



Σχολή Τεχνολογίας
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΣΥΓΧΡΟΝΑ ΣΥΣΤΗΜΑΤΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ
ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ»

“MSc in Modern Communication Systems and the
Internet of Things”

Τίτλος Διπλωματικής Εργασίας

Μελέτη της επίδρασης του HTTP/3 στο YouTube Video Streaming (Study
of HTTP3 impact on YouTube Video Streaming).

ΦΟΙΤΗΤΡΙΑ: ΣΑΚΟΡΑΦΑ ΟΛΥΜΠΙΑ του ΓΕΩΡΓΙΟΥ

Αριθμός Μητρώου: 00011

ΙΑΝΟΥΑΡΙΟΣ 2025

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

**«ΣΥΓΧΡΟΝΑ ΣΥΣΤΗΜΑΤΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ
ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ»**

**« Master of Science in Modern Communication Systems and
the Internet of Things”**

**«... Μελέτη της επίδρασης του HTTP/3 στο YouTube Video Streaming
(Study of HTTP3 impact on YouTube Video Streaming)....»**

Διπλωματική Εργασία

που υποβλήθηκε στο Τμήμα Ψηφιακών Συστημάτων του

Πανεπιστημίου Θεσσαλίας

ως μέρος των απαιτήσεων για την απόκτηση

Διπλώματος Μεταπτυχιακών Σπουδών στα Σύγχρονα Συστήματα Επικοινωνιών και
Διαδίκτυο των Πραγμάτων από την

Σακοράφα Ολυμπία του Γεωργίου

Δήλωση Αυθεντικότητας, ζητήματα Copyright

«Ο μεταπτυχιακός φοιτητής που εκπόνησε την παρούσα διπλωματική εργασία φέρει ολόκληρη την ευθύνη προσδιορισμού της δίκαιης χρήσης του υλικού, η οποία ορίζεται στη βάση των εξής παραγόντων: του σκοπού και χαρακτήρα της χρήσης (μη-εμπορικός, μη-κερδοσκοπικός, αλλά εκπαιδευτικός-ερευνητικός), της φύσης του υλικού που χρησιμοποιεί (τμήμα του κειμένου, πίνακες, σχήματα, εικόνες κ.λπ.), του ποσοστού και της σημαντικότητας του τμήματος που χρησιμοποιεί σε σχέση με το όλο κείμενο υπό copyright, και των πιθανών συνεπειών της χρήσης αυτής στην αγορά ή την γενικότερη αξία του υπό copyright κειμένου».

Η παρούσα διπλωματική εργασία εγκρίθηκε ομόφωνα από την τριμελή εξεταστική επιτροπή η οποία ορίστηκε από την Συνέλευση του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Θεσσαλίας, σύμφωνα με το νόμο και τον εγκεκριμένο Οδηγό Σπουδών του ΠΜΣ «Σύγχρονα Συστήματα Επικοινωνιών και Διαδίκτυο των Πραγμάτων».

Τα μέλη της Επιτροπής ήταν:

•...ΛΑΜΨΑΣ ΠΕΤΡΟΣ..... (Επιβλέπων)

•....ΚΑΡΕΤΣΟΣ ΓΕΩΡΓΙΟΣ..... (Μέλος)

•.....ΑΔΑΜ ΓΕΩΡΓΙΟΣ..... (Μέλος)

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Πέτρο Λάμπα για τις χρήσιμες παρατηρήσεις του, τις επιστημονικές συμβουλές και την καθοδήγησή του που βοήθησαν αποφασιστικά στην επιτυχή περάτωση αυτής της εργασίας.

Περιεχόμενα

Περίληψη.....	7
Abstract	9
Κεφάλαιο 1	10
Εισαγωγή.....	10
1.1 Εισαγωγή στα πρωτόκολλα HTTP και QUIC	10
1.2 Σημασία της μελέτης της διείσδυσης του HTTP/3 σε μεγάλους ISPs	12
1.3 Σημασία του YouTube ως σημείο εστίασης στην παρούσα μελέτη.....	13
Κεφάλαιο 2	13
Ανασκόπηση Βιβλιογραφίας.....	13
2.1 Επισκόπηση της βιβλιογραφίας για τα πρωτόκολλα HTTP/3 και QUIC	13
2.1.1 Τι είναι το πρωτόκολλο HTTP/3.....	14
2.1.2 Τι είναι το πρωτόκολλο QUIC	14
2.2 Πρωτόκολλο QUIC και ασφάλεια.....	15
2.2.1 Ιστορικό πλαίσιο και ανάπτυξη αυτών των πρωτοκόλλων	19
2.2.2 HTTP/1.0.....	20
2.2.3 HTTP/1.1.....	21
2.2.4 TCP.....	22
2.2.5 SSL.....	23
2.2.6 HTTP/2.....	23
2.2.7 HTTP/3.....	29
2.3 Προηγούμενες μελέτες σχετικά με την υιοθέτησή τους σε μεγάλους παρόχους υπηρεσιών διαδικτύου.....	34
Κεφάλαιο 3	35
Διείσδυση των HTTP/3 και QUIC σε μεγάλους ISPs	35
3.1 Ανάλυση των HTTP/3 και QUIC από τις Google, Cloudflare, Google	35
3.2 Στατιστικά στοιχεία και δεδομένα σχετικά με τη χρήση τους στους εν λόγω ISPs	38
Κεφάλαιο 4	41
Εστίαση στο Youtube.....	41
4.1 Λεπτομερής εξέταση του τρόπου με τον οποίο το YouTube χρησιμοποιεί τα HTTP/3 και QUIC.....	41
4.2 Στρατηγικές ενσωμάτωσης	42
4.3 Επιπτώσεις στη συνολική απόδοση και την εμπειρία του χρήστη του Youtube	43
Κεφάλαιο 5	44
Συγκριτική ανάλυση της QoE	44
5.1 Ανασκόπηση των υφιστάμενων μελετών σχετικά με το QoE των χρηστών του YouTube με το HTTP/3 και το QUIC	44
5.2 Μετρικές που χρησιμοποιούνται για την αξιολόγηση της QoE	46
5.3 Βασικά ευρήματα και τάσεις όσον αφορά τον αντίκτυπο στους χρόνους φόρτωσης βίντεο, τη ρυθμιστική μνήμη και τη συνολική ικανοποίηση των χρηστών	47
ΚΕΦΑΛΑΙΟ 6.....	48
Εκτέλεση πειραμάτων.....	48
6.1 Μεθοδολογία	48

6.2 Αποτελέσματα	50
Κεφάλαιο 7	54
Συμπεράσματα	54
7.1 Σύνοψη των βασικών ευρημάτων	54
7.2 Προτάσεις για μελλοντική έρευνα στον τομέα αυτό.....	55
Αναφορές – Πηγές.....	56

Περίληψη

Η διατριβή αυτή, πραγματεύεται την εξέλιξη των πρωτόκολλων HTTP. Συγκεκριμένα, διερευνούμε το πρωτόκολλο HTTP/3, όπως και το υποκείμενο QUIC, πραγματοποιώντας μια βιβλιογραφική ανάλυση των τεχνικών του χαρακτηριστικών, και αξιολογώντας τον αντίκτυπό του στην Ποιότητα Εμπειρίας (QoE) για τους χρήστες, με έμφαση την πλατφόρμα YouTube. Το HTTP/3 αντιπροσωπεύει μια σημαντική εξέλιξη στην επικοινωνία Ιστού, σχεδιασμένη να αντιμετωπίζει τους περιορισμούς των προκατόχων του ενσωματώνοντας το πρωτόκολλο μεταφοράς QUIC, το οποίο λειτουργεί μέσω UDP και όχι TCP. Αυτή η μετάβαση στοχεύει στη βελτίωση της απόδοσης, στη μείωση του χρόνου πραγματοποίησης μιας σύνδεσης και στη βελτίωση της ασφάλειας. Η τεχνική ανάλυση εμβαθύνει στους μηχανισμούς των HTTP/3 και QUIC, υπογραμμίζοντας τις δυνατότητές τους στην πολυπλεξία, τη μετεγκατάσταση συνδέσεων και τον ενισχυμένο έλεγχο συμφόρησης. Αυτές οι λειτουργίες συμβάλλουν συλλογικά σε μια πιο ανθεκτική και αποτελεσματική διαδικασία μετάδοσης δεδομένων, ζωτικής σημασίας για πλατφόρμες υψηλής «επισκεψιμότητας» όπως το YouTube. Για την αξιολόγηση της Ποιότητας Εμπειρίας Χρήστη, προβαίνουμε σε μία γενική εξέταση ορισμένων βασικών μετρήσεων, όπως για παράδειγμα, οι χρόνοι φόρτωσης βίντεο, η ποιότητα ανάλυσης, οι περιπτώσεις προσωρινής αποθήκευσης, τα συμβάντα ξαφνικής διακοπής ροής, κ.α. Μέσω της βιβλιογραφικής ανασκόπησης, συμπεραίνουμε πως το πρωτόκολλο HTTP/3 οδηγεί σε μια σημαντική βελτίωση της συνολικής ποιότητας της εμπειρίας χρήστη, βελτιώνοντας τη σταθερότητα αναπαραγωγής βίντεο, σε ανόμοιες συνθήκες δικτύου. Η σημασία του HTTP/3 σε πλατφόρμες όπως το Netflix και το Youtube απαντάται από τον αποτελεσματικό χειρισμό μεγάλων όγκων «επισκεψιμότητας», διατηρώντας ένα ικανοποιητικό επίπεδο ποιότητας, ακόμη και σε συμβάντα αιχμής. Έτσι, το γεγονός αυτό ωφελεί και τους χρήστες καθώς απολαμβάνουν μια πιο ομαλή εμπειρία σύνδεσης, αλλά παράλληλα βοηθά και τους στόχους του Youtube, βελτιστοποιώντας τη χρήση πόρων δικτύου και μειώνοντας το κόστος υποδομής. Συμπερασματικά, η ενσωμάτωση της συνέργειας των πρωτόκολλων HTTP/3 και QUIC στο Youtube, αδιαμφισβήτητα σηματοδοτεί ένα κομβικό βήμα στην εξέλιξη των διαδικτυακών πρωτοκόλλων, θέτοντας νέα σημεία αναφοράς για την απόδοση και την εμπειρία χρήστη στην ψηφιακή εποχή.

Λέξεις Κλειδιά: HTTP/3, QUIC, Video Streaming over HTTP/3, QoE in Youtube video streaming over HTTP/3.

Abstract

This thesis deals with the evolution of HTTP protocols. In particular, we investigate the HTTP/3 protocol, as well as the underlying QUIC, by performing a literature review of its technical characteristics, and evaluating its impact on the Quality of Experience (QoE) for users, with an emphasis on the YouTube platform. HTTP/3 represents a major development in Web communication, designed to address the limitations of its predecessors by incorporating the QUIC transport protocol, which operates over UDP rather than TCP. This transition aims to improve performance, reduce the time it takes to make a connection, and improve security. The technical analysis delves into the mechanisms of HTTP/3 and QUIC, highlighting their capabilities in multiplexing, connection migration, and enhanced congestion control. These features collectively contribute to a more robust and efficient data transmission process, vital for high "traffic" platforms like YouTube. To assess Quality of User Experience, we take a general look at some key metrics, such as video load times, resolution quality, buffering instances, dropout events, etc. Through the literature review, we conclude that the HTTP/3 protocol leads to a significant improvement in the overall quality of the user experience, improving the stability of video playback, in disparate network conditions. The importance of HTTP/3 on platforms such as Netflix and Youtube is answered by the efficient handling of large volumes of "traffic", maintaining a satisfactory level of quality, even during peak events. So this fact both benefits users as they enjoy a smoother connection experience, but also helps Youtube's goals by optimizing network resource usage and reducing infrastructure costs. In conclusion, the integration of the synergy of HTTP/3 and QUIC protocols in Youtube, undeniably marks a pivotal step in the evolution of Internet protocols, setting new benchmarks for performance and user experience in the digital age.

Keywords: HTTP/3, QUIC, Video Streaming over HTTP/3, QoE in Youtube video streaming over HTTP/3.

Κεφάλαιο 1

Εισαγωγή

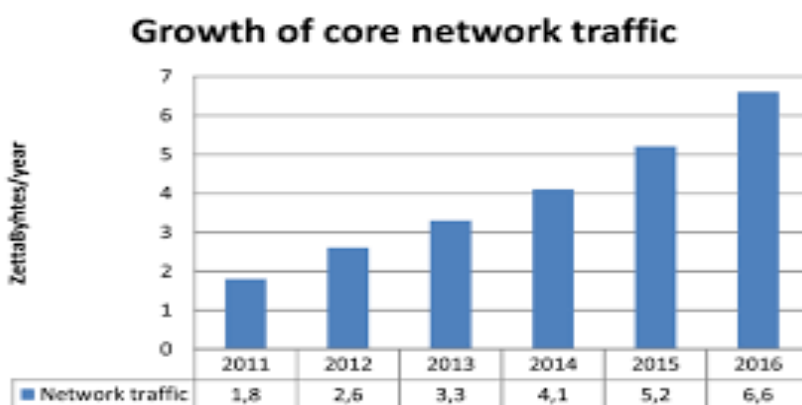
1.1 Εισαγωγή στα πρωτόκολλα HTTP και QUIC

Η συχνότητα χρήσης του Διαδικτύου αυξάνεται ραγδαία, οδηγώντας σε μεγαλύτερη ζήτηση για αξιόπιστη και γρήγορη μετάδοση δεδομένων. Οι ISP οργανισμοί ανταγωνίζονται ενεργά για δίκτυα που προσφέρουν ελάχιστη καθυστέρηση δημιουργίας σύνδεσης και βέλτιστη απόδοση, καθώς ακόμη και μια φαινομενικά μικρή καθυστέρηση των 100 ms δύναται να οδηγήσει σε σημαντική οικονομική ζημία ύψους εκατομμυρίων δολαρίων. Το τμήμα του περιεχομένου βίντεο που μεταδίδεται μέσω του Διαδικτύου βρίσκεται επί του παρόντος σε σημαντική επέκταση και γενική ανάπτυξη. Αυτό μπορεί να αποδοθεί στην αυξανόμενη προσβασιμότητα διαφόρων συσκευών και στην ευρεία διαθεσιμότητα σταθερών και κινητών ευρυζωνικών συνδέσεων Διαδικτύου. Η γρήγορη επέκταση της κρυπτογράφησης της κυκλοφορίας στο Διαδίκτυο οφείλεται σε αυξημένες ανησυχίες σχετικά με την ασφάλεια και το απόρρητο. Πλατφόρμες μετάδοσης βίντεο, όπως για παράδειγμα το Youtube, το Netflix και το Disney αλλά και άλλες χρησιμοποιούν μια υποδομή HTTP που περιλαμβάνει διακομιστές, μεσολάβησης, κρυφές μηνύες (από την πλευρά του παρόχου περιεχομένου) και προγράμματα περιήγησης ιστού (από την πλευρά του χρήστη) για να εγγυηθούν την επεκτασιμότητα. Το πρωτόκολλο HTTP/1.1, το οποίο δημιουργήθηκε και τυποποιήθηκε τη δεκαετία του 1990, χρησιμοποιείται συνήθως για ροή βίντεο. Ωστόσο, ως αποτέλεσμα της μετατόπισης από βασικές ιστοσελίδες που βασίζονται σε κείμενο σε περίπλοκες δομές που περιλαμβάνουν πολλά αρχεία σε διάφορους διακομιστές, αυτό το πρωτόκολλο θεωρείται ως ένας σημαντικός περιορισμός απόδοσης που μπορεί να έχει δυσμενή επίδραση στην Ποιότητα Εμπειρίας του Χρήστη – Quality of User Experience.

