



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Escola Tècnica Superior d'Enginyeria
de Telecomunicació de Barcelona



QUIC sobre IP Multicast

Treball Final de Grau realitzada a
l'Escola Tècnica d'Enginyeria de Telecomunicació de Barcelona
Universitat Politècnica de Catalunya
per

Enric Perpinyà Pitarch

En compliment parcial
dels requisits per al Grau en
Serveis i Sistemes de Telecomunicacions **ENGINYERIA**

Director: Jorge Mata Díaz
Barcelona, Data 2022



Contents

List of Figures	3
List of Tables	3
1 Introducció	6
1.1 Transfons del project	7
1.2 Objectius	7
1.3 Requeriments i especificacions	8
1.4 Pla de feina	9
1.4.1 Estructura de la feina	9
1.4.2 Paquets de feina, tasques i fites	10
1.5 Diagrama temporal (Diagrama de Gantt)	14
2 Estat de l'art sobre les tecnologies utilitzades	15
2.1 Contexte de QUIC	15
2.2 QUIC	15
2.2.1 QUIC: establiment de la connexió	16
2.2.2 QUIC: Migració	16
2.2.3 QUIC: capçaleres més dinàmiques	17
2.2.4 QUIC: Multiplexat	17
2.2.5 QUIC: Control de fluxe a nivell de connexió i de paquets de dades	18
2.2.6 QUIC: Autenticació i encriptació de la capçalera i càrrega útil	18
2.3 Multicast	18
2.3.1 Multicast: IGMP	19
2.3.2 Multicast: la seguretat	19
2.4 Programes i software important	19
3 Section 3	20
3.1 Subsection	20
4 Section 4	22
4.1 Subsection 4.1	22
4.2 Subsection 4.2	23
5 Section 5	24
5.1 Overview	24
6 Experiments and results	25
7 Budget	26
8 Environment Impact (Optional)	27
9 Conclusions	28
10 Future Work	28
Appendices	29

List of Figures

1	Trafic d'Internet	6
2	Trafic d'Internet	8
3	Diagrama de Gantt del projecte	14
4	Comparativa establiment connexió entre TCP+TLS i QUIC. Imatge de Cloudflare.	16
5	Unicast vs Broadcast vs Multicast	18
6	Prototype setup	22

Listings

List of Tables

1	This is the caption	23
---	-------------------------------	----

Abstracte

El present document descriu i compara la implementació d'una estació de radio IP fent ús de la tecnologia QUIC sobre multicast i sobre unicast per retransmetre contingut en temps real. L'objectiu és demostrar que l'ús de multicast és millor per distribuir aquest tipus de contingut en termes d'escalabilitat, energètics i econòmics. També es discuteix les dificultats i avantatges tècniques de l'ús de QUIC sobre multicast (Draft QUIC over Multicast, Pardue i Hurst) com la gestió de Connection IDs o l'ús d'RTP i RTCP per capes superiors i la seguretat.

Revision history and approval record

Revision	Date	Purpose
0	05/03/2022	Document creation
1	dd/mm/yyyy	Document revision

DOCUMENT DISTRIBUTION LIST

Name	e-mail
Enric Perpinyà Pitarch	enric.perpinya@estudiantat.upc.edu
Jorge Mata Díaz	jorge.mata@entel.upc.edu

Written by:		Reviewed and approved by:	
Date	05/03/2022	Date	dd/mm/yyyy
Name	Enric Perpinyà	Name	Jorge Mata
Position	Project Author	Position	Project Supervisor

1 Introducció

En els darrers anys, els serveis de contingut en temps real han experimentat un creixement quasi exponencial, sobretot arran de la popularitat de pàgines web com [youtube.com](https://www.youtube.com), [twitch.tv](https://www.twitch.tv) o sobretot amb l'ús de les videoconferències durant la pandèmia. No obstant això, les tècniques actuals per distribuir aquest tipus de contingut, malgrat haver millorat bastant amb el desenvolupament d'eines com WebRTC, encara és un problema molt greu tant a la part dels servidors, principalment per les CDN, com també pel volum de tràfic que implica a les xarxes, principalment pels ISP. De fet, s'està tornant una qüestió tecnològica tant greu que molts serveis d'aquests han decidit pujar els seus preus per poder fer front a la demanda.

Al mateix temps que hi ha aquest augment de la demanda per serveis nous d'Internet, també hi ha altres que estan intentant canviar de plataforma de distribució tecnològica com la televisió i la ràdio; és a dir, les cadenes de televisió estan intentant transmetre el seu contingut utilitzant Internet en lloc d'antenes o per cable utilitzant un canal freqüencial destinat per elles. De fet, fer-ho a través d'Internet permet estalviar costos significatius de distribució al mateix temps que permet tenir una retroactivitat i perspectiva més acurada de la quantitat de gent que està veient l'emissió.

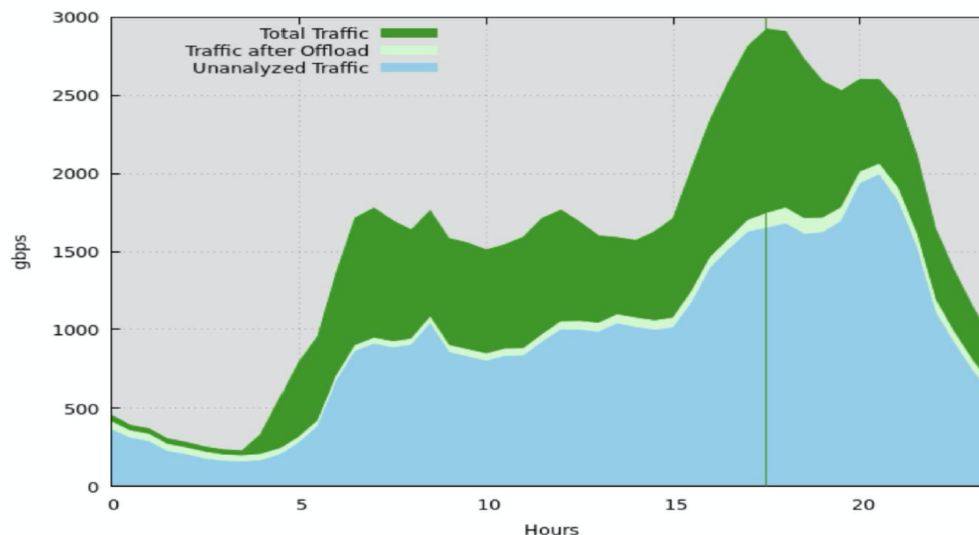


Figure 1: Volum de tràfic en un dia amb la sortida d'un nou videojoc. En blau el tràfic no analitzat, en verd fort el tràfic normal, en verd fluix el tràfic si la descarrega es fes amb multicast. Imatge d'Akamai.

