ADVANCED MESSAGE QUEUING PROTOCOL TRANSPORTED OVER QUIC

FAHEEM IQBAL
01-245201-002

SUPERVISED BY: Dr. MONEEB GOHAR

A thesis submitted in fulfilment of the requirements for the award of degree of Masters of Science (Telecom & Networking)

Department of Computer Science

BAHRIA UNIVERSITY ISLAMABAD

APRIL 2022

Approval of Examination

Scholar Name: **Faheem Iqbal**

Registration Number: **66445**

Enrollment: **01-245201-002**

Program of Study: **Master of Science in Telecom & Networking**

Thesis Title: **Advanced Message Queuing Protocol Transported Over QUIC**

It is to certify that the above scholar's thesis has been completed to my satisfaction and, to my belief, its standard is appropriate for submission for examination. I have also conducted plagiarism test of this thesis using HEC prescribed software and found similarity index **4%**, that is within the permissible limit set by the HEC for the MS degree thesis.

I have also found the thesis in a format recognized by the BU for the MS thesis.

Principal Supervisor Signature:

Principal Supervisor Name: **Dr. Moneeb Gohar**

Date: April 12, 2022

Author's Declaration

I, **Faheem Iqbal** hereby state that my MS thesis titled **"Advanced Message Queuing Protocol Transported over QUIC"** is my own work and has not been submitted previously by me for taking any degree from Bahria university or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw/cancel my MS degree.

Name of Scholar: **Faheem Iqbal**

Date: April 12, 2022

Plagiarism Undertaking

I, solemnly declare that research work presented in the thesis titled

"Advanced Message Queuing Protocol Transported over QUIC"

is solely my research work with no significant contribution from any other person. Small contribution / help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Bahria University towards plagiarism. Therefore I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred / cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the university reserves the right to withdraw / revoke my MS degree and that HEC and the University has the right to publish my name on the HEC / University website on which names of scholars are placed who submitted plagiarized thesis.

Name of Scholar: **Faheem Iqbal**

Date: April 12, 2022

Dedication

Dedicated to my beloved Parents, Wife and Daughter.

Acknowledgements

All praise is to the Almighty Allah, the most gracious, the most compassionate, and the most merciful. I am thankful to the Almighty Allah, who has given me the courage and skills to make this small contribution to knowledge.

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have helped me to better understand and think about things. I'd like to express my gratitude to Dr. Moneeb Gohar, my thesis supervisor, for his support, direction, criticism, counsel, and motivation. This thesis would not have been the same if it hadn't been for his continual interest and encouragement.

I am also grateful to all of my colleagues and those who have helped me on various occasions. Their suggestions and viewpoints were quite insightful. Unfortunately, it is not possible to list all of them in this limited space. All of my family members, especially my parents, wife, and loving daughter, deserve my gratitude.

Faheem Iqbal
Islamabad, Pakistan
April 12, 2022

“And it ought to be remembered that there is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things”

Niccolo Machiavelli

Abstract

The use of IoT devices is expanding every day in today's environment. An interoperable protocol like AMQP is essential for supporting multiple IoT use cases and interconnecting IoT devices from different providers. Many IoT applications are sensitive to delays, which researchers are working to avoid as much as possible. One of the main sources of the delay is the underlying transport layer protocol, such as TCP or UDP. TCP is more reliable than UDP, although it is slower due to the three-way handshake and the use of TLS for security. QUIC, a new transport layer protocol developed by the Internet Engineering Task Force, combines the finest aspects of UDP and TCP to provide quick and reliable communication. We used the Go programming language to implement AMQP over QUIC to reduce latency and improve battery life. The Docker tool was used to containerize the AMQP Broker, Sender, and Receiver implementations, and various scenarios were tested in the NS3 simulator. The performance of AMQP over TCP and AMQP over QUIC has been evaluated using variables such as Delay, Packet Loss, and Channel Bandwidth. In addition, the battery usage has been calculated. With the exception of low bandwidth conditions, where AMQP over QUIC takes longer to communicate than AMQP over TCP, the results show that AMQP over QUIC outperforms AMQP over TCP in all cases.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS & ABBREVIATIONS

AMQP	Advanced Message Queuing Protocol
BW	Bandwidth
CoAP	Constrained Application protocol
DDOS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication
Kbps	Kilo Bits Per Second
Kbytes	Kilo Bytes
KPI	Key Performance Indicator
LAN	Local Area Network
MQTT	Message Queuing Telemetry Transport
NS3	Network Simulator 3
OASIS	Organization for the Advancement of Structured Information Standards
QoS	Quality of Service
RFC	Request For Comments

RTT	Round Trip Time
RV	Rakhmatov Vrudhula
SASL	Simple Authentication and Security Layer
SCTP	Stream Control Transmission Protocol
SWIG	Simplified Wrapp er and Interface Generator
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
XEP	XMPP extensions
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
XSF	XMPP standards Foundation

CHAPTER 1

INTRODUCTION

This chapter presents an overview of the Internet of Things (IoT) and its characteristics. It also gives an overview of the protocols that are utilised in IoTs, as well as the significance of latency. Finally, and most importantly, the research's scope and objective are determined.