Αν και η κρυπτογράφηση στοχεύει πρωτίστως το επίπεδο εφαρμογής, οι πρόσφατες προσπάθειες έχουν κατευθυνθεί προς την υλοποίηση κρυπτογράφησης από άκρο σε άκρο στο επίπεδο μεταφοράς. Αυτή η τάση προς την κρυπτογράφηση αναμένεται να παραμείνει και ενδεχομένως να επιταχυνθεί στο μέλλον. Αν και είναι ζωτικής σημασίας για την ασφάλεια και το απόρρητο, η υιοθέτηση της κρυπτογράφησης από άκρο σε άκρο θέτει προκλήσεις για την Ποιότητα Εμπειρίας και τη διαχείριση δικτύου από τους φορείς

εκμετάλλευσης δικτύου. Για την αντιμετώπιση λειτουργικών ελλείψεων όπως για παράδειγμα η απουσία κρυπτογράφησης και η αδυναμία αιτήματος πολλαπλών αρχείων ταυτόχρονα, έχουν αναπτυχθεί πρωτόκολλα όπως το HTTP/2 και το QUIC. Τα πρωτόκολλα αυτά έχουν σχεδιαστεί με απώτερο σκοπό την ελαχιστοποίηση της καθυστέρησης όσον αφορά την ανταλλαγή δεδομένων των ιστοσελίδων, μειώνοντας έτσι σημαντικά το χρόνο φόρτωσης της εκάστοτε σελίδας. Αρκετές μελέτες έχουν εξετάσει τις επιπτώσεις αυτών των πρωτόκολλων στους χρόνους φόρτωσης της σελίδας και στις σχετικές μετρήσεις.

Είναι γνωστό πως η πλειοψηφία της Διαδικτυακής κίνησης αποτελείται πλέον από βίντεο. Σχεδόν τα τρία τέταρτα της συνολικής κίνησης στο Διαδίκτυο απεδείχθη βίντεο το 2022 (όπως βλέπουμε και γραφικά στην Εικόνα 1) και ο όγκος της κίνησης βίντεο σημείωσε σημαντικό πολλαπλασιασμό σε μέγεθος κατά τη διάρκεια των επόμενων ετών. Οι χειριστές δικτύου χρησιμοποιούν μια ποικιλία μηχανισμών διαχείρισης δικτύου για να φέρουν αποτελεσματικά εις πέρας τις αυστηρές απαιτήσεις Ποιότητας Εμπειρίας των σύγχρονων εφαρμογών ροής βίντεο. Συγκεκριμένα, δεδομένου ότι το αδειοδοτούμενο ραδιοφάσμα είναι ένας ακριβός και σπάνιος πόρος, οι φορείς εκμετάλλευσης δικτύων κινητής τηλεφωνίας χρησιμοποιούν τεχνικές διαχείρισης δικτύου που βασίζονται σε Deep Packet Inspection -DPI για τη βελτιστοποίηση του εύρους ζώνης και για αποτελεσματική κοινή χρήση του ραδιοφάσματος μεταξύ των χρηστών. Ωστόσο, η κρυπτογράφηση σπάει τους μηχανισμούς διαχείρισης δικτύου που χρησιμοποιούνται επί του παρόντος από τους χειριστές δικτύου για την παρακολούθηση και τη βελτιστοποίηση της Ποιότητας Εμπειρίας του Χρήστη.



Εικόνα 1. Απεικόνιση της αυξανόμενης δικτυακής κίνησης

1.2 Σημασία της μελέτης της διείσδυσης του HTTP/3 σε μεγάλους ISPs

Η συμβολή της εφαρμογής του HTTP/3 σε μεγάλους παρόχους υπηρεσιών Διαδικτύου (ISP), όπως για παράδειγμα η Google, Youtube, Meta είναι εξαιρετικά σημαντική. Παρακάτω παρατίθενται οι πιο σημαντικοί λόγοι:

- Εξέλιξη πρωτοκόλλου: Το σύστημα επικοινωνίας δεδομένων του World Wide Web είναι χτισμένο σε HTTP. Οι νεότερες εκδόσεις του HTTP, όπως το HTTP/2 και το HTTP/3 (με βάση το QUIC), έχουν σχεδιαστεί για να αυξάνουν την αποδοτικότητα, την ασφάλεια και την απόδοση καθώς οι τεχνολογίες Ιστού προχωρούν και οι απαιτήσεις των χρηστών αυξάνονται. Για να εγγυηθούν ότι οι καταναλωτές τους θα λαμβάνουν την καλύτερη δυνατή εξυπηρέτηση, οι πάροχοι υπηρεσιών Διαδικτύου πρέπει να προσαρμόσουν την υποδομή τους να χρησιμοποιεί αυτά τα πρωτόκολλα.
- Ενίσχυση της απόδοσης λόγω αντικατάστασης του TCP από το QUIC: Το QUIC έχει σχεδιαστεί για να μειώνει την καθυστέρηση που προέρχεται από τη δημιουργία σύνδεσης και να βελτιώνει την απόδοση σε αντίθεση με τα συμβατικά πρωτόκολλα που βασίζονται σε TCP. Οι ISP μπορούν να βελτιώσουν την ικανοποίηση των πελατών προσφέροντας στους πελάτες τους ταχύτερες και πιο ανταποκρινόμενες (responsive) εμπειρίες διαδικτυακής περιήγησης εφαρμόζοντας το QUIC.
- Ενίσχυση ασφάλειας: Το QUIC διαθέτει ενσωματωμένη κρυπτογράφηση, η οποία καθιστά τη μεταφορά δεδομένων πιο ασφαλή από ό,τι με παλαιότερα πρωτόκολλα όπως το HTTP/1.1. Αυτό βοηθά τους μεγάλους ISP να προστατεύουν τα προσωπικά δεδομένα πελατών και να αποτρέπουν διαδικτυακούς κινδύνους όπως η χειραγώγηση δεδομένων και η υποκλοπή.
- Ανταγωνιστικό πλεονέκτημα: Παρέχοντας καλύτερη απόδοση, ασφάλεια και αξιοπιστία, συγκριτικά πάντα με την αντιστοιχία αυτών από τους ανταγωνιστές που συνεχίζουν να χρησιμοποιούν ξεπερασμένη τεχνολογία, οι ISPs που υιοθετούν σύγχρονα πρωτόκολλα όπως το QUIC και το HTTP/3 μπορούν να ξεχωρίσουν στην αγορά. Αυτό θα μπορούσε να προσελκύσει επιπλέον πελάτες και να βελτιώσει τη θέση αυτών των ISP ως κορυφαίο προμηθευτή υπηρεσιών Διαδικτύου.

1.3 Σημασία του YouTube ως σημείο εστίασης στην παρούσα μελέτη

Αυτή η διατριβή εξετάζει πώς η εμπειρία χρήστη και η απόδοση του δημοφιλούς ιστότοπου ροής βίντεο του YouTube επηρεάζονται από τα πρωτόκολλα HTTP/3 και QUIC. Σε σύγκριση με τα συμβατικά πρωτόκολλα HTTP/1 και HTTP/2, τα HTTP/3 και QUIC προσφέρουν πιθανά κέρδη σε καθυστέρηση, απόδοση και αξιοπιστία, γεγονός που τα καθιστά αξιοσημείωτες εξελίξεις στα πρωτόκολλα επικοινωνίας ιστού. Η πρώτη ενότητα της μελέτης είναι μια διεξοδική αξιολόγηση της βιβλιογραφίας, η οποία συνοψίζει την κατάσταση της τεχνολογίας στο HTTP/3, QUIC και τις χρήσεις τους στη ροή βίντεο. Σημαντικά μέτρα απόδοσης αντιπαραβάλλονται μεταξύ των διαφόρων ρυθμίσεων πρωτοκόλλου, συμπεριλαμβανομένων των ρυθμών αποθήκευσης στην προσωρινή μνήμη, της απόδοσης.

Θα δούμε παρακάτω, πως αναλύονται βιβλιογραφικά η εισαγωγή του πρωτοκόλλου HTTP/3 σε μεγάλους ISPs, δίνοντας έμφαση στο Youtube, και ποια είναι η συνεισφορά του στο γενικό πλαίσιο της ποιότητας της εμπειρίας του χρήστη, και στην εξέλιξη της διαδικτυακής επικοινωνίας. Γίνεται ανάλυση των επιπτώσεων της μετάβασης του YouTube σε HTTP/3 και QUIC, λαμβάνοντας υπόψη τα πλεονεκτήματα και τα μειονεκτήματα για φορείς εκμετάλλευσης δικτύων, προμηθευτές περιεχομένου και τελικούς χρήστες.

Κεφάλαιο 2

Ανασκόπηση Βιβλιογραφίας

2.1 Επισκόπηση της βιβλιογραφίας για τα πρωτόκολλα HTTP/3 και QUIC

2.1.1 Τι είναι το πρωτόκολλο HTTP/3

Η πρώτη έκδοση του ευρέως αναγνωρισμένου Πρωτόκολλου Μεταφοράς Υπερκείμενου, ή αλλιώς του HTTP, εμφανίστηκε στη διάρκεια της δεκαετίας του 1990 με πρωταρχικό στόχο τη διευκόλυνση της μετάδοσης περιεχομένου πολυμέσων και υπερκειμενικών εγγράφων μέσω του Διαδικτύου. Το h1, με άλλα λόγια η έκδοση 1.1 του πρωτόκολλου αυτού κατείχε την κυρίαρχη θέση ανάμεσα στα πρωτόκολλα ιστού για σχεδόν δύο δεκαετίες, με εξαίρεση το 2014 όπου το ξεπέρασε η δεύτερη έκδοση, δηλαδή το HTTP/2. Το HTTP/2 εισήγαγε μια σειρά από καινοτόμες λειτουργίες, που στοχεύουν κυρίως στη βελτίωση του πλαισίου και της μεταφοράς δεδομένων. Παρά τις πολλαπλές μελέτες στις οποίες αμφισβητούνται τα οφέλη του, δεσμεύτηκε να βελτιώσει την ταχύτητα στο Διαδίκτυο.

Το HTTP/3 αποτελεί την πιο πρόσφατη διαδικασία τυποποίησης. Η έκδοση αυτή, έχει επιτύχει σταθερότητα και καθίσταται πλέον κατάλληλη για πρακτικές εφαρμογές. Οι κύριες βελτιώσεις που εισήχθησαν στην έκδοση h2 περιλαμβάνουν βελτιωμένη απόδοση συμπίεσης κεφαλίδας, προηγμένες λειτουργίες ασφάλειας οι οποίες προέρχονται από το TLS 1.3, και συγκεκριμένα, την ενσωμάτωση του QUIC στο επίπεδο μεταφοράς. Το πρωτόκολλο μεταφοράς QUIC, το οποίο δημιουργήθηκε αρχικά από την Google βασίζεται στο πρωτόκολλο UDP και επί του παρόντος βρίσκεται σε διαδικασία τυποποίησης [22]. Το πρωτόκολλο αυτό λοιπόν εκμεταλλεύεται το πρωτόκολλο TCP μεταφέροντας τον έλεγχο συμφόρησης στο χώρο χρήστη (user space) και επιτρέποντας έτσι ταχεία χειραψία. Επιπλέον, επιλύει το επίμονο πρόβλημα «μπλοκάρισμα εξαιτίας του επικεφαλής» ή όπως συναντάται στην αγγλική βιβλιογραφία του «Head of line Blocking», (συντομογραφία αυτού, που θα χρησιμοποιηθεί και σε επόμενα σημεία είναι το: «HoLb») επιτρέποντας έτσι την παρουσία πολλών αυτόνομων ροών σε μία μόνο σύνδεση.

2.1.2 Τί είναι το πρωτόκολλο QUIC

Το πρωτόκολλο QUIC πρωτοεμφανίστηκε το έτος 2012. Εκείνη τη χρονιά η Google εισήγαγε το QUIC ως πρωτόκολλο δικτύου επιπέδου μεταφοράς με στόχο την πιο

αποτελεσματική διαχείριση της κυκλοφορίας HTTP. Η αποτελεσματικότητα έγκειται στην υπόσχεση αυτού του πρωτοκόλλου να διεκπεραιώσει σημαντικά υψηλότερη μεταφοράς περιεχομένου HTTP και ταυτόχρονα, ελάχιστη καθυστέρηση δημιουργίας σύνδεσης (η οποία θεωρείται αναπόφευκτη στο πρωτόκολλο TCP). Ωστόσο αξίζει να σημειωθεί, ότι τα προαναφερθέντα πρωτόκολλα παρουσιάζουν δυσκολία στην αποτελεσματική διαχείριση της καθυστέρησης όσον αφορά το επίπεδο μεταφοράς. Η αδυναμία τους αυτή, οφείλεται στο γεγονός ότι βασίζονται στο πρωτόκολλο TCP. Αυτή η αδυναμία ήταν η αφορμή που οδήγησε την επιστημονική κοινότητα να αναπτύξει το πρωτόκολλο QUIC, και στην ουσία να αντικαταστήσει το TCP για τη διαχείριση της κρυπτογραφημένης κίνησης HTTP. Το QUIC βασίζεται στο πρωτόκολλο μεταφοράς UDP.

Το πρωτόκολλο QUIC, επιτρέπει την αυτόνομη αναμετάδοση υπό-ροών και διαχωρίζει από τους μηχανισμούς ελέγχου συμφόρησης. Αυτή η διαδικασία αναμένεται να βελτιώσει αρκετά την ποιότητα εμπειρίας των χρηστών, ή αλλιώς το QoE, βελτιώνοντας έτσι την ανταπόκριση του ιστότοπου, ιδιαίτερα σε καταστάσεις που χαρακτηρίζονται από μη βέλτιστες συνδέσεις δικτύου. Το HTTP/3 απαιτεί τη χρήση του TLS 1.3 [23], το οποίο είναι άμεσα ενσωματωμένο στο επίπεδο QUIC. Τέλος, ενεργοποιεί τις χειραψίες 1-RTT και την επανάληση 0-RTT, μειώνοντας έτσι σημαντικά τη διάρκεια που απαιτείται για τη δημιουργία σύνδεσης.

2.2 Πρωτόκολλο QUIC και ασφάλεια

Παρά τη διασφάλιση της επικοινωνιακής ασφάλειας των πληροφοριών που υπόσχεται το πρωτόκολλο QUIC, είναι εφικτή ακόμη η «παράνομη» διακοπή της συχνής επικοινωνίας μεταξύ πελάτη και διακομιστή. Παρακάτω, παρατίθενται διαφορετικά είδη προκλήσεων όσον αφορά την ασφάλεια του πρωτοκόλλου QUIC.