L'any 2015, el tràfic de serveis de vídeo en temps real, com Netflix, YouTube o Twitch, va representar pràcticament el 70% del tràfic. Normalment, aquest tipus de tràfic ja per pocs, ja que quan una nova temporada d'una sèrie famosa, quan un youtuber important puja un nou vídeo o s'està fent un esdeveniment en directe la quantitat de gent veient el contingut sol augmentar de manera sobtada sobretot als primers moments. Això sol implicar en general problemes per donar accés a tothom al servei depenent de quanta gent sigui, mentre que al mateix temps altres serveis també es vegin afectats (les CDN solen tenir molts serveis simultàniament distribuïts en microserveis).

Per ficar dades i posar-nos en context del volum de tràfic, el màxim que s'ha arribat a donar simultàniament per part de la CDN Akamai ha estat un pico de 167 Tbps en abril de 2020. Suposant un tràfic lineal, per simplificar, ja que normalment s'utilitzen codificacions CBR en directe en temps real, amb una resolució de 1080p el tràfic és de 5 Mbps/connexió i fins a 20 Mbps/connexió en cas de 4k. Llavors, en 1080p suposant aquell tràfic màxim suportat llavors es podrien arribar fins a 33.4 milions de clients en 1080p i fins a 8.35 milions en 4k. Si tota Espanya volgués mirar un contingut en directe, seria impossible donar el servei.

Aquests problemes de subministrament solen ser a causa que les connexions que es fan són punt a punt; dit d'una altra manera, són unicast. Això implica que el servei que pots donar en gran part està limitat

al nombre de connexions simultànies que es pot donar. Malgrat que l'ús d'unicast té grans avantatges com la facilitat en la seguretat, la simplificació en l'arquitectura del programa o que pràcticament tots els dispositius del món suporten, també comporta un gran inconvenient.

Si el contingut que has de distribuir als clients és exactament el mateix com en el cas de la televisió o la ràdio, unicast pot arribar a saturar un servei si el volum d'usuaris és molt alt. Arran d'aquesta qüestió de distribuir el mateix contingut a tothom que sol·licita, ja en els anys 80 amb la creació d'IP, es va pensar en una tecnologia que soluciona aquests casos: **IP Multicast**. Malgrat no estar tan establerta com IP unicast, sí que la gran majoria de dispositius l'accepten.

Per altra banda, al llarg dels anys, a les connexions unicast normalment han fet ús d'un protocol anomenat TCP. Aquest protocol va ser especialment important en els anys 90 i a principis dels 2000 perquè Internet pogués funcionar i popularitzar-se, ja que les connexions eren lentes i poc fiables. Aquest protocol incorpora una sèrie de mecanismes per intentar pal·liar aquesta qüestió. No obstant això, amb la millora de les connexions i la seva fiabilitat hi ha altres protocols que poden ser més útils i millors en l'Internet que tenim actualment, incorporant funcionalitats que antigament no s'havien plantejat o que no semblaven rellevants. Un protocol que pareix que substituirà TCP és QUIC, ja que millora bastant certs aspectes de TCP com l'establiment de la connexió molt més ràpidament (menys RTTs) o el fet de poder restablir la sessió amb el servidor en canviar de xarxa.

1.1 Transfons del projecte

Aquest projecte es fa des de zero, encara agafa principalment dos projectes de codi lliure d'Internet i un borrador del IETF:

1. ***Hypertext Transfer Protocol (HTTP) over multicast QUIC***, de Lucas Pardue, Richard Bradbury i Sam Hurst.
2. ***NGHQ***: Llibreria escrita en C que implementa part de l'esborrany de *HTTP sobre multicast QUIC* fins la versió 7.
3. ***NGTCP2***: Llibreria escrita en C que implementa el protocol QUIC segons l'estàndard escrit en el RFC 9000.

La idea original ha estat de l'autor, encara que l'enfocament i la metodologia han estat proposades pel professor, Jorge Mata.

Tot el codi utilitzat és de codi lliure desenvolupat per enginyers i que està pràcticament tot allotjat en plataformes online com Github. Tot el codi desenvolupat en aquest projecte està allotjat també al Github i també és de codi lliure.

1.2 Objectius

El principal objectiu d'aquest projecte és desenvolupar un servidor de contingut en temps real que faci ús de la tecnologia QUIC sobre IP multicast utilitzant la llibreria de software lliure. Al mateix temps, es pretén fer una comparativa de l'avantatge i inconvenients enfront del desenvolupament d'un servidor similar fent servir QUIC sobre IP unicast; és a dir, el perfil de QUIC genèric que proposa el RFC 9000.

El sistema estarà conformat per un servidor que rebrà peticions dels clients que demanaran el contingut de ràdio en directe a través d'IP. Aquest servidor reencaminarà en el cas de multicast al flux multicast o enviarà directament la informació en cas d'unicast.

[ESBORRANY - FALTA L'IMATGE FINAL]

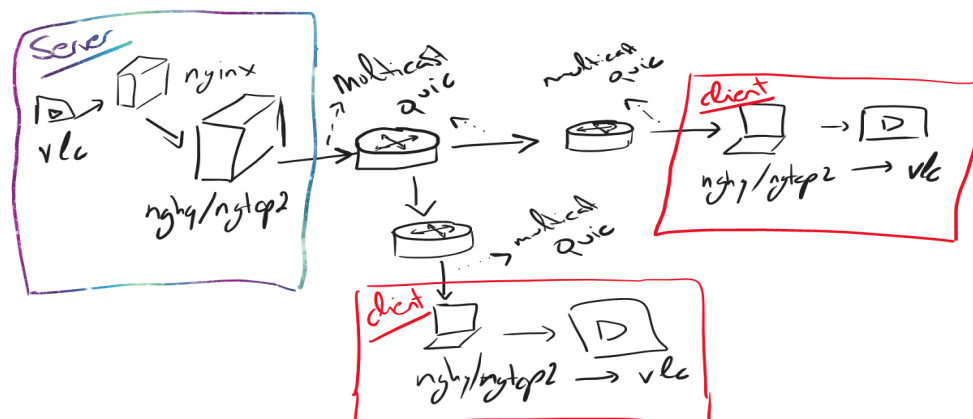


Figure 2: Topologia de la configuració plantejada.

