increase of over a fifth with a compromised IoT device on the network will have a negative effect on the QoS to the other users of the network.

An experimental traffic prioritisation system developed by Attia et al. (2019) uses a series of prioritised queues to organise traffic based on the required QoS as well as the needed Quality of Enjoyment (QoE). This combination allows for a more detailed prioritisation structure, for example recognising that CCTV systems could work on 7 frames per second (fps), but a TV requires a higher frame rate starting at 60 fps. The system explored how assigning a packet a maximum allowable delay offered them the ability to hold less-sensitive traffic, which whilst degraded individual devices network performance, did perform better overall compared to existing solutions. Attia et al. (2019) found that the system worked, demonstrating the importance of understanding the data on the network and the QoS required to maintain sufficient QoE.

Hager et al. (2012) developed an experimental traffic control system system for ethernet networks in which they ranked traffic from high priority control traffic; to time critical smart home applications; to all other smart home applications; and finally best effort. A higher class of traffic does not necessarily mean that there is a higher data-rate, or a higher frequency of transmission, rather recognising that when a packet of this class is detected - it's delivery is more important than others. Their study used a Linux server to run a bespoke traffic control algorithm which analysed the traffic on the network and through automatic identification of the packet's class using the destination port, it could be prioritised. A traffic measurement database added a heuristic for deciding to dynamically increase a traffic class' data rate. Their system also provided the capabilities for some networked devices to be assigned to a separate priority class - as to not impact the smart home devices while sharing the same network (Hager et al., 2012).

The traffic prioritisation systems presented by both Hager et al. (2012) and Attia et al. (2019) were successful in what they set out to achieve. Both present a different yet similar approach, with a common element being that they require some amount of additional hardware to run the application in addition to the router existing already in the network. Neither solution are especially applicable to domestic settings, due to their high complexity of implementation and operation.

There are a number of existing solutions to QoS management within domestic LANs. TP-Link provides instructions for configuring a built-in QoS feature within their Deco product range (TP-Link, 2024). UniFi also provide a more feature-rich set of options for managing QoS within the Network function of their gateway products (UniFi, n.d.). The UniFi options provide a comprehensive and granular set of controls to limit and/or prioritise traffic to/from certain devices on a schedule. This is a good solution as it provides the level of control that some users may be comfortable using; however it requires a substantial amount of technical knowledge to be able to define these policies.

3 The Problem

The underlying problem with QoS within domestic LANs is twofold; firstly the sheer volume of devices are to blame where the second issue, a poorly configured LAN, amplifies the QoS issues experienced. The first problem isn't solvable - people generally like IoT devices, finding them beneficial to their daily life (Kennedy et al., 2024). That leaves the second problem: poor QoS management within domestic networks.

There are existing solutions to this problem available on the market. However these existing solutions require an above-average technical ability to be able to implement and maintain them. Even the domestic options such as TP Link's offering require an understanding of technical network management to be able to effectively configure this; where someone with a menagerie of disparate smart home devices may not have these skills and therefore not be able to reap the benefits of them, leaving them with a poorly configured network with significant performance issues.

4 Proposed Solution

The proposed solution is to develop an application which is capable of running on domestic routers that automates traffic prioritisation ensuring good QoS while ensuring it is suitable for non-technical users to use. This solution may be applicable for some users, and not to others. The feasibility of implementing a product like this has not been studied as part of this paper.

This proposed application is powered by Artificial Intelligence (AI) wherein all routers running the application pass the cloud-based global AI model details of the traffic on the network and the model determines the priority of traffic based on its properties. These properties would include factors such as the type of device, the port used, usage patterns of the device, as well as any optional user defined priorities. The same model is being used by all routers running this application, to provide the model a vast dataset for rule generation.

The AI powered traffic prioritisation engine works in real time, where new devices or changes in existing devices are detected, the priority of all device on the network will be altered to suit current network conditions. A flowchart showing this process can be seen in Figure 1. Furthermore, it would be possible for this application to detect compromised device traffic and alert the user while automatically isolating the infected device to prevent subsequent infection of other devices within their network further aiding overall QoS for devices on the network.

There are a number of ethical considerations with this proposal. The key concern would be with the amount of data which needs to be shared with the AI model not just in the training stage but also in the utilisation stage. There would be a need to consider what data

the router needs to pass on, and what does not need to be passed on. For example, it would not be needed to pass on the contents of the payload of a frame, rather just the source and destination / port.