- I) «Επίθεση DDos Reflection»: Η επίθεση «DDos» έχει ως στόχο τον κατακλυσμό ενός διακομιστή – στόχου μέσω QUIC. Σε περιπτώσεις όπου ο αριθμός επιθέσεων κρίνεται σημαντικά μεγάλος, η αρμόδια «υπηρεσία θυμάτων» υπόκειται επιβράδυνση με αποτέλεσμα μια αντίστοιχη επίδραση σε χρήστες που έχουν εξουσιοδοτηθεί. Καθώς από τη φύση του το πρωτόκολλο QUIC είναι βασισμένο στο UDP, πράγμα που σημαίνει ελάχιστη παροχή

δεδομένων αποστολέα στο δέκτη, μια DDos επίθεση αποτελεί πράγματι σημαντική πρόκληση όσον αφορά τη διατήρηση ασφάλειας σε ένα δίκτυο με QUIC. Σε αυτό το σημείο βέβαια, αξίζει να σημειωθεί ότι το QUIC κλονίζεται ακόμη περισσότερο από επιθέσεις «DDoS Reflection». Στη συγκεκριμένη περίπτωση επίθεσης, μεγάλος αριθμός διακομιστών δέχεται πολλά ερωτήματα ενώ παράλληλα η διεύθυνση δικτυακού πρωτοκόλλου του μέρους – θύμα «αλλάζει παράνομα». Έπειτα, το θύμα, και όχι ο «δράστης», γίνεται ο παραλήπτης όλων των απαντημένων μηνυμάτων των διακομιστών. Εφόσον, η κρυπτογράφηση TCP – TLS εμπεριέχεται στο QUIC βάσει σχεδιασμού, το πιστοποιητικό TLS περιέχεται στο 1^ο απαντημένο μήνυμα, ενώ παράλληλα το μέγεθός του κρίνεται σημαντικά μεγαλύτερο από το μήνυμα ερωτήματος από την πλευρά του πελάτη. Με αυτό τον τρόπο, οι δράστες, καταφέρνουν να μποϊκοτάρουν ξένους διακομιστές με σκοπό την αποστολή σημαντικά μεγάλου αριθμού μηνυμάτων σε ένα οποιοδήποτε μέρος – στόχο.

- II) Άρνηση υπηρεσίας χειραψίας: Με στόχο την διαγραφή ψεύτικων δεδομένων, το QUIC, βάσει σχεδιασμού, επιτελεί πιστοποίηση και κρυπτογράφηση όσον αφορά τη διακίνηση δεδομένων. Τα τελικά σημεία, μέσω της τεχνολογίας – χειραψίας, απορρίπτουν παραποιημένα πακέτα. Έτσι η παραβίαση σε ενεργές ροές από μη επαληθευμένους χρήστες εμποδίζεται σημαντικά. Ωστόσο, κάποια ICMP περνάνε από αυτή τη διαδικασία χωρίς την πιστοποιημένη επαλήθευση τους αφού πραγματοποιηθεί μια ροή. Το restart με απύουσα κατάσταση, το οποίο εμφανίζει εξάρτιση ως προς την επαλήθευση του «token», αποτελεί ένα διαφορετικό είδος πακέτου με ικανότητα αναγνώρισης τελικού σημείου. Το πρωτόκολλο QUIC προστατεύει μια ροή αποκλειστικά από «έξω – δικτυακές» απειλές εκεί όπου υπάρχει εγκατάσταση σύνδεσης. Από την άλλη, η προστασία αυτή δεν επεκτείνεται και σε απειλές υποκλοπής πακέτων πριν την πραγματοποίηση της ροής.
- III) Απειλές εντός σύνδεσης. Στο [37] επεξηγείται η διαδικασία κατά την οποία μια πλαστή σύνδεση δύναται να γίνει αντιληπτή ως αληθής για μεγάλη διάρκεια, πράγμα που οδηγεί στην παραβίαση του «αναγνωριστικού σύνδεσης» χρησιμοποιούμενο από τον πελάτη στο στάδιο της χειραψίας. Η ανάλυση ωστόσο των λειψθέντων πληροφοριών δεν δύναται να αξιολογηθεί κανονικά. Έτσι, στη συνέχεια πραγματοποιείται δικτυακή διακοπή. Το «αναγνωριστικό διεύθυνσης πηγής» αποτελεί επίσης στόχο παραβίασης, η

οποία πραγματοποιείται παρόμοια με την παραπάνω διαδικασία, κατά την οποία κανένα μέλος της επικοινωνίας δεν έχει τη δυνατότητα να αναλύσει τα ληφθέντα δεδομένα. Η επιτυχία της σύνδεσης πετυχαίνει στα πρώτα μόλις δεύτερα πριν την διακοπή της.

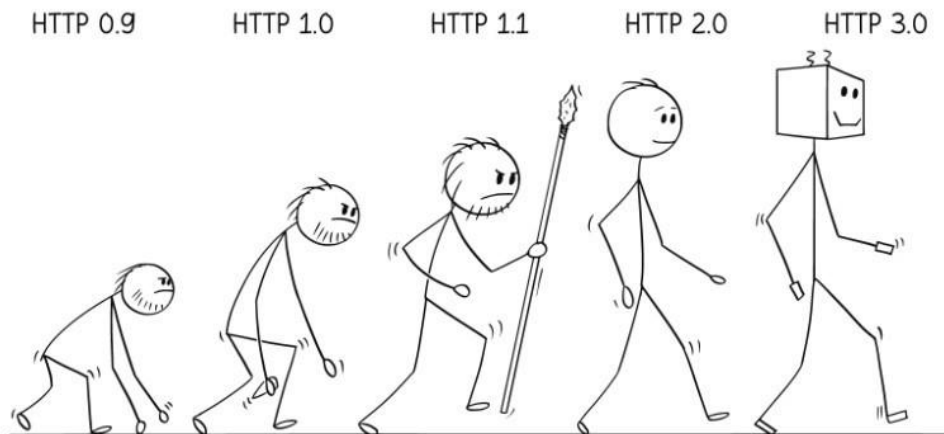
- IV) Απειλές εκτός σύνδεσης: Στο [37] περιγράφεται επίσης μια συνεχής απειλή «διαμόρφωσης διακομιστή». Εδώ, τα δεδομένα διαμόρφωσης του διακομιστή εκμαιεύονται από τον παράνομο χρήστη. Στη συνέχεια, τα δεδομένα και ένας μανδύας της IP διακομιστή αξιοποιούνται με σκοπό τη μετάδοση των πληροφοριών – reset στο μέλος – πελάτη, πράγμα που οδηγεί στην επαναφορά της ροής QUIC. Στο [22], βλέπουμε ότι ένα reset χωρίς κατάσταση, συχνά οδηγεί στην κατηγορία επιθέσεων (I) που αναλύσαμε πιο πάνω. Η επίθεση αυτή κρίνεται επιτυχής όταν μια σύνδεση γίνεται μεταξύ ενός αναγνωριστικού σύνδεσης και ενός αντίστοιχου αναγνωριστικού «reset χωρίς κατάσταση» Κατ' αυτόν τον τρόπο, η επαναφορά μιας ανοικτής ροής δύναται να γίνει με το αναγνωριστικό σύνδεσης παραγόμενο από τον εκάστοτε παράνομο χρήστη.
- V) Επίθεση Ανακλαστικής Ενίσχυσης και Επίθεση Κατάστασης Εξάντλησης.: Πολλές μελέτες σημείωσαν τον κίνδυνο πίσω από την ελλιπή ασφάλεια που προσφέρει η διαδικασία χειραψίας. Οι επιθέσεις αυτές είναι δυνατές, καθώς κατά την 1^η διαδρομή μετ' επιστροφής, γίνεται απόκριση του διακομιστή σε μη εξουσιοδοτημένη πηγή.
- VI) Επίθεση ACK: Στο [22] παρουσιάστηκε το εξής φλέγον ζήτημα ασφάλειας του πρωτόκολλου QUIC: δύναται από τη μεριά του παράνομου χρήστη η λήψη ενός «διακριτικού επικύρωσης διεύθυνσης διακομιστή». Ύστερα, μπορεί να αποκαλυφθεί εύκολα η IP που αξιοποιήθηκε με σκοπό την εκμαίευση του διακριτικού. Με σκοπό τη σύνδεση σε έναν διακομιστή, αξιοποιώντας μια 0-RTT, ο κακόβουλος χρήστης θα παραποιήσει την IP αυτή. Μετά από αυτό, η παραποίηση των ACK στον διακομιστή κρίνεται εύκολη καθώς ο κακόβουλος χρήστης πραγματοποιεί μετάδοση μεγάλου όγκου πληροφοριών στην IP.
- VII) Επιθέσεις κατακερματισμού και επανασυναρμολόγησης ροής: Με σκοπό την υπερφόρτωση του buffer, και τη δημιουργία μη αποτελεσματικής πληροφοριακής δομής, ένας κακόβουλος χρήστης μπορεί να προβεί σε μετάδοση «θραυσμάτων δεδομένων ροής». Ο κακόβουλος χρήστης, δεν

αναγνωρίζει επίτηδες πακέτα πληροφοριών ροής ώστε να πετύχει τη διατήρηση των μη επαληθευμένων πληροφοριών ροής του αποστολέα για αναμετάδοση.

- VIII) «Επιθέσεις δηλητηρίασης προσωρινής μνήμης»: Αφορά επίθεση κυβερνοχώρου κατά την οποία ένας κακόβουλος χρήστης μεταφέρει ψευδή δεδομένα σε μια κρυφή μνήμη Ιστού ή στην κρυφή μνήμη DNS με σκοπό να βλάψουν τους χρήστες.
- IX) Επιθέσεις «Slowloris»: Οι επιθέσεις αυτές μπορούν να πραγματοποιηθούν ενάντια σε ένα τελικό σημείο QUIC δημιουργώντας το μικρότερο δυνατό αριθμό δραστηριοτήτων που απαιτείται για να αποφευχθεί ο τερματισμός του λόγω αδράνειας. Στόχος τους είναι να διατηρήσουν όσο το δυνατόν περισσότερες συνδέσεις ανοιχτές στον προορισμό-στόχο, στέλνοντας αραιές ποσότητες δεδομένων, ανοίγοντας προοδευτικά παράθυρα ελέγχου ροής για τη ρύθμιση του ρυθμού αποστολέα ή δημιουργώντας πλαίσια ACK που μιμούνται υψηλό ποσοστό απώλειας.
- X) «Optimistic ACK Attack»: Ένας ελεγκτής συμφόρησης θα μπορούσε να επιτρέψει τη μετάδοση με ρυθμούς υψηλότερους από αυτούς που μπορεί να χειριστεί το δίκτυο, επειδή ένα τελικό σημείο αναγνωρίζει πακέτα που δεν έχει λάβει. Προκειμένου να προσδιοριστεί αυτή η συμπεριφορά, ένα τελικό σημείο μπορεί να παραλείψει αριθμούς πακέτων κατά τη μετάδοση πακέτων. Μόλις συμβεί αυτό, ένα τελικό σημείο έχει την επιλογή να τερματίσει αμέσως τη σύνδεση με σφάλμα σύνδεσης **PROTOCOL VIOLATION**
- XI) Πρόβλημα αμέλειας τείχους προστασίας: Όταν η διαδικτυακή κυκλοφορία ανακαλύπτεται από ένα τείχος προστασίας, συχνά περνά μέσω μιας διαδικτυακής μονάδας προστασίας που εκτελεί εκτενείς ελέγχους χρησιμοποιώντας βαθιά επιθεώρηση πακέτων και φιλτράρισμα ιστού. Τα τείχη προστασίας, αυτές τις μέρες, μπορούν να παρέχουν πολλές πληροφορίες, συμπεριλαμβανομένων βελτιωμένων αναφορών και σάρωσης κακόβουλου λογισμικού. Ωστόσο, τα περισσότερα τείχη προστασίας δεν αναγνωρίζουν την κυκλοφορία QUIC ως διαδικτυακή κίνηση. Τα πακέτα QUIC δεν λαμβάνουν τον ίδιο αριθμό επιθεώρησης και καταγραφής. Αυτό εγείρει σοβαρά ζητήματα ασφάλειας με συνέπειες όπως η αδυναμία περιορισμού της πρόσβασης σε ιστότοπους ή η ενεργοποίηση της ασφαλούς αναζήτησης στο Google.

2.2.1 Ιστορικό πλαίσιο και ανάπτυξη αυτών των πρωτοκόλλων

Evolution of HTTP protocol



Σε αυτή την υπό ενότητα, θα προβούμε σε μια γενική ανάλυση πρωτοκόλλων που προηγούνται των HTTP/3 και QUIC. Μία τέτοια επεξήγηση και ανάλυση προηγούμενων πρωτοκόλλων, καθώς και των μεταξύ τους σχέσεων, θεωρείται αναγκαία, καθώς, όπως έχουμε προαναφέρει, τα HTTP/3 και QUIC είναι ουσιαστικά μετεξελίξεις προηγούμενων γενιών – πρωτοκόλλων. Έτσι, παρακάτω, αναλύονται (κυρίως επιγραμματικά) τα: HTTP, HTTPS, HTTP/2, SSL/TLS, SPDY, UDP, TCP. Εν γένει, αξίζει να σημειωθεί πως επί το πλείστον, το HTTP (1997), το οποίο βασίζεται στο Πρωτόκολλο Ελέγχου μετάδοσης ή αλλιώς στο TCP (1981), είναι το πρωτόκολλο εκείνο το οποίο συναντάται περισσότερο από κάθε άλλο πρωτόκολλο στα πρωτόκολλα περιήγησης στο Ίντερνετ. Από την άλλη, το πρωτόκολλο δεδομένων χρήστη, ή αλλιώς το UDP αποτελεί το πρωτόκολλο εκείνο στο οποίο βασίζεται το HTTP3 μέσω του πρωτοκόλλου QUIC. Παρόλες τις διαφορές που παρουσιάζουν αυτά τα πρωτόκολλα, εμπεριέχουν συνάμα κοινούς στόχους και χρησιμοποιούμενες τεχνολογίες.

- Το HTTP/0.9 το οποίο αποτελεί την πρωταρχική έκδοση του πρωτοκόλλου HTTP, εισήχθη στο επιστημονικό κοινό από τον Tim Berners-Lee στο Σερν, το 1990. Η συγκεκριμένη έκδοση υποστήριζε αποκλειστικά α) αιτήματα GET και μεταφορά εγγράφων HTML.
- Ο ορισμός του HTTP/1.0 καθιερώθηκε στο RFC 1945 το έτος 1996. Στο συγκεκριμένο RFC περιγράφονται οι επικρατούσες μέθοδοι και εφαρμογές του

HTTP κατά την ανάπτυξή του από διάφορες οντότητες, οι οποίες συχνά οδηγούσαν σε ζητήματα διαλειτουργικότητας. Ένας σημαντικός εγγενής περιορισμός αυτής της έκδοσης HTTP συναντάται στην αδυναμία επαναχρησιμοποίησης μιας σύνδεσης για πολλαπλά ερωτήματα.