L'arquitectura del sistema està basada en el següent escenari: s'utilitzarà un reproductor d'àudio en directe, aquest serà captat per un servidor intermedi i li passarà el contingut al servidor que hem desenvolupat perquè el transmeti a través de la xarxa fins als clients perquè ho reproduïxin.

El que es pretén demostrar és que hi ha un límit d'usuaris en el cas d'unicast i, en canvi, no hi ha un límit en el cas d'usuaris multicast. Donat que la majoria de la gent accedeix a través d'HTTP als serveis d'aquest tipus de contingut es farà ús de QUIC, un protocol desplegat pensat en HTTP. Cal indicar que QUIC permet l'ús de fils simultanis que es faran servir per enviar tràfic també a través de multicast. El perfil de QUIC en el cas de multicast difereix en alguns paràmetres i configuracions d'un perfil de QUIC normal.

1.3 Requeriments i especificacions

Requeriments del projecte:

- Proveir un sistema integrat de transmissió de contingut en directe tant per la part del client com la part del servidor que permeti la transmissió via unicast i/o multicast.
- Donar una guia als usuaris finals per fer la instal·lació tan simple com sigui possible (annexe?)
- Tot el software extern o implementat ha de ser gratuït i de codi lliure.
- Evaluar la solució final emulant-la en diferents escenaris i proveir uns resultats consistents.
- La transferència del contingut ha de ser en el màxim possible fluid i continua.
- El software desenvolupat ha de ser el més flexible possible per poder utilitzar-lo en futures implementacions d'altres softwares si es volgués.
- S'ha de poder avaluar el tràfic de manera quantitativa i qualitativa.

Especificacions del projecte:

- Hi ha d'haver com a mínim dos clients reben el contingut, ja que si no multicast deixa de tenir sentit encara que és viable fer-ho per un.
- El mostreig de la ràdio ha de poder variar durant la transmissió.
- Per avaluar el sistema en un entorn controlat, el servidor i els clients seran màquines virtual Linux que corren damunt el mateix sistema operatiu; Linux també.

- S'avaluarà el tràfic amb eines d'ús extensiu, proveint els filtres necessaris per descodificar els missatges transmesos.

1.4 Pla de feina

En aquesta secció de document es descriu en detall tots els blocs de treball en el qual s'ha dividit la feina i els temps (Diagrama de Gantt) en els que s'ha fet la tasca corresponent.

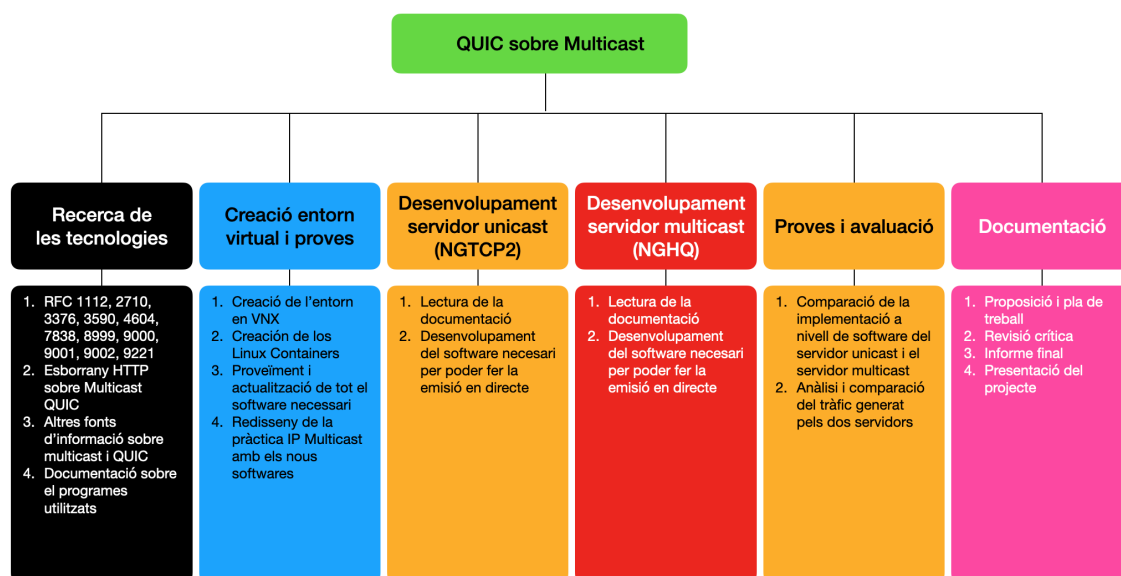
Al llarg del projecte, hi ha hagut diversos canvis en respecte al pla original. Els principals canvis han estat els següents:

- **Lectura de RFCs.** Donat la complexitat del projecte i la profunditat d'aquest s'ha vist que la quantitat de documentació al respecte que s'ha hagut de llegir ha estat molt major de la qual s'esperava, en gran part, ja que el nombre de tecnologies necessaries per poder entendre i desenvolupar una plataforma com la que es demana és molt major del qual es podria esperar a priori. També, a causa que s'utilitzen tecnologies noves com QUIC, hi ha hagut RFCs que han aparegut durant el transcurs com el 9221.
- **Certs programes no existien o no compilaven.** Per fer l'escenari de proves s'ha volgut fer servir un software nou per virtualitzar la xarxa intentant imitar la de la pràctica IP multicast de l'assignatura TCGI del grau d'Enginyeria de serveis i sistemes de telecomunicacions del ETSETB. Es va trobar que les màquines virtuals i el software utilitzat en aquelles màquines és antic i qualcun ja no està disponible. S'ha buscat alternatives al respecte.

El que més ha dificultat i endarrerit el desenvolupament ha estat la lectura de la documentació, ja que era molt més extensa del que s'esperava a priori a més que també entrava en molts detalls que semblaven contradictoris amb la idea, encara que sembla que no. S'ha de pensar que la proposta és una tecnologia que encara no s'ha desenvolupat del tot i encara està en procés, llavors això és més una prova del concepte que una demostració per ficar-ho a producció. Encara s'està lluny d'aquest punt com es veurà al llarg del treball.