1.1 Introduction to IoT

The Internet of Things (IoT) refers to objects that are connected to the internet. IoTs do not have a single universal or standard definition. These gadgets have an embedded system that collects data, processes it, and sends it to other devices. The communication with the internet is the only distinction between IoTs and wireless sensor networks. Wireless sensor networks are not directly connected to the internet, whereas IoT devices are. Instead, the sensors are connected to the central node, also known as the Cluster Head, which is then connected to the internet. The goal of the Internet of Things is to connect relatively inept items, like as temperature sensors, to the internet. Mostly IoTs have limited resources in terms of storage, computation, battery etc. [1] provides a more comprehensive definition of IoT, encompassing both physical and virtual things which can be identified and connected to the internet. IoTs have many use cases like smart cities, smart grids, telemetry, smart manufacturing, smart agriculture etc. These devices can be densely deployed and their number is very huge i.e. in billions. According to a study carried by CISCO [2] number of devices connected to IP are expected to reach 29.3 billion up from 18.4 billion in 2018, which will more than three folds of global human population.

1.2 Characteristics of IoT devices

ITU-T Y-2060 recommendations[1] identifies four fundamental characteristics of IoT devices which are as under:

1.2.1 Inter-connectivity

Inter connectivity is the core requirement for IoT devices and this characteristic differentiate IoT from wireless sensor network. The devices need to be connected to the internet so that they remain accessible at all time from all the locations.

1.2.2 Enormous scale

IoT devices are everywhere and their number is very huge which is ever increasing. Therefore, the networks need to be established to accommodate such huge number of devices. The capacity need to be built and more IPs need to made available i.e. shift from IPV4 to IPV6 is imminent.

1.2.3 Heterogeneity

IoT devices are manufactured by many different vendors and unfortunately no specific standard is being followed due to which devices differ to a great extend. Moreover, there are different use cases of IoT devices which completely have different sets of requirements. For instance, remote surgery, industrial manufacturing, autonomous vehicles etc. are very sensitive to delay and very high precision is required. On the other side, temperature sensing device for weather forecasts etc. does not have such stringent requirements. Capabilities of the devices also differ, depending on their use case. Few have limited battery resources, while other do not have any such constraints, hence, heterogeneity pertaining to capabilities of the devices, the way these devices communicate and transport data is at higher end.

1.2.4 Dynamic change

The main purpose of IoT devices is to gather data from the surroundings, which is changing from time to time. Therefore, the IoT devices also need to adapt to these changes like changing states from connected mode to sleeping mode and vice versa. Moreover, the requirements may change as new devices get connected to the internet, generating new insights. Hence, dynamic change is the prime characteristic of IoTs.

1.3 IoT Protocols

IoT use cases have different requirements, therefore, a single application layer protocol does not fit for all. Consequently, there are many application level protocols currently being used, a few of which are as under:

- Message Queuing Telemetry Transport (MQTT)
- Constrained Application protocol (CoAP)
- Extensible Messaging and Presence Protocol (XMPP)
- Advanced Message Queuing Protocol (AMQP)

These protocols have their own advantages and disadvantages due to which selecting a specific protocol for IoT device is a challenge [3]. Authors in [4] present comprehensive overview of different IoT protocols along with strengths and weakness of each, which can be helpful in choosing the desired protocol for a particular use case. However, there is a dire need for having an interoperable and extensible protocol to cater for heterogeneity and adopting to the evolving new use cases of IoTs. Keeping these requirements in view, XMPP and AMQP standout from rest of the protocols. XMPP does not provide any QoS and encoding is text based, whereas AMQP provides three level of QoS and supports binary encoding.

1.4 Latency

Latency is an important parameter for many IoT use cases and researchers are working to find out ways to reduce it as much as possible. Researchers in [5] studied the performance of MQTT broker in smart city scenario and showed that latency is impacted by bandwidth and hardware resources. One of the factors introducing delay in communication is the underlying transport protocol like TCP (Transmission Control Protocol) and UDP (User datagram Protocol). TCP uses three-way handshake for establishing connections and depends on TLS for security due to which additional delay occurs. Although TCP provide reliable communication yet it is slow. Moreover, it faces issues like head of line blocking, half open connections etc. A detailed discussion on the issues being faced by TCP in IoT scenario are presented in [6]. On the other hand, UDP provides quick but unreliable communication which is not desirable in many IoT scenarios. Recently a new protocol [7], QUIC has been standardization at IETF whose aim is to combine the good qualities of both UDP and TCP so that quick and reliable communication can be realized. Moreover, QUIC can solve various problems being faced by TCP like head of line blocking, half open connections, sending keep alive messages for maintaining established connections etc. which will be very beneficial for IoT scenarios.

1.5 Research Significance

The prime purpose of this research was to reduce delay in communication and prolong battery life of the device. More specifically the below mentioned research questions were to be addressed:

1. How to achieve quick and reliable communication in IoT devices?

2. How to prolong battery life of IoT devices while ensuring reliable transmission of data?

We transported AMQP over QUIC protocol to address the aforementioned research questions. We chose AMQP because it is an interoperable and extendable protocol that would handle interconnectivity in a heterogeneous IoT environment. Using QUIC instead of TCP, on the other hand, lowered communication time because cryptographic and transport parameters could be exchanged between client and server in a single QUIC handshake. As a result, communication time was significantly reduced. Furthermore, because the communication time was shortened, QUIC assisted in extending the battery life of IoT devices.