- Η πρωταρχική τυποποιημένη έκδοση του HTTP, γνωστή και ως HTTP/1.1 (ή h1) , εισήχθη το 1997, μέσω του RCF 2068. Η έκδοση αυτή περιλάμβανε πρόσθετες λειτουργίες όπως νέες κεφαλίδες, επαναχρησιμοποίηση σύνδεσης, διοχέτευση τέτοια που επιτρέπει τη μετάδοση πολλών αιτημάτων πριν από τη λήψη απάντησης καθώς και λοιπές συμπληρωματικές λειτουργίες.
- Η μετάδοση δεδομένων κειμένου περιορίστηκε στα πρωτόκολλα HTTP/0.9, HTTP/0 και HTTP/1.1. Το HTTP/2, ή αλλιώς h2 συνιστά ένα δυαδικό πρωτόκολλο το οποίο καθορίστηκε το 2015 στο RFC 7540. Η έννοια του HTTP/2 προέρχεται από το Google SPDY1. Περαιτέρω λειτουργίες περιλαμβάνουν την ενοποίηση αιτημάτων (με τη χρήση ροών) σε μια μεμονωμένη σύνδεση, ιεράρχηση των ροών και περαιτέρω δυνατότητες.
- Η μετεξέλιξη του HTTP/2, ή αλλιώς το HTTP/3 (h3), έλαβε χώρα τον Ιούνιο του 2022. Το πρωτόκολλο αυτό χρησιμοποιεί το πρωτόκολλο QUIC, το οποίο όπως ήδη αναφέραμε, αποτελεί πρωτόκολλο μεταφοράς βασιζόμενο στο UDP (σε αντίθεση με τα υπόλοιπα προηγούμενα πρωτόκολλα τα οποία βασίζονται στο TCP. Η αρχική ανάπτυξη του QUIC έγινε στην Google. Τα δυο αυτά πρωτόκολλα λοιπόν, προσφέρουν παραπάνω λειτουργίες, όπως η δυνατότητα για χειραψίες 0-RTT2, συμπίεση κεφαλίδας με QPACK και διάφορες λοιπές βελτιώσεις. Στις επόμενες ενότητες, αναλύονται περαιτέρω εκτενώς οι τεχνολογίες αυτές.

2.2.2 HTTP/1.0

Μηνύματα: Το HTTP χρησιμοποιεί μηνύματα HTTP για να διευκολύνει τη μετακίνηση δεδομένων, μεταξύ τελικών σημείων, όπως διακομιστή και πελάτη. Τα μηνύματα δύναται να ταξινομηθούν σε δύο ξεχωριστές κατηγορίες. Τα αιτήματα εξυπηρετούν είτε την ανάκτηση είτε τη μετάδοση δεδομένων. Οι απαντήσεις αποτελούν αντίστοιχες απαντήσεις σε μια δεδομένη είσοδο. Οι επικοινωνίες HTTP συνήθως περιλαμβάνουν τρία κύρια στοιχεία: α) μια γραμμή αιτήματος ή μια γραμμή κατάστασης, β) μια συλλογή κεφαλίδων που χρησιμεύουν για τη μετάδοση περαιτέρω πληροφοριών και γ) το σώμα

του μηνύματος που περιέχει τα πραγματικά δεδομένα. Τα αιτήματα περιλαμβάνουν συνήθως μια γραμμή αιτήματος που περιλαμβάνει μια μέθοδο HTTP (όπως GET, POST, PUT, κ.α.), ένα αίτημα URL για τον καθορισμό του διακομιστή και του πόρου που πρόκειται να ανακτηθεί ή να παραδοθεί και την έκδοση HTTP. Μια γραμμή κατάστασης αποτελείται από την έκδοση HTTP, έναν κωδικό κατάστασης για να υποδείξει την επιτυχία ενός αιτήματος και μια φράση αιτιολογίας, η οποία είναι γραπτή περιγραφή του κωδικού κατάστασης. Οι απαντήσεις περιέχουν γραμμές κατάστασης.

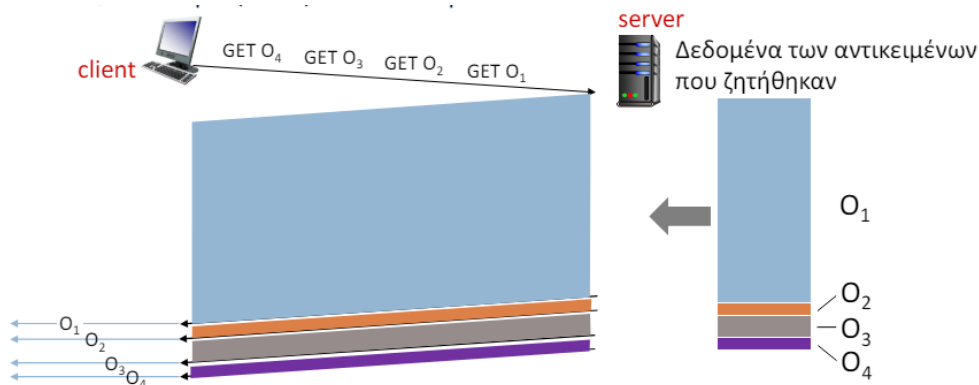
Κεφαλίδες: Οι κεφαλίδες χρησιμοποιούνται για τη μετάδοση συμπληρωματικών πληροφοριών μαζί με ένα μήνυμα. Αποτελούν υποχρεωτικά στοιχεία που οφείλεται να περιλαμβάνονται τόσο στα αιτήματα όσο και στις απαντήσεις. Κεφαλίδες όπως οι «Content-Length» και «Cache-Control» χρησιμοποιούνται για να υποδείξουν το μήκος του σώματος του μηνύματος, τον τύπο του πόρου που μεταφέρεται μέσω του σώματος του μηνύματος, τις οδηγίες για τους μηχανισμούς προσωρινής αποθήκευσης σχετικά με τον τρόπο αποθήκευσης των πόρων στην κρυφή μνήμη και τα cookie που παρέχουν διαχείριση κατάστασης σε HTTP.

2.2.3 HTTP/1.1

Μόνιμες Συνδέσεις: Σε αντίθεση με το HTTP/1.0, το HTTP/1.1 επιτρέπει τη δημιουργία μόνιμων συνδέσεων. Αυτό σημαίνει ότι είναι δυνατή η μετάδοση πολυάριθμων αιτημάτων και απαντήσεων μέσω μιας μεμονωμένης σύνδεσης TCP. Η γενική επιβάρυνση μειώνεται εξαλείφοντας την ανάγκη ανοίγματος πολλών συνδέσεων TCP για πολλαπλά αιτήματα. Η διοχέτευση εισάγεται επίσης από το h1. Η έννοια της διοχέτευσης επιτρέπει τη μετάδοση πολλών αιτημάτων ταυτόχρονα, χωρίς να χρειάζεται να περιμένουμε τις απαντήσεις των προηγούμενων. Η αναμετάδοση των απαντήσεων σε αιτήματα με διοχέτευση θα πρέπει να ακολουθεί τη διαδοχική σειρά με την οποία ελήφθησαν. Η διοχέτευση δεν είναι δυνατή για μη ισχυρά αιτήματα, όπως αυτά που γίνονται μέσω της μεθόδου POST.

Περιορισμοί του HTTP/1.1: Ένα ζήτημα που σχετίζεται με τη διοχέτευση είναι το HoLB. Το HoLB μπορεί να εμφανιστεί όταν το αρχικό αίτημα αφορά ένα σημαντικό μέγεθος αρχείου. Η μετάδοση αυτού του μεγάλου αρχείου θα έχει ως αποτέλεσμα την παρεμπόδιση των επακόλουθων απαντήσεων. Η διοχέτευση, η οποία στην αγγλική

βιβλιογραφία απαντάται ως «pipelining» συνήθως δεν προτιμάται από πελάτες και διακομιστές λόγω της δύσκολης υλοποίησης της. Για την αντιμετώπιση αυτού του ζητήματος, δημιουργούνται πολλαπλές συνδέσεις TCP προκειμένου να μεταδίδονται ταυτόχρονα πολλαπλά αιτήματα. Αυτό έχει ως αποτέλεσμα αυξημένα γενικά έξοδα, ιδιαίτερα όταν χρησιμοποιείται το HTTPS. Έτσι, τα προγράμματα περιήγησης επέβαλαν περιορισμούς στον αριθμό των επιτρεπόμενων συνδέσεων TCP ανά κεντρικό υπολογιστή. (Εικόνα 2)



Εικόνα 2. Διαδικασία HolB

2.2.4 TCP

Ένα από τα κύρια και πιο σημαντικά πρωτόκολλα μεταφοράς είναι το TCP. Το πρωτόκολλο συνοδεύεται από πολλά πλεονεκτήματα όπως σταθερότητα, αξιοπιστία και έλεγχο συμφόρησης βάσει απωλειών. Παρόλο που συμβάλει στον έλεγχο συμφόρησης, το πρωτόκολλο αυτό δεν θεωρείται απόλυτα αποτελεσματικό όσον αφορά την ανάκτηση απωλειών. Το πρωτόκολλο σε επίπεδο εφαρμογής που ονομάζεται HTTP, διευκολύνει τους χρήστες να έχουν πρόσβαση σε σελίδες και υλικό υπερκειμένου και άλλους πόρους σε μια ιστοσελίδα. Το πρωτόκολλο αυτό εφαρμόζεται πάνω από το TCP και αποτελεί βάση για αντίστοιχα πρωτόκολλα. Ενδεικτικά αναφέρουμε τα WebSocket, HTTPS όπως και επόμενες εκδόσεις του HTTP (2 και 3). Το πιο κύριο «σφάλμα» θα έλεγε κανείς του HTTP είναι ότι δεν μερίμνησε για τη μέγιστη χρήση του εύρους ζώνης και της ασφάλειας. Αυτό βέβαια έγκειται στο γεγονός ότι το HTTP δημιουργήθηκε κατά το αρχικό στάδιο του Διαδικτύου.

2.2.5 SSL

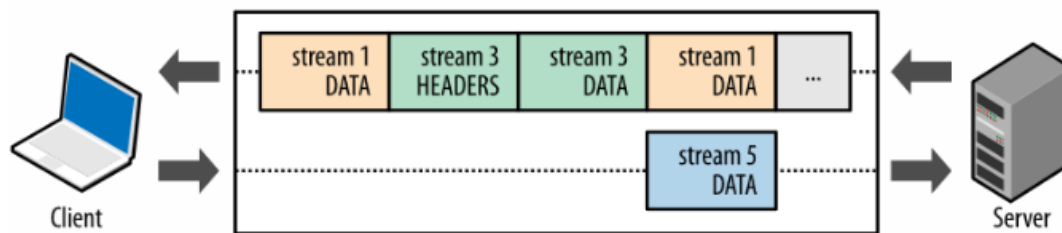
Τα πρωτόκολλα ασφάλειας που αποτελούν τα α) Πρωτόκολλο Επιπέδου ασφαλούς υποδοχής, ή αλλιώς το SSL, και β) Πρωτόκολλο Ασφάλειας επιπέδου μεταφοράς, ή αλλιώς το TLS, προορίζονται να παρέχουν κρυπτογραφημένες και εξουσιοδοτημένες επικοινωνιακές σχέσεις μεταξύ υπολογιστών. Παράλληλα, η ασφαλής έκδοση του HTTP, γνωστή ως HTTPS, εν ολίγοις, κρυπτογραφεί την επικοινωνία HTTP και υπόσχεται διασύνδεση ασφάλειας μεταξύ του πελάτη και του διακομιστή μέσω του πρωτόκολλου ασφάλειας TLS. Ωστόσο, αξίζει να σημειωθεί, πως κατά την ανταλλαγή ζευγών κλειδιών μεταξύ του πελάτη και του προγράμματος περιήγησης, το HTTPS προϋποθέτει πλήρη χρονική καθυστέρηση μετ' επιστροφής.

2.2.6 HTTP/2

Το πρωτόκολλο HTTP/2.0 ή αλλιώς (πιο ευρέως χρησιμοποιημένο) HTTP/2, όπως περιγράφεται από τους Belshe, Peon και Thomson, προήλθε από αρχικές δοκιμές που διεξήγαγε η Google, οι οποίες συναντώνται ως πρωτόκολλο SPDY. Αρχικά, κρίθηκε σημαντικό να διατηρηθεί η συμβατότητα μεταξύ του HTTP/2 και του αρχικού πρωτόκολλου HTTP/1.1. Ταυτόχρονα, η έκδοση αυτή μειώνει την καθυστέρηση δημιουργίας σύνδεσης και παράλληλα ενισχύει την ταχύτητα φόρτωσης της σελίδας μέσω της χρήσης της πολυπλεξίας ροής, της ώθησης διακομιστή και της τεχνικής συμπίεσης κεφαλίδων. Επιπλέον, αντιμετωπίζει το πρόβλημα του HoLB στο HTTP.

Πολυπλεξία: Η επικοινωνία που ξεκινά από έναν πελάτη και έναν διακομιστή μέσω HTTP2 πραγματοποιείται μέσω μιας μεμονωμένης σύνδεσης TCP. Η σύνδεση δικτύου χωρίζεται σε πολλές ροές, με κάθε ανταλλαγή αιτήματος και απάντησης να έχει τη δική της ροή. Μια ροή καταναλώνεται πλήρως από μια ανταλλαγή αιτήματος/απόκρισης. Οι πελάτες και οι διακομιστές έχουν τη δυνατότητα να ξεκινούν νέες ροές. Κάθε ροή διαθέτει ένα μοναδικό αναγνωριστικό, το οποίο εκχωρείται από το τελικό σημείο που ξεκινά τη ροή και είναι μη ανακυκλώσιμο, και προαιρετικές πληροφορίες προτεραιότητας που αξιοποιούνται για τη μεταφορά αμφίδρομων μηνυμάτων. Κάθε μήνυμα είναι ένα λογικό μήνυμα HTTP, (για παράδειγμα μήνυμα αιτήματος ή απάντησης) που αποτελείται από ένα ή περισσότερα πλαίσια. Ο όρος πλαίσιο – frame αναφέρεται ως η πιο μικρή μονάδα επικοινωνίας που μεταφέρει έναν συγκεκριμένο τύπο δεδομένων, όπως είναι οι κεφαλίδες HTTP. Το ενσωματωμένο αναγνωριστικό ροής στην κεφαλίδα κάθε πλαισίου επιτρέπει στα πλαίσια από διάφορες ροές να παρεμβληθούν και

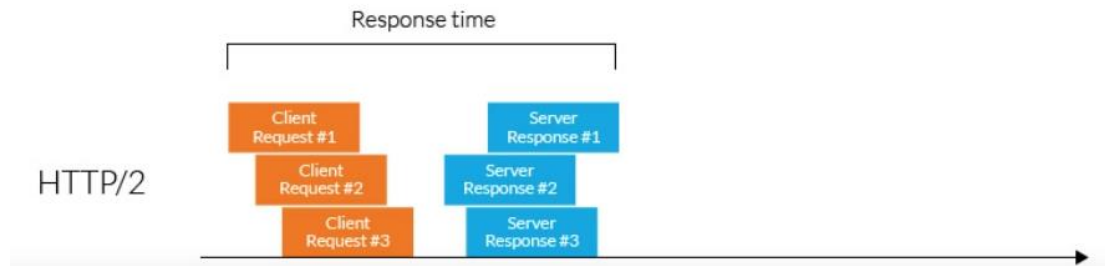
στη συνέχεια να επανασυναρμολογηθούν. Υπάρχουν διάφορες κατηγορίες πλαισίων. Το «DATA frame», είναι υπεύθυνο για την αποθήκευση δεδομένων, ενώ το πλαίσιο «HEADER», χρησιμοποιείται για την έναρξη του ανοίγματος μιας ροής. Κάθε σύνδεση περιέχει μια ροή με αναγνωριστικό μηδέν, η οποία χρησιμοποιείται για την ανταλλαγή μηνυμάτων ελέγχου. Σε αντίθεση με το HTTP/1, το οποίο, μεταδίδει κυρίως πληροφορίες σύνδεσης μέσω κεφαλίδων, το HTTP/2 παρέχει αυτές τις πληροφορίες κυρίως μέσω της ροής ελέγχου.