1.4.1 Estructura de la feina

[ESBORRANY - FALTA L'IMATGE FINAL]



1.4.2 Paquets de feina, tasques i fites

Projecte: Recerca de les tecnologies	WP ref: WP1	
Element principal: Lectura de la documentació	Pàg. 1 de 6	
Breu descripció: Lectura del RFCs necessaris per tal d'entendre i proposar solucions adequades per crear un perfil de QUIC sobre multicast. Lectura de la documentació necesaria	Data d'inici estimada: 01-10-2021 Data de finalització estimada: 01-11-2021	
	Data d'inici real: 14-09-2021 Data de finalització real: 30-04-2022	
Tasques internes: T1. RFC 1112, 2710, 3376, 3590, 4604, 7838, 8999, 9000, 9001, 9002, 9221 T2. Esborrany HTTP sobre Multicast QUIC T3. Altres fonts d'informació sobre multicast i QUIC T4. Documentació sobre el programes utilitzats	Entregables: Tasca 1 i 2	Dates: incluídes en el document

Projecte: Creació entorn virtual i proves	WP ref: WP2	
Element principal: Entorn virtual	Pàg. 2 de 6	
Breu descripció: Creació de l'entorn virtual amb VNX, proveïment de les màquines virtuals amb el software necessari i fer la pràctica d'IP multicast de TCGI per testejar que l'entorn funciona correctament	Data d'inici estimada: 16-09-2021 Data de finalització estimada: 10-10-2021	
	Data d'inici real: 16-09-2021 Data de finalització real: 30-12-2022	
Tasques internes: T1. Creació de l'entorn en VNX T2. Creació dels Linux Containers T3. Proveïment i actualització de tot el software necessari T4. Rediseny de la pràctica IP Multicast amb els nous softwares	Entregables: Presentació al professor de l'escenari montat	Dates: 14-01-2022

Projecte: Desenvolupament servidor unicast (NGTCP2)	WP ref: WP3	
Element principal: Desenvolupament de software	Pàg. 3 de 6	
Breu descripció: Creació d'un servidor unicast que utilitzi el protocol QUIC per poder utilitzar-lo per comparar amb un que utilitzi multicast. També s'ha de fer el client.	Data d'inici estimada: 01-11-2021 Data de finalització estimada: 01-12-2021	
	Data d'inici real: 15-02-2022 Data de finalització real: 05-05-2022	
Tasques internes: T1. Lectura de la documentació T2. Desenvolupament del software necessari per poder per poder fer la emissió en directe.	Entregables: Tasca 1 Tasca 2 Tasca 3	Dates: 15-05-2022

Projecte: Desenvolupament servidor multicast (NGHQ)	WP ref: WP4	
Element principal: Desenvolupament de software	Pàg. 4 de 6	
Breu descripció: Creació d'un servidor multicast que utilitzi el protocol QUIC per poder utilitzar-lo per comparar amb un que utilitzi unicast. També s'ha de fer el client.	Data d'inici estimada: 01-11-2021 Data de finalització estimada: 01-12-2021	
	Data d'inici real: 15-02-2022 Data de finalització real: 05-05-2022	
Tasques internes: T1. Lectura de la documentació T2. Desenvolupament del software necessari per poder per poder fer la emissió en directe.	Entregables: Tasca 1 Tasca 2 Tasca 3	Dates: 15-05-2022

Projecte: Proves i avaluació	WP ref: WP5	
Element principal: Simulació i proves de qualitat	Pàg. 5 de 6	
Breu descripció: Totes les simulacions i avaluacions necessaries per aconseguir proves concloents de en quin cas és millor utilitzar unicast i quin multicast.	Data d'inici estimada: 01-11-2021 Data de finalització estimada: 15-12-2021	
	Data d'inici real: 15-02-2022 Data de finalització real: 05-05-2022	
Tasques internes: T1. Comparació de l'implementació a nivell de software del servidor unicast i el servidor multicast T2. Anàlisi i comparació del tràfic generat pels dos servidors	Entregables: Tasca 1 Tasca 2 Tasca 3	Dates: 15-05-2022

Projecte: Documentació	WP ref: WP6	
Element principal: Documentació	Pàg. 6 de 6	
Breu descripció: Documentació que s'ha d'entregar. Un manual d'usuari per poder configurar ambdós servidors serà inclòs en el document final.	Data d'inici estimada: 15-09-2021 Data de finalització estimada: 15-01-2022	
	Data d'inici real: 20-01-2022 Data de finalització real: 15-05-2022	
Tasques internes: T1. Proposició i pla de treball T2. Revisió crítica T3. Informe final T4. Presentació del projecte	Entregables: Tasca 1 Tasca 2 Tasca 3	Dates: 08-10-21 30-11-21 15-05-22 28-05-22

Objectius

WP#	Tasca#	Títol curt	Objectius/Entregables	Data (setmana)
WP1	T1	RFC 1112, 2710, 3376, 4604, 7838, 8999, 9001, 9002, 9221	Estat de l'art	Inclós en el document
WP1	T1	Esborrany HTTP sobre Multicast QUIC	Estat de l'art	Inclós en el document
WP1	T1	Altres fonts d'informació sobre multicast i QUIC	Estat de l'art	Inclós en el document
WP1	T2	Documentació sobre el programes utilitzats	Guies	Inclós en el document
WP2	T2	Creació de l'entorn en VNX	Entorn virtual montat	Setmanes 37 a 52
WP2	T2	Creació de los Linux Containers	Màquines disponibles per l'entorn virtual	Setmanes 37 a 52
WP2	T2	Proveïment i actualització de tot el software necessari	Màquines provistes del software requerit	Setmanes 37 a 52
WP2	T2	Redisseny de la pràctica IP Multicast amb els nous softwares	Comentaris per actualitzar la pràctica d'IP Multicast amb software actual (annexe)	Setmanes 37 a 52
WP3	T1	Lectura de la documentació (NGTCP2)	Explicació del software a estat de l'art	Setmanes 7 a 19
WP3	T3	Desenvolupament del software necessari per poder fer la emissió en directe	Creació del servidor per enviar la radio IP via unicast	Setmanes 7 a 19
WP4	T1	Lectura de la documentació	Explicació del software a l'estat de l'art	Setmanes 7 a 19
WP4	T3	Desenvolupament del software necessari per poder fer la emissió en directe	Creació del servidor per enviar la radio IP via multicast	Setmanes 7 a 19

WP#	Tasca#	Títol curt	Objectius/Entregables	Data (setmana)
WP5	T4	Comparació de la implementació a nivell de software del servidor unicast i el servidor multicast	Explicació de les avantatges i inconvenients del desenvolupament a l'apartat de resultats del document	Setmanes 7 a 19
WP5	T4	Anàlisi i comparació del tràfic generat pels dos servidors	Gràfica comparativa de la quantitat de tràfic generat per les dues implementacions	Setmanes 7 a 19
WP6	T1	Proposició i pla de treball	Proposició i pla de treball	Setmana 37
WP6	T2	Revisió Crítica	Revisió Crítica	Setmana 48
WP6	T3	Informe final	Informe final	Setmana 19
WP6	T4	Presentació del projecte	Presentació del projecte	Setmana 20