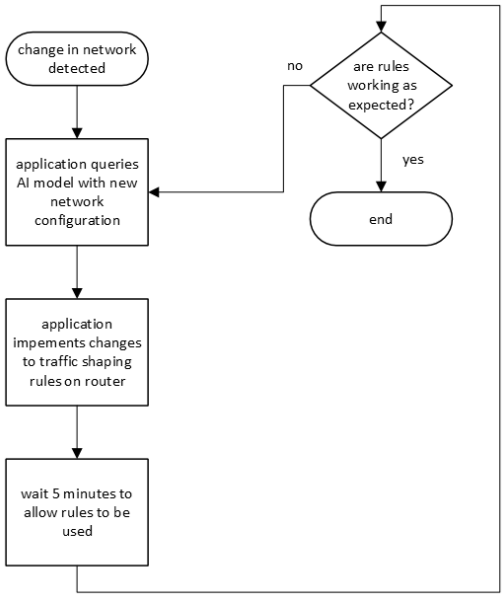

Figure 1: Proposed solution flowchart of operations

5 Conclusion

From this research, it can be clearly see that QoS is a significant and going concern within domestic LANs, especially those containing any number of IoT devices, which are on the rise. The competition between these devices fighting for network space to be able to communicate as they wish causes congestion on the network which leads to degraded QoS for other devices. Often the non-technical users administering their domestic networks do not have the skills to be able to manually prioritise network traffic, therefore the proposed solution would work towards a hands-off solution to this problem suitable for many domestic networks.

References

Attia, M. B., Nguyen, K.-K., & Cheriet, M. (2019). Dynamic qoe/qos-aware queuing for heterogeneous traffic in smart home. *IEEE Access*, *7*, 58990–59001. https://doi.org/10.1109/ACCESS.2019.2914658

Bitdefender. (2025). *The 2025 iot security landscape report* (tech. rep.). https://blogapp.bitdefender.com/hotforsecurity/content/files/2025/10/2025_iot_security_report.pdf

Crissy Joshua. (2025). Retrieved December 9, 2025, from https://uk.norton.com/blog/wifi/why-is-my-internet-so-slow

Fortinet. (n.d.). Retrieved December 9, 2025, from https://www.fortinet.com/uk/resources/cyberglossary/qos-quality-of-service

Hager, M., Begerow, P., Krasovsky, P., Renhak, K., & Seitz, J. (2012). Quality of service concept for smart home services. *2012 Fourth International Conference on Ubiquitous and Future Networks (ICUFN)*, 266–271. https://doi.org/10.1109/ICUFN.2012.6261708

Kebande, V. R., Karie, N. M., Michael, A., Malapane, S. M., & Venter, H. (2017). How an iot-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime. *2017 IST-Africa Week Conference (IST-Africa)*, 1–10. https://doi.org/10.23919/ISTAFRICA.2017.8102362

Kennedy, C., Head, T., Landzaat, W., & Duke, C. (2024). *Consumer survey on app stores, internet of things (iot) and connected places* (tech. rep.). https://assets.publishing.service.gov.uk/media/67055c9e30536cb927482e3c/Consumer_survey_on_app_stores__internet_of_things_and_connected_places.pdf

Mark Tyson. (2024). Retrieved November 29, 2025, from https://www.tomshardware.com/networking/your-washing-machine-could-be-sending-37-gb-of-data-a-day

Ofcom. (2024). *Connected nations uk report 2024* (tech. rep.). https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/multi-sector/infrastructure-research/connected-nations-2024/connected-nations-uk-report-2024.pdf?v=386497

Oxford English Dictionary. (2025, December). 'internet of things' in internet, n. Oxford University Press. https://doi.org/10.1093/OED/9540187193

Phillips Hue. (n.d.-a). Retrieved December 9, 2025, from https://www.philips-hue.com/en-gb/explore-hue/works-with/the-google-assistant

Phillips Hue. (n.d.-b). Retrieved December 9, 2025, from https://www.philips-hue.com/en-gb/explore-hue/works-with/the-google-assistant/set-up

Proofpoint. (2014). Retrieved November 29, 2025, from https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack

Stannard, J., Writer-Davies, R., Spielman, D., & Nurse, J. (2020). *Consumer attitudes towards iot security report* (tech. rep.). https://assets.publishing.service.gov.uk/media/607d7e588fa8f57358f07e60/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf

TP-Link. (2024). Retrieved November 26, 2025, from https://www.tp-link.com/us/support/faq/1601/

Transforma Insights. (2025). Retrieved December 9, 2025, from https://www.statista.com/statistics/1194701/iot-connected-devices-use-case/

UniFi. (n.d.). Retrieved November 26, 2025, from https://help.ui.com/hc/en-us/articles/204911354-UniFi-QoS-and-Traffic-Shaping