Εικόνα 3. Σύνδεση HTTP/2

Με τη βοήθεια της πολυπλεξίας το HTTP/2 εξαλείφει το πρόβλημα HoLB και επιτρέπει στους πελάτες και τους διακομιστές να στέλνουν πολλαπλά αιτήματα και απαντήσεις σε μία μόνο σύνδεση TCP.

Προτεραιότητα: Το HTTP/2 επιτρέπει στους πελάτες και τους διακομιστές να εκχωρούν προτεραιότητες σε μια ομάδα αιτημάτων που μπορούμε να ελέγξουμε τη σειρά των αναμενόμενων απαντήσεων. Αυτή η ιεράρχηση προτεραιοτήτων βοηθά να διασφαλιστεί ότι οι πιο σημαντικοί πόροι παραδίδονται πρώτα, βελτιώνοντας την εμπειρία χρήστη και τους χρόνους φόρτωσης της σελίδας. Οι ροές στο HTTP2 δύνανται να παρουσιάσουν αλληλεξάρτηση με άλλες ροές. Η προτεραιότητα μιας εξαρτώμενης είναι σταθερά χαμηλότερη από εκείνη του γονέα του. Όταν μια ροή υφίσταται εκ νέου ιεράρχηση προτεραιότητας, οι εξαρτώμενες από αυτή υφίστανται επίσης μια αντίστοιχη κίνηση. Μια ανεξάρτητη ροή ορίζεται ως η ροή που έχει το αναγνωριστικό μηδέν όπως και η ροή – γονέας. Στην περίπτωση που υπάρχει εξάρτηση μεταξύ δύο ροών, η οποία μπορεί να περιλαμβάνει τη μηδενική ροή, δύναται να εκχωρηθούν αντίστοιχα βάρη τα οποία κυμαίνονται από 1 έως 256 σε κάθε ροή. Σε τέτοιες περιπτώσεις, οι πόροι θα πρέπει να κατανέμονται αναλογικά με βάση το βάρος που αποδίδεται σε κάθε ροή. Η πράξη ανάθεσης προτεραιοτήτες αποτελεί απλώς μια σύσταση και δεν είναι υποχρεωτική η τήρηση άλλων τελικών σημείων.



Εικόνα 4 Το H2 οδηγεί σε σημαντική μείωση του αριθμού των TCP συνδέσεων

Push διακομιστή: Το πρωτόκολλο HTTP/2 επιτρέπει στον εκάστοτε διακομιστή να μεταδίδει δεδομένα σε έναν αντίστοιχο πελάτη χωρίς την απαίτηση ειδικού αιτήματος από τον τελευταίο. Η περίπτωση κατά την οποία ένας πελάτης ξεκινά ένα μήνυμα - αίτημα για κάποιον ιστότοπο από το διακομιστή, αποδεικνύεται πλεονεκτική. Αντί να μεταδίδει αποκλειστικά το HTML και να περιμένει αιτήματα για επιπρόσθετους πόρους, ένας διακομιστής έχει τη δυνατότητα να προωθήσει απευθείας αυτούς τους πόρους (πχ CSS και εικόνες). Πριν τη μετάδοση δεδομένων στον πελάτη, ο διακομιστής οφείλει να μεταδώσει ένα πλαίσιο «PUSH PROMISE» με σκοπό την ειδοποίηση του πελάτη σχετικά με την ώθηση.

Έλεγχος Ροής: Το HTTP/2 υποστηρίζει λειτουργικά τον έλεγχο ροής, ή αλλιώς το «flow control» για πλαίσια δεδομένων τόσο στο επίπεδο μεμονωμένης ροής όσο και στο συνολικό επίπεδο σύνδεσης. Ο έλεγχος ροής θεωρείται εγγενώς συνδεδεμένος με τη σύνδεση και δεν δύναται να απενεργοποιηθεί. Ο παραλήπτης έχει τη δυνατότητα να ελέγχει την ποσότητα δεδομένων που λαμβάνει με τη μετάδοση του πλαισίου «WINDOW UPDATE» στο αντίθετο τελικό σημείο.

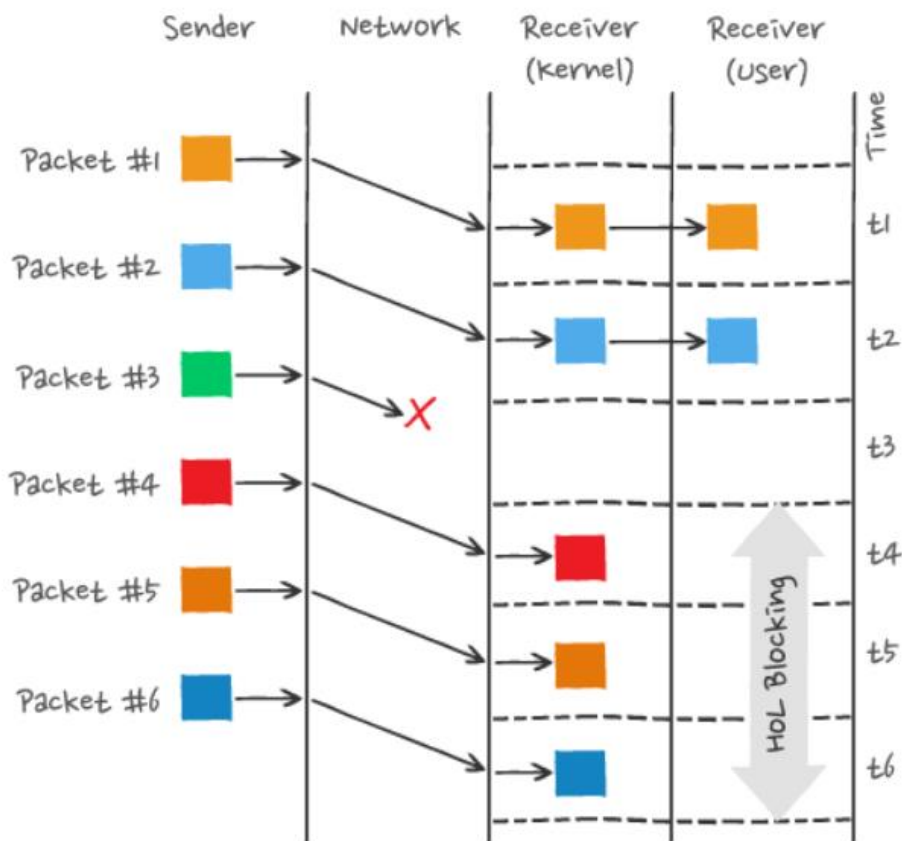
Περιορισμοί του HTTP/2: Ένα πρόβλημα που συναντάται στο πρωτόκολλο HTTP/2 είναι οι οικονομικές επιπτώσεις του TCP και TLS, καθώς η δημιουργία μιας σύνδεσης απαιτεί την ολοκλήρωση των χειραψιών. Το TLS αποτελεί προαιρετικό γνώρισμα του HTTP/2. Ωστόσο, είναι γεγονός ότι τα περισσότερα προγράμματα περιήγησης υποστηρίζουν αποκλειστικά το HTTP/2 μέσω του πρωτοκόλλου TLS. Κατά τη διάρκεια της εξέλιξης του Διαδικτύου και του HTTP, ο βασικός μηχανισμός μεταφοράς του HTTP παρέμεινε, σε μεγάλο βαθμό, ο ίδιος. Ωστόσο, καθώς ο μέσος όρος επίσκεψης στο Διαδίκτυο έχει αυξηθεί μετά τη μαζική δημόσια υιοθέτηση της τεχνολογίας φορητών συσκευών, το HTTP ως πρωτόκολλο δυσκολεύεται να προσφέρει μια ομαλή, διαφανή

εμπειρία περιήγησης στον Ιστό. Και με την αυξανόμενη ζήτηση για εφαρμογές σε πραγματικό χρόνο, οι ελλείψεις του HTTP/2 έγιναν όλο και πιο εμφανείς.

Πρώτον, η τελική έκδοση του HTTP/2 δεν περιελάμβανε πολλές από τις αναμενόμενες βελτιώσεις στην αναβάθμιση από το HTTP/1.1. Για να παραμείνει συμβατό με το HTTP/1.1, το πρωτόκολλο έπρεπε να διατηρεί τα ίδια αιτήματα POST και GET, κωδικούς κατάστασης (200, 301, 404 και 500) και ούτω καθεξής. Επίσης, ορισμένες από τις δυνατότητες που εφαρμόστηκαν εισήγαγαν ζητήματα ασφάλειας. Εκτός από την παλαιού τύπου έλλειψη υποχρεωτικής κρυπτογράφησης, αυτό περιλάμβανε κεφαλίδες σελίδων συμπίεσης και cookie τα οποία βρέθηκαν ευάλωτα σε επιθέσεις.

Το πρωτόκολλο h2 έρχεται να λύσει το ζήτημα του HoLB. Η λύση που προσφέρει το H2 είναι η κοινή χρήση τομέα, η οποία περιλαμβάνει τη διανομή πόρων σε πολλούς κεντρικούς υπολογιστές προκειμένου να παρακαμφθεί αυτός ο περιορισμός. Στη συνέχεια, τα προγράμματα περιήγησης επέβαλαν περιορισμούς στη συνολική ποσότητα των συνδέσεων TCP. Πρόσθετες λύσεις για το h1 περιλαμβάνουν τη χρήση CSS sprinting.

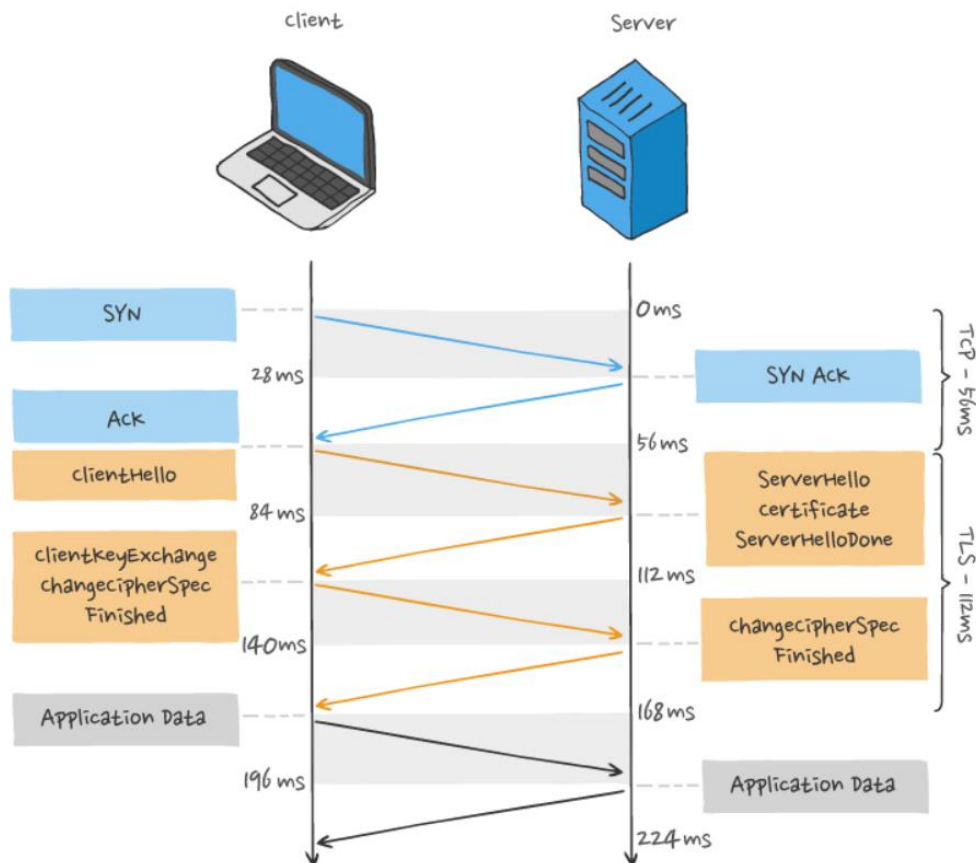
Περιορισμοί TCP: Το συρόμενο παράθυρο του δέκτη του TCP δεν προχωρά εάν ένα τμήμα με μικρότερο αριθμό σειράς δεν έχει φτάσει / έχει ληφθεί ακόμη, ακόμη και αν έχουν φτάσει τα τμήματα με μεγαλύτερο αριθμό. Αυτό μπορεί να προκαλέσει στιγμιαία διακοπή ή ακόμα και διακοπή της ροής, ακόμη και στην περίπτωση που ένα μόνο τμήμα δεν καταφέρει να φτάσει. Αυτό το πρόβλημα είναι γνωστό ως αποκλεισμός HoLB σε επίπεδο πακέτου.



Εικόνα 5. Το ζήτημα του HoLB μπορεί να οδηγήσει σε διακοπή ροής

Το TCP δεν υποστηρίζει πολυπλεξία σε επίπεδο ροής: Ενώ το TCP επιτρέπει πολλαπλές λογικές συνδέσεις προς και από το επίπεδο εφαρμογής, δεν επιτρέπει την πολυπλεξία πακέτων δεδομένων σε μία μόνο ροή TCP. Με το HTTP/2, το πρόγραμμα περιήγησης μπορεί να ανοίξει μόνο μία σύνδεση TCP με τον διακομιστή. Χρησιμοποιεί την ίδια σύνδεση για να ζητήσει πολλά αντικείμενα, όπως CSS, JS και άλλα αρχεία. Κατά τη λήψη αυτών των αντικειμένων, το TCP σειριοποιεί όλα τα αντικείμενα στην ίδια ροή.