1.5 Diagrama temporal (Diagrama de Gantt)

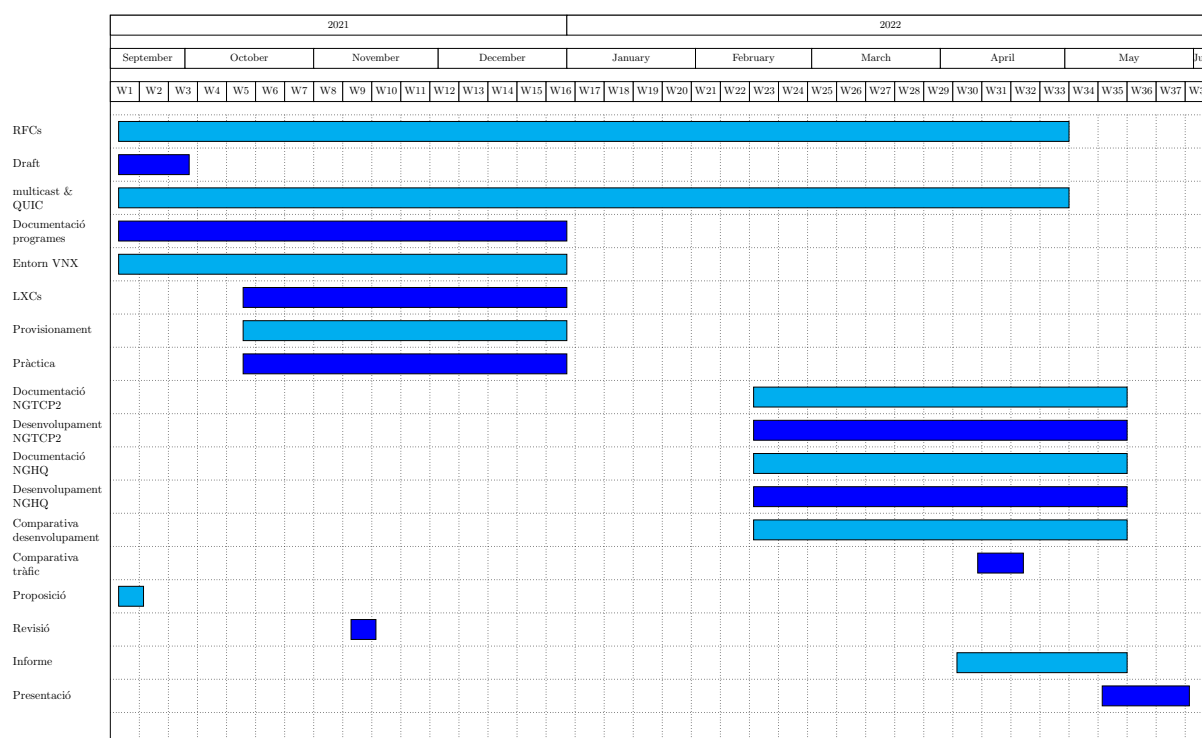


Figure 3: Diagrama de Gantt del projecte

2 Estat de l'art sobre les tecnologies utilitzades

L'interès en les transmissions en directe ha fet que molts esforços d'empreses i grups de recerca es focalitzin en desenvolupar noves tecnologies per fer front a la creixent demanda en termes de qualitat i al mateix temps que donar servei cada cop a més clients. Les tecnologies que permeten aquestes transmissions se centren principalment en dos grups: protocols i codificacions. Això no obstant, en el nostre cas només ens centrarem en els protocols, perquè aquests poden funcionar independentment de les codificacions.

Per tal d'entendre millor el projecte, en els següents apartats s'explicaran els principis i objectius de les tecnologies implicades. A l'annex 1 hi ha un resum extens de l'evolució de les tecnologies implicades fins a arribar la creació de QUIC o l'ús que es fa avui en dia de multicast. Es recomana donar una ullada si hi ha alguna sigla o tecnologia que no s'entén.

2.1 Contexte de QUIC

Transmission Control Protocol (TCP) és un protocol dissenyat per enviar un flux de dades entre dos punts. Les dades són trameses pel sistema TCP que s'encarrega d'assegurar que les dades arribaran a l'altre extrem exactament iguals o que en el cas que no fos així indicar que hi ha un error a la connexió.

Per aconseguir això, TCP parteix les dades en petits paquets i afegeix una sèrie de capçaleres. Aquestes dades extres inclouen un número de seqüència que s'utilitza per detectar quan un paquet s'ha perdut o arribar tard (Out-of-order) i una suma de comprovació s'utilitza per detectar que hi ha hagut un error a les dades. Quan algun problema ocorre, TCP automàticament usa un algorisme que es diu Automatic Repeat Request (ARQ) en el que es notifica a l'emissor que reenvii el paquet perdut o mal transmès.

En la majoria d'implementacions, quan hi ha TCP detecta un error parerà la transmissió fins que l'error s'hagi resolt o consideri que la connexió ha fallat. En cas de fer servir una connexió multiplexada en diversos fluxos de dades, com en el cas de HTTP/2, tots es veuran afectats i es pararan encara que només hi hagi hagut un error en un flux. Per exemple, si hi ha un error carregant una imatge d'una pàgina web, tota la resta de fluxos hauran d'esperar fins que la qüestió s'hagi solucionat. Això es coneix com la qüestió d'encapçalament de línia o head-of-line blocking.

TCP està dissenyat com una canonada de dades en la qual no entén el que s'està enviant. Si es requereixen necessitats addicionals com encriptació (TLS), aquests s'han de fer des de capes superiors a TCP, utilitzant TCP per comunicar-se amb l'altre extrem que utilitza software semblant. Cadascun d'aquests protocols necessita el seu propi *handshake*. Normalment, això implica que hi hagi diversos intercanvis de paquets de sol·licitud i resposta per establir la connexió fins que aquesta finalment s'ha establert. Això pot arribar a ser un molt greu problema en sistemes de comunicacions amb alta latència, ja que pot significar sobrecàrrega de dades de control en el transcurs de la connexió.

2.2 QUIC

QUIC és un nou protocol d'Internet que es diu que canviarà com funciona actualment Internet. Daniel Stenberg, creador de l'aplicació curl i un dels contribuïdors a l'estàndard de QUIC, va dir que fins ara HTTP s'ha fet sobre TCP i això ha implicat grans limitacions, però amb la vinguda d'aquest nou protocol (QUIC), les regles del joc podran canviar millorant les velocitats i altres aspectes de l'Internet actual.

A principis de la dècada passada, a Google varen començar a platejar un nou estàndard pensat per substituir TCP i al mateix temps simplificar i millorar coses com la seguretat o que l'establiment del canal fos el més ràpid possible inclús arribant al punt que en la primera resposta el servidor pogués donar informació útil al client. Amb aquesta idea en ment varen començar a treballar en el que anomenaren Quick UDP Internet Protocol o QUIC.

Avui en dia es tracta d'un estàndard redactat publicat en els RFC 8999 (Version-independent Properties of QUIC), **RFC 9000** (QUIC: A UDP-Based multiplexed and Secure Transport), RFC 9001 (Using TLS to Secure QUIC) i RFC 9002 (QUIC Loss Detection and Congestion Control). L'estàndard de QUIC de Google es coneix com gQUIC a dia d'avui i està pràcticament deixat. Es recomana l'ús de l'estàndard proposat per l'IETF que va sortir en maig de 2021.

A l'inici aquest protocol estava pensant per fer feina pràcticament en la capa de transport (capa L4 del model OSI). Això no obstant, varen trobar un greu problema amb com s'havien implementat els dos protocols predominants fins al moment, TCP i UDP: estaven implementats en la majoria de nuclis dels sistemes operatius. Això implica que el desplegament o actualització d'un protocol sigui extremadament lent i pugui tardar més d'una dècada. Sobretot també s'ha de pensar que hi ha molts firewalls que no accepten tràfic que no sigui d'aquests dos protocols.

Al veure, aquesta situació varen optar per una solució en una capa superior, la qual normalment està implementada en l'espai d'usuari i sol ser més fàcil d'actualitzar a priori¹. Donat que UDP és un protocol tan senzill i que delega pràcticament totes les tasques de retransmissions o control de flux a capes superiors, varen decidir fer ús d'aquest per assegurar la interoperabilitat en els nodes intermedis que no entenen aquest nou protocol. Aconseguint saltar aquesta gran barrera, ja varen poder començar a treballar en els aspectes d'aquest nou protocol.

2.2.1 QUIC: establiment de la connexió

Un dels aspectes rellevant de QUIC és que utilitza menys paquets per arribar a establir la connexió inicialment. La filosofia per poder arribar a aconseguir això és que es realitzi el *handshake* tant en l'àmbit de connexió (imitant TLS) com en l'àmbit de seguretat (TLS).

Si comparen el *handshake* de QUIC, que inclou implícitament el *handshake* de TLS 1.3, amb el *handshake* de TCP + TLS 1.2 podrem observar que el nombre de paquets intercanviats entre els dos extrems és molt major en el segon cas. El problema resideix en què en mirar als dos protocols com dos protocols diferents, llavors l'establiment de la connexió primer s'ha de fer per TCP i després per TLS. A QUIC es proposa fer els dos al mateix temps.

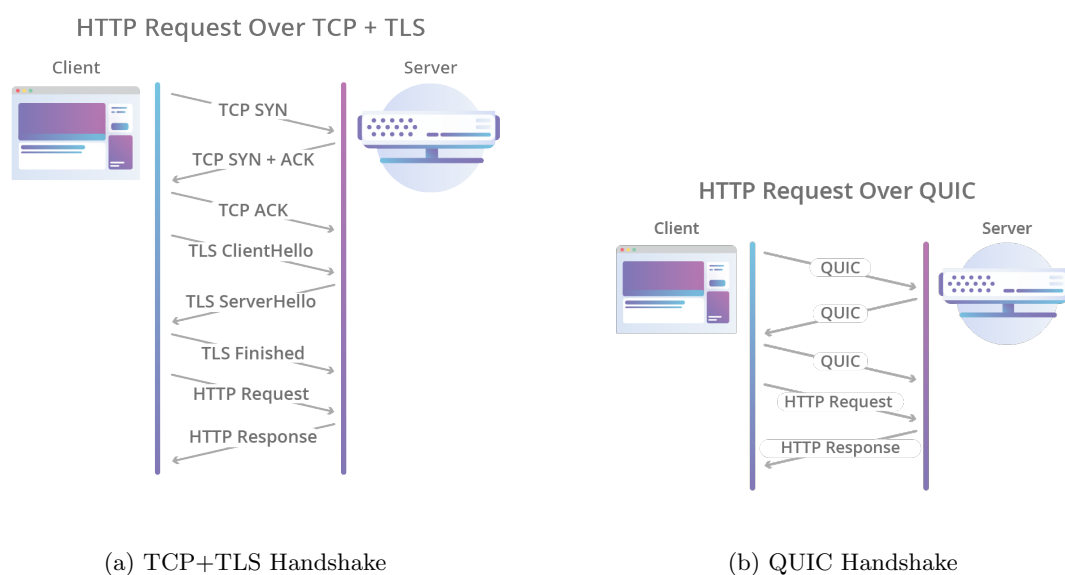


Figure 4: Comparativa establiment connexió entre TCP+TLS i QUIC. Imatge de Cloudflare.

2.2.2 QUIC: Migració

A QUIC al mateix temps s'introdueix un concepte molt interessant que és el **Connection ID**. Bàsicament, es tracta d'un tiquet l'identifica la teva connexió. Això comporta grans avantatges com la fàcil migració

¹En teoria hauria de ser així, però per exemple en el cas de TLS 1.2 va ser una qüestió molt gran la seva actualització. Recomanat l'article de Cloudflare al respecte. Està a la bibliografia

de connexió que a continuació s'explica, que en el mateix port puguin córrer diverses aplicacions, principalment a la banda del client o ajudar a evitar atacs d'amplificació (s'explica en detall en el RFC 9000).

Fins ara, quan s'estableix la connexió, sempre es parlava d'una tupla per identificar a l'altre extrem: una IP i un port. Aquest plantejament de baix nivell funciona molt bé per dispositius que no canvien de xarxa o IP. Tanmateix, amb la vinguda dels dispositius mòbils i sobretot dels smartphones aquest concepte d'identificar a l'altre extrem amb la IP i el port pot arribar a ser un problema, ja que aquest canvien de xarxa mòbil a xarxa wifi bastant sovint. Això no permet reprendre una connexió a on s'havia deixat si s'estaven enviant dades havent de tornar a fer el *handshake* un altre cop. Amb QUIC i el plantejament d'identificadors de connexió o *Connection IDs* canvia completament.