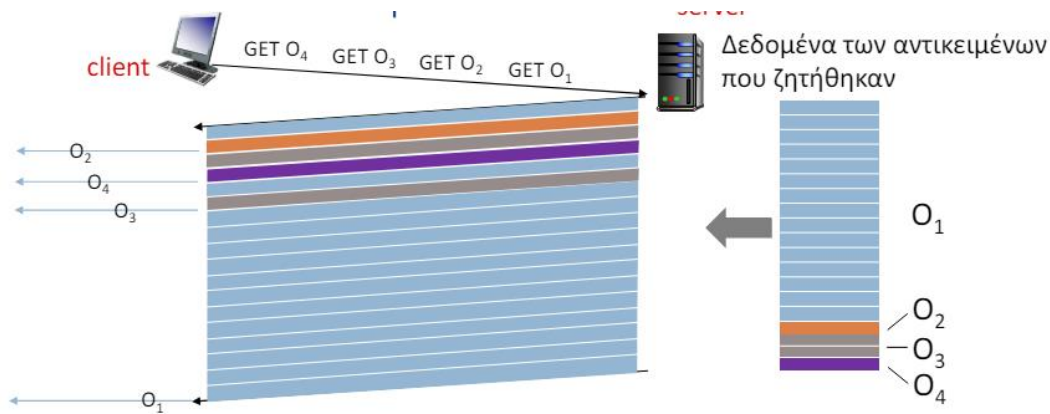
Το TCP προκαλεί περιττή επικοινωνία: Κατά την πραγματοποίηση της χειραψίας σύνδεσης, το TCP ανταλλάσσει μια ακολουθία μηνυμάτων, μερικά από τα οποία είναι περιττά εάν η σύνδεση δημιουργηθεί με έναν γνωστό κεντρικό υπολογιστή.



Εικόνα 6. Χειραψία TCP+TLS στην αρχή μιας συνεδρίας επικοινωνίας που χρησιμοποιεί κρυπτογράφηση TLS

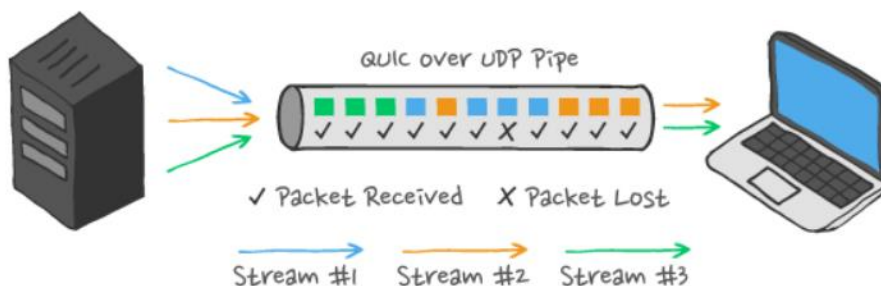
Έχοντας τα παραπάνω υπόψιν, το QUIC εισήχθη με σκοπό την αφορία των δυσκολιών που αναλύθηκαν παραπάνω. Ένα σημαντικό πλεονέκτημα είναι ότι το QUIC είναι χτισμένο σε επίπεδο χρήστη, επομένως δεν απαιτεί αλλαγές στον πυρήνα με κάθε αναβάθμιση πρωτοκόλλου, ανοίγοντας το δρόμο για ευκολότερη υιοθέτηση.

Το QUIC εισάγει την έννοια των πολλαπλών ροών που πολυπλέκονται σε μία μόνο σύνδεση. Βάσει σχεδιασμού, εφαρμόζει ξεχωριστό έλεγχο ροής ανά κάθε ροή, πράγμα που αποτελεί λύση στο ζήτημα HoLB



Εικόνα 7. Το HOLB λύνεται μέσω του κατακερματισμού πόρων

Το HTTP/2 είχε αρχικά αντιμετωπίσει αυτό το θέμα μόνο σε επίπεδο HTTP. Ωστόσο, στο HTTP/2, το HoL σε επίπεδο πακέτου της ροής TCP θα μπορούσε να μπλοκάρει όλες τις συναλλαγές στη σύνδεση.

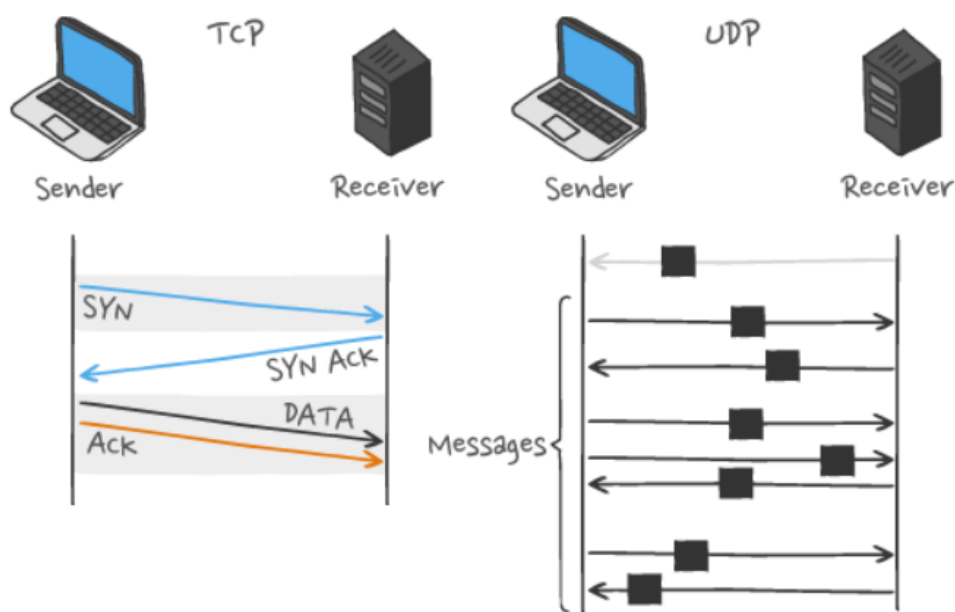


Εικόνα 8. Με τη βοήθεια του πρωτοκόλλου UDP, αντιμετωπίζεται το πρόβλημα HoLB

2.2.7 HTTP/3

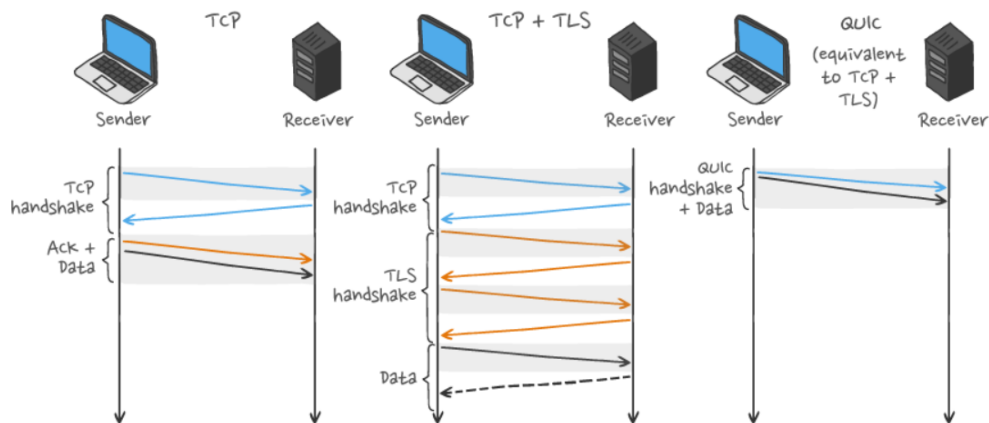
Η πιο πρόσφατη έκδοση του HTTP αναφέρεται ως HTTP/3 ή αλλιώς h3. Το h3 λειτουργεί πάνω από το QUIC, πρωτόκολλο που βασίζεται σε UDP και TLS. Το QUIC μετριάξει το πρόβλημα του TCP HoLB. Το HTTP/3 ενσωματώνει πολλαπλά χαρακτηριστικά τα οποία παρουσιάστηκαν αρχικά με το HTTP/2. Ορισμένες υλοποιήσεις ενσωματώνονται αμέσως στο HTTP/3, ενώ άλλες έχουν μεταφερθεί στο QUIC. Η έννοια του h3 αρκετά συμβατή με εκείνη των προηγούμενων 2 εκδόσεων. Όπως το HTTP/2, έτσι και το HTTP/3 διευκολύνει την επέκταση πρωτοκόλλου. Το HTTP/3 είναι επίσης συμβατό με το διακομιστή push

Ο στόχος του HTTP/3 είναι να παρέχει γρήγορες, αξιόπιστες και ασφαλείς συνδέσεις ιστού σε όλες τις μορφές συσκευών, διορθώνοντας τα ζητήματα που σχετίζονται με τη μεταφορά του HTTP/2. Για να γίνει αυτό, χρησιμοποιεί ένα διαφορετικό πρωτόκολλο δικτύου επιπέδου μεταφοράς, ονομαστέι QUIC, το οποίο εκτελείται μέσω πρωτοκόλλου Διαδικτύου UDP αντί του TCP που χρησιμοποιείται από όλες τις προηγούμενες εκδόσεις του HTTP. Σε αντίθεση με το σύστημα ανταλλαγής διατεταγμένων μηνυμάτων του TCP, το UDP επιτρέπει τη μετάδοση μηνυμάτων πολλαπλών κατευθύνσεων, η οποία, μεταξύ άλλων, βοηθά στην αντιμετώπιση του HoLB στο επίπεδο πακέτου.



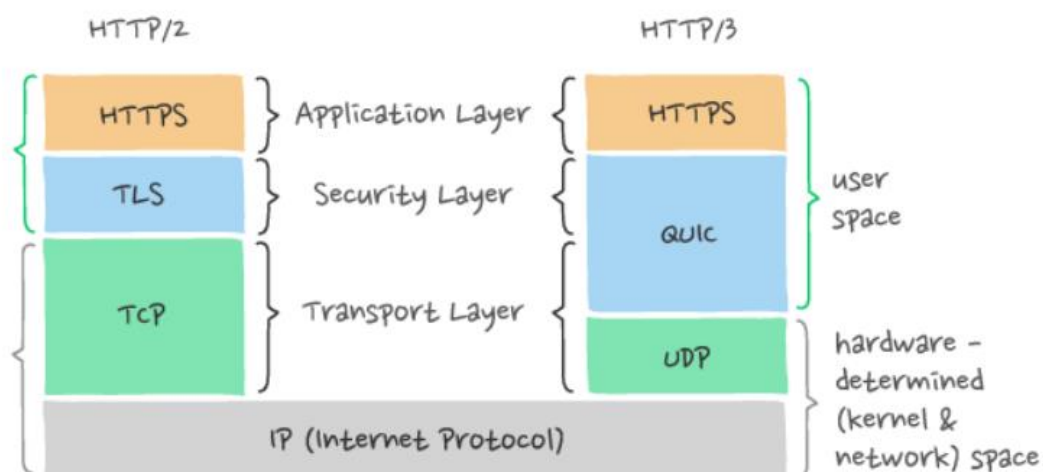
Εικόνα 9. Σύγκριση των TCP – UDP ως προς την παραγγελία μηνυμάτων

Επιπλέον, το QUIC έχει επανασχεδιάσει τον τρόπο με τον οποίο εκτελούνται οι χειραψίες μεταξύ πελάτη και διακομιστή, μειώνοντας τον χρόνο δημιουργίας σύνδεσης που σχετίζεται με τη δημιουργία επαναλαμβανόμενων συνδέσεων.



Εικόνα 10. Αριθμός μηνυμάτων στο πρώτο byte δεδομένων σε επαναλαμβανόμενη σύνδεση στα τρία πρωτόκολλα

Το HTTP/3 παρουσιάζει συντακτική και σημασιολογική ομοιότητα με το H2. Το HTTP/3 ακολουθεί την ίδια ακολουθία ανταλλαγής μηνυμάτων αιτήματος και απάντησης, με μια μορφή δεδομένων που περιέχει μεθόδους, κεφαλίδες, κωδικούς κατάστασης και σώμα. Ωστόσο, η σημαντική διαφορά του HTTP/3 έγκειται στα πρωτόκολλα πάνω από το UDP, όπως φαίνεται στο παρακάτω διάγραμμα.



Εικόνα 11. Ιεραρχία στοίβας των επιπέδων του H3

Πολυπλεξία: Το HTTP/3 «επικοινωνεί» μέσω ροών QUIC λόγω της απουσίας διακριτού μηχανισμού πολυπλεξίας. Μια δυνάδα αιτήματος – απόκρισης καταναλώνει μια ροή. Τα πλαίσια που χρησιμοποιούνται για την επικοινωνία ροής είναι αντίστοιχα με αυτά του

h2. Τα πλαίσια χωρίζονται σε πολλές κατηγορίες, όπως για παράδειγμα DATA, SETTINGS, HEADERS. Για τη μετάδοση πληροφοριών ελέγχου το HTTP/3 χρησιμοποιεί δύο ξεχωριστές μονοκατευθυντικές ροές QUIC. Δύο μονοκατευθυντικές ροές επιτρέπουν στα τερματικά να μεταδίδουν δεδομένα αμέσως μετά από μια σύνδεση 0-RTT ή 1-RTT

Συμπίεση Κεφαλίδας: Το HTTP/3 χρησιμοποιεί επίσης έναν νέο μηχανισμό συμπίεσης κεφαλίδων που ονομάζεται QPACK, ο οποίος είναι μια τροποποίηση του HPACK που χρησιμοποιείται στο HTTP/2. Αυτό οφείλεται στο ότι το HPACK εξαρτάται από τη διαδοχική παράδοση όλων των πλαισίων σε όλες τις ροές. Η χρήση του HPACK σε συνδυασμό με το HTTP/3 θα οδηγούσε αναπόφευκτα στο HoLB, καθώς το QUIC δεν παρέχει διαδοχική παράδοση μεταξύ των ροών, αλλά μέσα σε μια ροή. Το QPACK και το HPACK παρουσιάζουν κοινά σημεία όσον αφορά τους στόχους και τις αρχές, όπως η χρήση δυναμικού και στατικού πίνακα και μιας στατικής κωδικοποίησης Huffman. Ωστόσο το QPACK, χρησιμοποιεί διαφορετικούς μηχανισμούς για την επίτευξη των στόχων αυτών. Κάτω από το QPACK, οι κεφαλίδες HTTP μπορούν να φτάνουν εκτός σειράς σε διαφορετικές ροές QUIC. Σε αντίθεση με το HTTP/2, όπου το TCP διασφαλίζει την παράδοση πακέτων κατά παραγγελία, οι ροές QUIC παραδίδονται εκτός σειράς και μπορεί να περιέχουν διαφορετικές κεφαλίδες σε διαφορετικές ροές. Για να το αντιμετωπίσει αυτό, το QPACK χρησιμοποιεί έναν μηχανισμό πίνακα αναζήτησης για την κωδικοποίηση και την αποκωδικοποίηση των κεφαλίδων.