A QUIC s'introdueix el concepte de **0-RTT**; és a dir, que encara que és canvi de xarxa la connexió es pot reprendre a on s'havia deixat evitant fer tants de *handshakes* i pràcticament transmetre dades des de la primera resposta si s'ha establert una connexió anteriorment. Per aconseguir això, tant el servidor com el client ha de mantenir una sèrie de paràmetres de transport (principalment de TLS) i el mateix *Connection ID* tant en la banda del servidor com del client (detalls a la secció 7 de [QUIC-Transport]).

2.2.3 QUIC: capçaleres més dinàmiques

A QUIC hi ha dos tipus principals de paquets en termes de mida i el que duen². Per una banda, estan els paquets amb una capçalera llarga o *long header* que són utilitzats principalment durant els *handshakes* o altres paquets especials. Aquest tipus de paquets inclouen el *SCID* (*Source Connection ID*), el *DCID* (*Destination Connection ID*), altres paràmetres de transport, etc. Aquests paquets també poden dur càrrega útil de capes superiors, encara que aquest tipus no és el més adequat per connexions llargues.

Per altra banda, hi ha un altre tipus de paquets que tenen una capçalera curta o *short header* que sí que són emprats després que la connexió s'ha establert i es transfereixen les dades de manera més extensa. Aquest tipus de paquets només duen el *DCID* i el número de paquet pràcticament, ja que són les úniques dues dades fonamentals perquè la connexió pugui funcionar.

Si s'ha d'enviar un tipus de trama especial, normalment s'envia a través dels fluxos o *streams* que es generen durant el *handshake* o en fases posteriors. Sol haver-hi un canal destinat a aquest tipus de trames.

2.2.4 QUIC: Multiplexat

Ja des de HTTP/2 s'ha plantejat el concepte de multiplexat en l'enviament de dades. Per ficar context, només la pàgina inicial de la gran majoria de pàgines web que podem visitar a través de cercadors estan fetes a base de molts arxius, ja sigui l'arxiu HTML (.html), l'arxiu per decorar (.css), l'arxiu per afegir interactivitat (.js) o fotos i altres (.jpg, .mp3, .ts, etc.). En veure aquesta situació ja en el seu moment es va plantejar que descarregar paral·lelament aquests arxius podia accelerar en gran manera la velocitat de càrrega i descarregar al servidor de feina (sobretot si apliquem també *server push*).

Encara que aquesta idea al final si ha millorat molt les velocitats de càrrega, xoca frontalment amb el concepte d'un únic flux de dades que proposa TCP. En el cas que es perdi un paquet d'un flux de dades HTTP/2, llavors tots els fluxos han d'esperar al fet que aquest paquet es recuperi fent que la millora velocitat que guanyàvem abans es perdi, ja que s'activa el mecanisme de ARQ de TCP. Aquest fenomen s'anomena *Head-of-line blocking*.

Amb HTTP/3 (HTTP sobre QUIC), com a la capa de transport s'utilitza UDP, llavors quan es perd un paquet d'un flux de dades, els altres fluxos no es veuen interromputs, ja que no hi ha mecanismes en capes inferiors com ARQ com si li passa a HTTP/2 amb TCP. De fet, es pot pensar en cada flux de QUIC com un flux TCP independent que incorpora mecanisme de recuperació i validació de paquets.

²S'adjunta el següent enllaç on s'expliquen en una mica detall tots els tipus: <https://gist.github.com/martinthomson/744d04cbcec9be554f2f8e7bae2715b8>

2.2.5 QUIC: Control de fluxe a nivell de connexió i de paquets de dades

Donat que es realitza un multiplexat individual per cada *stream* llavors el control de flux s'ha de fer per cada *stream* individualment, encara que també es comptabilitza a escala general (mirar més especificacions en la secció 4 de [QUIC-transport]).

A manera de resum molt ràpid, les dades s'envien en trames STREAM i quan l'aplicació de capa superior no vol enviar més dades temporalment s'utilitza STREAM_DATA_BLOCKED per mantenir la connexió viva. Els fluxos poden ser unidireccionals, des del client al servidor o viceversa, o bidireccionals. Els *streams* poden tenir prioritats i és important respectar els estats d'aquests perquè la connexió funcioni (es recomana llegir l'apartat 3 de [QUIC-transport] per més detalls).

2.2.6 QUIC: Autenticació i encriptació de la capçalera i càrrega útil

Finalment, per acabar de contar entre altres coses interessants que afegeix QUIC, ens falta parlar dels seus mecanismes d'autenticació i encriptació tant de la capçalera com de la càrrega útil. Fins ara, quan s'envia un paquet via TCP, únicament s'encriptava a la càrrega útil i es deixava a capes superiors (TLS) aquesta feina. El fet de poder encriptar la majoria de la capçalera i verificar que el receptor és qui realment diu ser fa que atacs del tipus amplificació siguin especialment complicats.

2.3 Multicast

IP va néixer com un protocol per interconnectar xarxes d'àrea local amb tecnologies diferents. Aquestes xarxes funcionaven de manera *unicast*, un a un, o *broadcast*, un per a tots. Malgrat això, l'any 1988 es va publicar el RFC 988 anomenat [?]. Aquest proposava fer una extensió de la tecnologia IP per permetre la connexió d'un emissor a molts receptors, però no tots, només els que volguessin rebre la informació d'aquest.

Per fer una analogia de multicast amb el nostre entorn quotidià, es podria dir que funciona com la TDT o la ràdio. Es pot pensar com una antena que emet el senyal i si vols rebre el senyal únicament ficat el canal o la freqüència a la qual aquesta emet per poder rebre i veure o escoltar la transmissió, però si algú no la vol rebre no la pot ignorar.

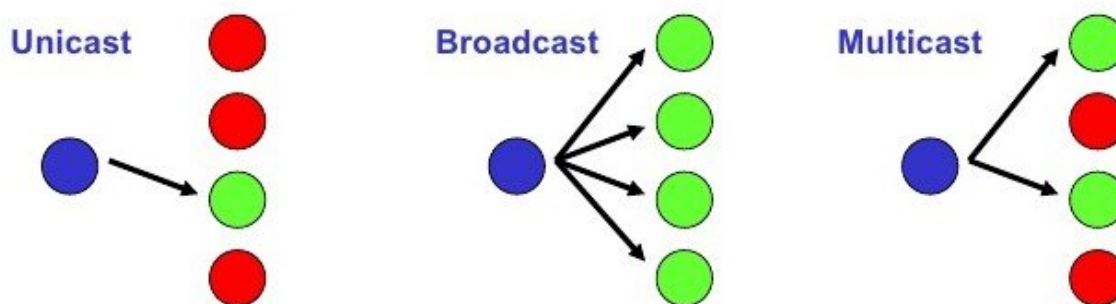


Figure 5: En blau l'emissor de la senyal, en verd els usuaris que reben la senyal i en vermell els que no. Imatge de pc-solucion.es

Dins la tecnologia IP hi ha un rang d'adreces destinades a aquesta tecnologia. El rang és la classe D que va des de **224.0.0.0** fins **239.255.255.255**.

Encara que a priori sembla una idea força senzilla, en realitat, és molt complicada, ja que té diversos problemes associats, encara que la majoria actualment ja tenen solució excepte un que s'esmentarà al final i és el seu gran problema a l'hora d'implementar-lo extensament. Normalment, les qüestions d'IP multicast se solen derivar a capes superiors.

2.3.1 Multicast: IGMP

Per poder dir a un router que pot arribar a rebre l'emissió que es vol rebre aquesta es fa ús d'un protocol anomenat IGMP o Internet Group Management Protocol. La idea d'aquest protocol és implementar un model de subscripció al senyal en el qual mitjançant un paquet que s'envia al router a una distància 1 s'informa que es vol rebre l'emissió d'una direcció destinatària i un port concrets. Aquest protocol permet també dir que la connexió ha d'arribar d'un lloc concret (*source specific*).

2.3.2 Multicast: la seguretat

Un dels majors problemes encara no resolts de multicast és l'encriptació de les comunicacions. El mètode actual per xifrar les comunicacions es basa a canviar la clau d'accés cada poc temps transferint-la via un canal alternatiu (via *unicast*). Malgrat que aquesta solució a priori sembla suficient, si aquesta clau es comparteix a un usuari que no ha de poder veure el senyal (televisió de pagament per exemple) llavors la transmissió multicast no és segura. És més, que es comparteixi la clau per qualsevol agent escoltant el senyal pot implicar altres riscos de seguretat per la transmissió com la suplantació d'identitat per introduir codi maliciós.

2.4 Programes i software important

3 Section 3

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula. EU is the European Union. Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetur. Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio. ETSETB is Telecos. Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

3.1 Subsection

Algorithm 1 Temperature-Distributed algorithm

```

1: procedure TEMP-SPREAD( $GN_i, HN_j, temperatures$ ) ▷ Lowest temperature priority
2:    $temperature\_list \leftarrow short(temperatures)$ 
3:    $max\_temperature \leftarrow max(temperature\_list)$ 
4:    $ThresHold \leftarrow 0.5$ 
5:    $temperature\_impact \leftarrow 0.2$ 
6:   for  $GN_i$  in  $i = 1, 8$  do ▷ Iterate every hardware node on the given GN
7:      $it\_temperature \leftarrow temperature\_list(GN_i)$ 
8:      $temp\_weight \leftarrow \frac{max\_temperature - it\_temperature}{max\_temperature} * temperature\_impact$ 
9:      $\omega(Master - GN_i) \leftarrow ThresHold * temp\_weight$ 
10:    for  $HN_j$  in  $j = 1, n$  do
11:      if  $available\_accel_{i,j} > busy\_accel_{i,j}$  then
12:         $policy_\omega = \frac{AvailableHW}{TotalHW} * ThresHold$ 
13:         $\omega(GN_i - HN_{i,j}) \leftarrow ThresHold + policy_\omega$ 
14:      else
15:         $\omega(GN_i - HN_{i,j}) \leftarrow 1$ 
16:    $node \leftarrow find\_djistra\_shortest\_path(Master\_Node, aux\_node)$ 
17:   return  $node$  ▷ The gcd is b

```

4 Section 4

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetur at, consectetur sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

4.1 Subsection 4.1

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetur at, consectetur sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

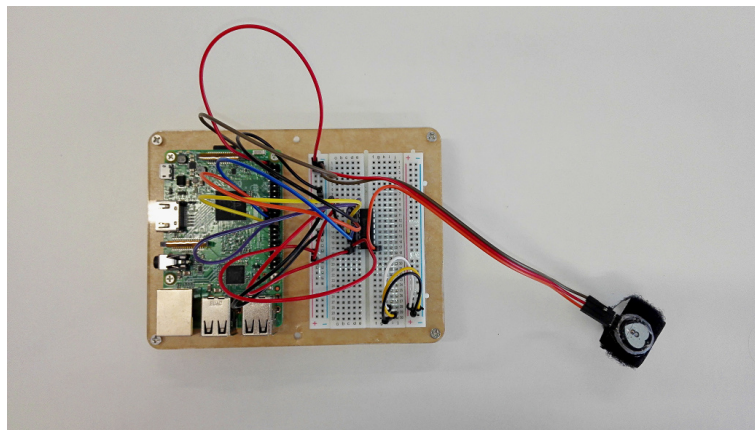


Figure 6: Prototype setup.

Etiam ac leo a risus tristique nonummy. Donec dignissim tincidunt nulla. Vestibulum rhoncus molestie odio. Sed lobortis, justo et pretium lobortis, mauris turpis condimentum augue, nec ultricies nibh arcu pretium enim. Nunc purus neque, placerat id, imperdiet sed, pellentesque nec, nisl. Vestibulum imperdiet neque non sem accumsan laoreet. In hac habitasse platea dictumst. Etiam condimentum facilisis libero. Suspendisse in elit quis nisl aliquam dapibus. Pellentesque auctor sapien. Sed egestas sapien nec lectus. Pellentesque vel dui vel neque bibendum viverra. Aliquam porttitor nisl nec pede. Proin mattis libero vel turpis. Donec rutrum mauris et libero. Proin euismod porta felis. Nam lobortis, metus quis elementum commodo, nunc lectus elementum mauris, eget vulputate ligula tellus eu neque. Vivamus eu dolor.

4.2 Subsection 4.2

Table 1: This is the other caption. Since the trial size of the experiments showed is one second, the number of *Target* and *Impostor* data corresponds to number of trials or seconds

Dataset	Label	Train	Validation	Develop	Test
First	Target	135	45	30	30
	Impostor	5, 220	1, 740	1, 890	2, 880
	#Subjects	31			12
Second	Target	144	80	48	48
	Impostor	2, 014	1, 119	1, 343	1, 545
	#Subjects	15			5

5 Section 5

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

5.1 Overview

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

6 Experiments and results

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetur a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetur. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

7 Budget

Depending on the thesis scope this document should include:

8 Environment Impact (Optional)

Whether the tasks that have led to the realization of this thesis, as if its results have identifiable environmental impact, describe it in this section.

9 Conclusions

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetur adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

10 Future Work

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetur odio sem sed wisi.

Appendices

Appendices may be included in your thesis but it is not a requirement.