Βελτιστοποιημένη λειτουργία προώθησης διακομιστή: Η αυτή η οποία εισήχθη στο HTTP/2, μπορεί να θεωρηθεί ως πρόβλεψη ενός αιτήματος που δεν έχει υποβληθεί ακόμη από τον πελάτη. Αυτό εξακολουθεί να υπάρχει στο HTTP/3, αλλά η εφαρμογή του γίνεται μέσω διαφορετικών μηχανισμών και μπορεί να περιοριστεί. Παρόλο που οι ωθήσεις διακομιστή εξοικονομούν μισό ταξίδι μετ' επιστροφής, εξακολουθούν να καταλαμβάνουν εύρος ζώνης. Ένα πλαίσιο PUSH_PROMISE αποστέλλεται από τον διακομιστή μέσω της ροής αιτημάτων που δείχνει τι θα περιείχε ένα αίτημα στο οποίο μια ώθηση θα ήταν απάντηση. Στη συνέχεια στέλνει αυτήν την πραγματική απόκριση μέσω μιας νέας ροής.

Οι ωθήσεις διακομιστή μπορούν να περιοριστούν από τον πελάτη. Οι μεμονωμένες προωθημένες ροές μπορούν να ακυρωθούν με ένα CANCEL PUSH, ακόμα κι αν προηγουμένως θεωρηθεί αποδεκτό.

QUIC: Το πρωτόκολλο αυτό χρησιμοποιεί ροές για την πολυπλεξία δεδομένων. Η έννοια των ροών χρησιμεύει ως απτή αναπαράσταση για πρωτόκολλα εφαρμογών, όπως το HTTP/3, που λειτουργούν πάνω από το QUIC. Το QUIC χρησιμοποιεί πληροφορίες από το πρωτόκολλο εφαρμογής για να ιεραρχήσει τις ροές, καθώς δεν υπάρχει εγγενής μέθοδος για την κοινή χρήση προτεραιοτήτων. Χρησιμοποιούνται πολλαπλά πλαίσια για τη διαίρεση των ροών, όπως τα πλαίσια STREAM για τη μετάδοση δεδομένων, ή τα πλαίσια ACK για την αναγνώριση πακέτων. Το QUIC χρησιμοποιεί πακέτα QUIC, τα οποία περιλαμβάνουν διάφορα πλαίσια που προέρχονται από διαφορετικές ροές, με σκοπό τη μεταφορά δεδομένων. Τα πακέτα μεταδίδονται από διαγράμματα δεδομένων UDP, τα οποία δύναται να περιέχουν πολλαπλά πακέτα. Το πρωτόκολλο QUIC διευκολύνει τις χειραψίες 0-RTT και 1-RTT μέσω της ενσωμάτωσης κρυπτογραφικών πρωτοκόλλων, συγκεκριμένα του TLS 1.3, με χειραψίες μεταφοράς. Η σκοπιμότητα των χειραψιών 0-RTT εξαρτάται από την ύπαρξη προ υπάρχουσας σύνδεσης μεταξύ των τελικών σημείων. Από την άλλη πλευρά, η χειραψία 3-RTT χρησιμοποιείται από το HTTP/2 πάνω από TCP και TLS. Οι συνδέσεις QUIC είναι εξοπλισμένες με το Connect ID, επιτρέποντας έτσι στη σύνδεση να διατηρήσει τη σταθερότητά της ακόμη και σε περίπτωση τροποποιήσεων στην υποκείμενη IP. Το QUIC προσφέρει επιπλέον συμπληρωματικές λειτουργίες, όπως έλεγχο μεμονωμένης ροής και ροής σύνδεσης, διαδικασίες ανίχνευσης και ανάκτησης απωλειών και διάφορες άλλες δυνατότητες.

Το QUIC επίσης χειρίζεται πιο βέλτιστα τα σφάλματα. Προτείνει τη χρήση βελτιωμένου μηχανισμού ανάκτησης απωλειών και διόρθωσης σφαλμάτων προώθησης για την καλύτερη αντιμετώπιση λανθασμένων πακέτων, ειδικά με αποσπασματικά και αργά ασύρματα δίκτυα επιρρεπή σε υψηλά ποσοστά σφαλμάτων στη μετάδοση.

Περιορισμοί του HTTP/3: Η χρήση της CPU της εφαρμογής QUIC της Google είναι διπλάσια από αυτή του TCP/TLS. Η υψηλότερη χρήση της CPU δύναται να αποδοθεί στην κρυπτογραφία, την ανταλλαγή πακέτων UDP και τη διατήρηση της κατάστασης QUIC. Οι κρυπτογραφικές χειραψίες, συγκεκριμένα τα 0-RTT και 1-RTT, διευκολύνονται από το TLS 1.3. Η χρήση του τελευταίου σε συνδυασμό με το HTTP/2 μειώνει τα οφέλη του QUIC σε σύγκριση με το TCP/TLS.

2.3 Προηγούμενες μελέτες σχετικά με την υιοθέτησή τους σε μεγάλους παρόχους υπηρεσιών διαδικτύου

Λόγω της πρώιμης εισαγωγής του στο επιστημονικό κοινό, ο αριθμός των μελετών που έχει επικεντρωθεί στο HTTP/3 καθίσταται πράγματι περιορισμένος. Οι μελέτες που πραγματοποιήθηκαν από τους Saif et al [13] περιλαμβάνουν τον έλεγχο της πρόσβασης τόσο του πελάτη όσο και του διακομιστή σε μια μόνο ιστοσελίδα. Οι ερευνητές εξετάζουν την επίδραση της καθυστέρησης, της απώλειας πακέτων όπως και της απόδοσης, ωστόσο, δεν παρατηρούν καμία σημαντική επίπτωση όσον αφορά την απόδοση. Επιπλέον, στη μελέτη τους, οι Marx et al. [14] διεξήγαγαν μια ανάλυση κατά την οποία πραγματοποιήθηκε σύγκριση 15 εφαρμογών του HTTP/3, αποκαλύπτοντας έτσι σημαντικές πληροφορίες, λεπτομέρειες αλλά πιο σημαντικά, μια ετερογένεια όσον αφορά τους μηχανισμούς που χρησιμοποιούνται για τον έλεγχο της συμφόρησης, την σειρά προτεραιοτήτων και την ανάπτυξη πακέτων. Στη μελέτη τους πραγματοποίησαν αποκλειστικά και μόνο λήψεις μεμονωμένων αρχείων. Παρ' όλ' αυτά, τα αποτελέσματά τους απαιτούν πράγματι ολοκληρωμένες μετρήσεις με «πραγματικά» δεδομένα. Στη μελέτη [15], η οποία διεξήχθη από το «Cloudflare», η ομάδα του Cloudflare προέβη σε υλοποίηση ενός δικού τους προσχέδιου, συγκεκριμένα του 27 HTTP/3. Μετά τη σχετική αξιολόγηση, συμπέραναν ότι το συγκεκριμένο προσχέδιο, παρουσιάζει μείωση της απόδοσης σε σύγκριση με το HTTP/2. Πιο συγκεκριμένα, αποδείχθηκε 1 – 4% πιο αργό από το h2. Βέβαια, αξίζει να σημειωθεί, ότι οι ερευνητικές τους προσπάθειες περιορίζονται προς το παρόν στην πλατφόρμα της Cloudflare. Τέλος, η τεχνική ελέγχου για την προσαρμοστική ροή που έχει σχεδιαστεί ειδικά για το HTTP/3 προτάθηκε από τους Guillen et al στο [16]

Όσον αφορά το QUIC, όπως προαναφέραμε, εισήχθη από την Google το 2012 και έκτοτε έχει βρεθεί στο επίκεντρο πολυάριθμων μελετών. Αρχικά, οι Wolsing et al. στο [17] αποδεικνύουν ότι το QUIC ξεπερνά το TCP, και αυτό λόγω της γρήγορης εγκατάστασης σύνδεσής του. Επιπλέον, στη μελέτη τους, οι Manzoor et al, συμπεραίνουν ότι το QUIC παρουσιάζει κατώτερη απόδοση σε σύγκριση με το TCP σε δίκτυα ασύρματου πλέγματος, λόγω μη βέλτιστων αλληλεπιδράσεων μεταξύ του πρωτοκόλλου και του επιπέδου WIFI (στη συγκεκριμένη περίπτωση). Σύμφωνα με τους Carlucci et al. στο [18] το QUIC μειώνει τη συνολική διάρκεια ανάκτησης σελίδας. Παράλληλα, οι Kakhi et al στο [19], διεξήγαγαν μια εκτεταμένη μελέτη μέτρησης όσον αφορά το QUIC,

και συμπερασματικά διαπίστωσαν ότι ξεπερνά το TCP στην πλειονότητα των περιπτώσεων. Αν και αυτές οι μελέτες στην ουσία επικεντρώνονται μόνο στις εκδόσεις QUIC της Google, αξίζει να σημειωθεί ότι το τρέχον πρότυπο που προτείνεται στο IETF [20] έχει σημειώσει αξιοσημείωτη πρόοδο. Τέλος, οι συγγραφείς της μελέτης αυτής, οφείλουμε να σημειώσουμε, πως επικεντρώνονται κυρίως στο επίπεδο μεταφοράς, αγνοώντας έτσι τις εξελίξεις που επιφέρει το HTTP/3 σε ανώτερα επίπεδα.

Κεφάλαιο 3

Διείσδυση των HTTP/3 και QUIC σε μεγάλους ISPs

3.1 Ανάλυση των HTTP/3 και QUIC από τις Google, Cloudflare, Google

Όπως αναφέραμε, το HTTP/3 (H3) αποτελεί την τρίτη έκδοση του πρωτόκολλου HTTP, του οποίου η βάση έγκειται στο πρωτόκολλο QUIC, πρωτόκολλο που αναφέρθηκε στο «RFC 9000». Το τελευταίο, αποτελεί προϊόν της Google, με σκοπό την παροχή ασφάλειας και αξιοπιστίας όσον αφορά τη μεταφορά μέσω UDP. Παρόμοια με το TCP, το QUIC αποτελεί πρωτόκολλο με βασικό προσανατολισμό τη σύνδεση το οποίο διευκολύνει την επικοινωνία μεταξύ πελάτη και διακομιστή. Μια μεμονωμένη σύνδεση δύναται να αξιοποιηθεί από μια εφαρμογή με σκοπό την αποτελεσματική πολυπλεξία ροών ελεγχόμενης ροής χάρη στο πρωτόκολλο αυτό. Σε δεύτερο χρόνο, η «μετεγκατάσταση διαδρομής δικτύου» κρίνεται επίσης εφικτή δίχως διακοπή σύνδεσης. Σύμφωνα με την Google, το QUIC, κατάφερε την μείωση του «rebuffering» βίντεο κατά δεκαοκτώ τις εκατό για «επιτραπέζιους υπολογιστές» ενώ, παράλληλα κατάφερε αντιστοίχως τη μείωση της καθυστέρησης δημιουργίας σύνδεσης αναζήτησης κατά οκτώ τις εκατό [7]. Ένα ακόμη σημαντικό προτέρημα που εντοπίζουμε στο QUIC σε σύγκριση με το TCP έγκειται στην παροχή βελτιωμένης απόδοσης δικτύων, όταν σε αυτά παρουσιάζονται απώλειες πακέτων.

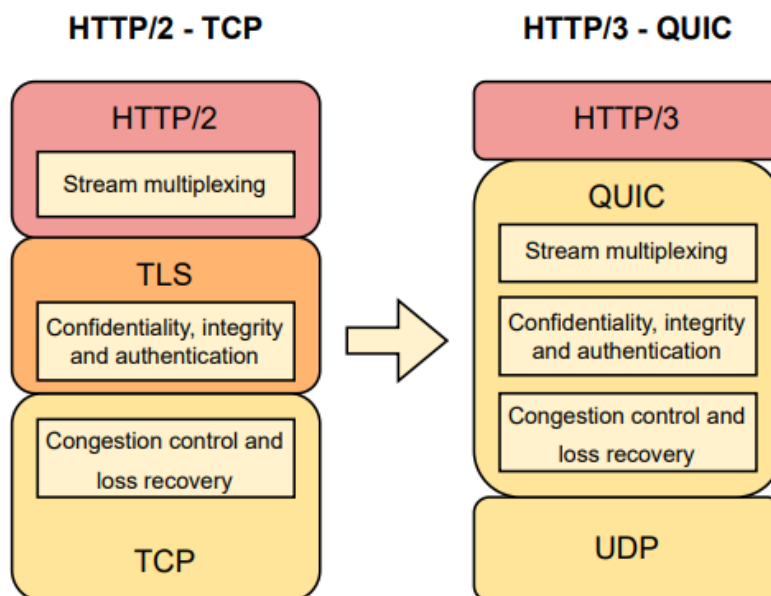
Παρατηρήθηκαν στο πέρασμα των χρόνων πολλές υλοποιήσεις του «QUIC2», οι οποίες μάλιστα παρουσίασαν ασυμβατότητα, με ανόμοια σετ χαρακτηριστικών, τα οποία υπόκεινται σε εξέταση και σύγκριση όσον αφορά την αξιολόγηση της

διαλειτουργικότητας τους. Από την άλλη, με την σχετικά τωρινή δημοσίευση του RFC, αναμένεται ότι η πληθώρα, ίσως και η ολότητα των σημαντικών βάσεων κωδικών θα στραφούν προς το «απλό» QUIC. Καθώς το H3 βασίζεται στο QUIC, αυτό σημαίνει ότι εκμαιεύει σημαντικό ποσοστό των δυνατοτήτων του. Η διαμόρφωση σύνδεσης μηδενικού χρόνου μετ'επιστροφής αποτελεί ένα μία από αυτές τις δυνατότητες. Το H3 αξιοποιεί το TLS 1.3, το οποίο είναι άμεσα ενσωματωμένο στο QUIC, με σκοπό την εξοικονόμηση ενός τουλάχιστον RTT για τη ρύθμιση σύνδεσης, ενώ το H2 σπαταλά μερικά «RTT για την τριπλή χειραψία» λόγω του πρωτοκόλλου TCP. Λόγω της παρουσίας του QUIC επίσης, το H3 δεν «απασχολείται» από αντίστοιχα ζητήματα HoL, τα οποία σχετίζονται με το TCP. Τοποθετώντας κάθε ζεύγος αιτημάτων και απαντήσεων HTTP στη δική του ροή, η πολυπλεξία ροής επιτρέπει την ταυτόχρονη επεξεργασία πολλαπλών αιτημάτων. Μια αυτόνομη ακολουθία παράδοσης δεδομένων μεταξύ του πελάτη και του διακομιστή ονομάζεται ροή.

Ένα μόνο αίτημα «HTTP GET» δύναται να αξιοποιηθεί από το μέλος – πελάτη (Π) για να αιτηθεί πάνω από μία απάντηση από το μέλος – διακομιστή (Δ), χάρη στη δυνατότητα ώθησης του τελευταίου. Αυτό, απαντάται ιδιαίτερα σε περιπτώσεις κατά τις οποίες το μέλος (β) γνωρίζει ότι το μέλος (α) χρειάζεται τις παραπάνω απαντήσεις για να επεξεργαστεί πλήρως ένα σχετικό αίτημα. Λόγω αυτού, είναι εφικτή η αποθήκευση πολλών RTT, σε αντίθεση με το H1 «δίχως διοχέτευση» κατά το οποίο ένα νέο αίτημα εκδίδεται μόνο υπό τη προϋπόθεση ότι το προηγούμενο ιεραρχικά έχει απαντηθεί πλήρως (Βλέπε περίπτωση (α) της εικόνας παρακάτω). Το H1 καθιστά εφικτή την αποστολή πολλαπλών αιτημάτων μέσω μιας και μόνο μιας σύνδεσης TCP, χωρίς να είναι αναγκαία η λήψη κάθε απάντησης (βλέπε περίπτωση β). Βέβαια, για να ληφθούν οι ίδιες απαντήσεις με το HTTP/2 και HTTP/3 απαιτούνται περισσότερα αιτήματα. Η λειτουργία προτεραιότητας ροής δίνει στον (Π) τη δυνατότητα επιλογής ανάμεσα στο σύνολο των διαθέσιμων ροών σε μια μόνο σύνδεση. Στην περίπτωση κατά την οποία η προτεραιότητα ροής παραμένει απροσδιόριστη, οι ροές «διαχωρίζουν» την διεκπεραίωση της σύνδεσης σε ίσα κομμάτια, ομοιόμορφα. Η λειτουργία αυτή απαντάται και στην έκδοση 2 και στην 3 του HTTP πρωτοκόλλου. Ωστόσο, η λειτουργία προτεραιότητας ροής της δεύτερης έκδοσης αναφέρεται στο «RFC 7450» ως πιο περίπλοκη ως προς τον σχεδιασμό της, σε σύγκριση με την Τρίτη έκδοση [35]. Μια επεκτάσιμη μέθοδος προτεραιότητας βρίσκεται αυτό τον καιρό υπό ανάπτυξη από την «IETF HTTP», η εφαρμογή της οποίας εκτελείται

στο HTTP/3, ενώ παράλληλα, υπάρχει στο προσκήνιο η πιθανότητα υιοθέτησής της και από το HTTP/2 μέσω αναθεώρησης [36].

Η σύμπραξη των HTTP και QUIC κρίνεται σημαντικά ωφέλιμη, ιδίως για το πρωτόκολλο HTTP. Αρχικά, ο έλεγχος ροής ανά ροή στο επίπεδο μεταφοράς, όπως και ο έλεγχος συμφόρησης στη σύνδεση ενσωματώνονται από το QUIC. Σε λογική HTTP πλαισίου αυτό κρίνει εφικτή την ικανότητα εκκίνησης αιτημάτων πολυπλεξίας σε μια σύνδεση, κάνοντας έτσι δυνατή την ομοιόμορφη λειτουργία όσον αφορά τον έλεγχο συμφόρησης σε όλα. Αυτό έχει ως αποτέλεσμα τη μετάβαση στο νέο επίπεδο H3-QUIC, όπως βλέπουμε και στην παρακάτω εικόνα. Η εφαρμογή του QUIC στο H3 συνοδεύεται από αξιοπιστία, έλεγχο ταυτότητας ομότιμων, πολλαπλή ροή και σιγουριά όσον αφορά το πληροφοριακό απόρρητο.



Εικόνα 12

Η γενική διαδικασία που απαντάται στη διαδικασία πελάτη – διακομιστή H3 αναφέρεται επιγραμματικά παρακάτω:

- I) Μια σύνδεση QUIC δημιουργείται από τον πελάτη H3, η οποία ακολουθείται από «διαπραγμάτευση πρωτόκολλου, πολυπλεξία βάσει ροής και έλεγχο ροής»
- II) Μια μεμονωμένη σύνδεση QUIC, δύναται να χειριστεί διαφορετικά αιτήματα HTTP από τον πελάτη H3. Για να αποφευχθεί το HOL, κάθε δυάδα αιτήματος και απάντησης ταξιδεύει σε ξεχωριστή ροή QUIC.

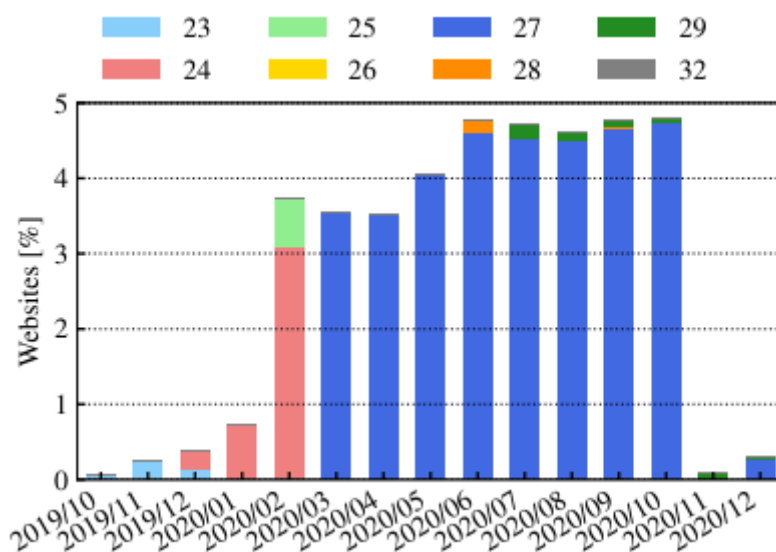
III) Το αίτημα πελάτη κρίνεται μη αναγκαίο για την παροχή αντικειμένων HTTP από τον διακομιστή H3, λόγω της ύπαρξης του «push διακομιστή»

IV) QPACK αποτελεί ωφέλιμη δυνατότητα όσον αφορά τα τελικά σημεία H3

3.2 Στατιστικά στοιχεία και δεδομένα σχετικά με τη χρήση τους στους εν λόγω ISPs

Στο έργο τους [11], οι Martino Trevisan et al, πραγματοποίησαν μια έρευνα αναλύοντας και συγκρίνοντας μεγάλους ISPs που υιοθέτησαν το H3. Εκμεταλλευόμενοι το σετ «HTTP Archive», παρατήρησαν ότι το H3 απέκτησε μεγαλύτερη αξιοπιστία ως προς την υιοθέτησή τους κατά τους τελευταίους μήνες 2019 και έτσι, παρατηρήθηκε αύξηση του αριθμού των ιστοτόπων που χρησιμοποιούν το συγκεκριμένο πρωτόκολλο

(βλέπε Εικόνα 13)

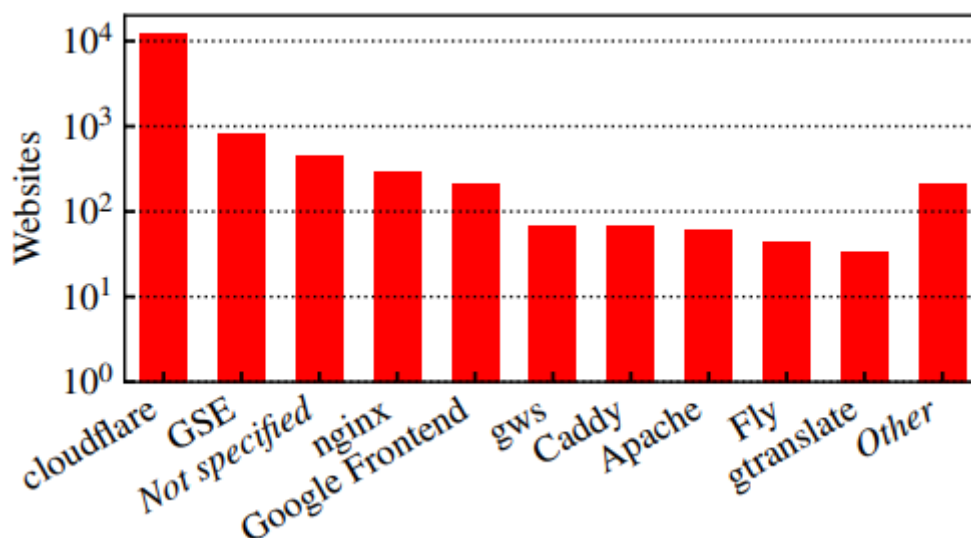


Εικόνα 13. Ποσοστιαία μέτρηση πλατφόρμων στο «HTTPArchive» που ενσωματώνουν το H3

Παρατηρήθηκε μια σταδιακή αύξηση κατά τη διάρκεια των 4 πρώτων μηνών όσον αφορά το ποσοστό των ιστοτόπων που υποστηρίζουν H3, η οποία έφτασε το 0,7% όλων των ιστοτόπων. Οι δύο ISPs που προσφέρουν σε αυτή την περίοδο H3 είναι οι «Google – Facebook». Τον 2ο μήνα του 2020 ο αριθμός αυτός εκτοξεύτηκε στα ύψη. Βασικός καταλύτης για την «εκτόξευση» αυτήν αποτελεί το Cloudflare το οποίο ενσωμάτωσε το

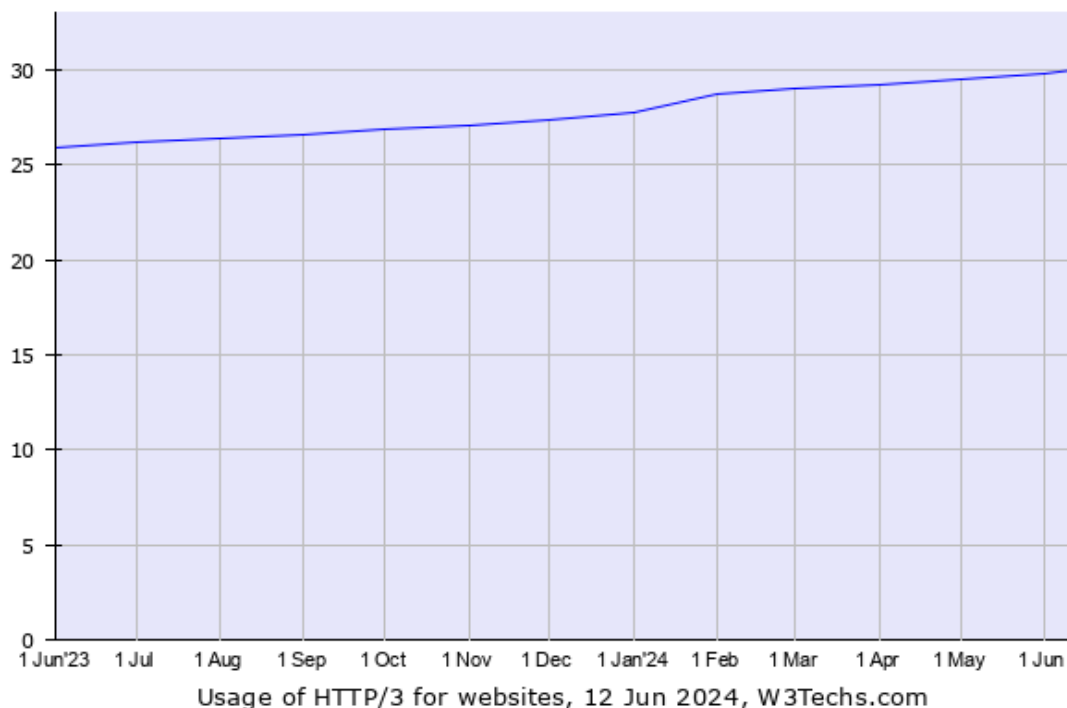
H3 στην πλειοψηφία των ιστοτόπων του. Σε αυτή τη φάση, το ποσοστό είναι μεγαλύτερο από 4% ενώ τον 10^ο μήνα του ίδιου χρόνου φτάνει στο ζενίθ του, δηλαδή στο 4.8% του συνόλου των ιστότοπων. Τον επόμενο μήνα, το ποσοστό εμφάνιση ξαφνική πτώση σε λιγότερο από 0.1% καθώς το Cloudflare, σταμάτησε τη «σύμπραξη» με το H3, με γνώμονα την επίλυση λειτουργικών προβλημάτων. Ένα μήνα μετά αυτός ο ISPs ενσωμάτωσε πάλι το H3 ωστόσο σε συγκεκριμένους μόνο ιστότοπους (14.707 στο σύνολο).

Μεγάλα ονόματα επιχειρήσεων που φιλοξενούν ιστότοπους οι οποίοι είναι μάλιστα συμβατοί με τα πρωτόκολλα H3 και QUIC διαθέτουν το δικό τους λογισμικό διακομιστή. Στην εικόνα παρακάτω, παρέχεται μια αριθμητική ανάλυση σχεδόν 15 χιλιάδων ιστοτόπων, η οποία δείχνει τα δέκα πιο γνωστά λογισμικά διακομιστών. Η πλειοψηφία των συμβατών με το H3 ιστοτόπων φιλοξενούνται από το Cloudflare. Έπειτα, η Google κατατάσσεται δεύτερη με τα «Google Web Server, Google Frontend, Google Web Server». Όπως φαίνεται από τους οκτακόσιους εννιά ιστότοπους που χρησιμοποιούν την Blogspoit, η GSE αναπτύσσεται ουσιαστικά εκεί. Δεν βρέθηκε κάποιο στοιχείο διακομιστή στις απαντήσεις HTTP για πεντακόσιους εβδομήντα πέντε ιστότοπους, ενώ μετέπειτα διαπιστώνεται ότι τετρακόσιοι σαράντα πέντε από αυτούς αποτελούν κτήμα του Facebook. Το υπόλοιπο των ιστότοπων τροφοδοτούνται α) από γνωστούς διακομιστές ανοιχτού κώδικα, εκ των οποίων «Apache», και β) αντίστοιχους ασυνήθιστους HTTP όπως «Caddy» που υποστηρίζουν τα H2 και H1.



Εικόνα 14

Στο [41] μπορούμε να δούμε ακόμη πιο πρόσφατα στοιχεία αναφορικά με την καταμέτρηση της ποσοστιαίας δικτυακής κίνησης - HTTP». Πιο συγκεκριμένα, σύμφωνα με μέτρηση η οποία πραγματοποιήθηκε τον Αύγουστο του 2023, σχεδόν το 27% της κίνησης αυτής ήδη αξιοποιεί το H3. Ανάμεσα στους ιστότοπους που αξιοποιούν ή υποστηρίζουν το πρωτόκολλο H3, οι πιο δημοφιλείς αποτελούν το Youtube, το Google, το Netflix, το Instagram, το Mozilla, κτλ. Αξίζει να σημειωθεί, πως σύμφωνα με την έρευνα, προβλέπεται ότι ο αριθμός των ιστότοπων που θα χρησιμοποιούν μελλοντικά το H3, σίγουρα θα αυξηθεί, πράγμα που βασίζεται στην παράλληλη αύξηση της ποσοστιαίας κίνησης του πρωτόκολλου H3. Τέλος, σχεδόν όλα τα προγράμματα περιήγησης υποστηρίζουν πλέον το H3



Εικόνα 15. Χρήση του H3 κατά την περίοδο 2023 – 2024

Κεφάλαιο 4

Εστίαση στο Youtube

4.1 Λεπτομερής εξέταση του τρόπου με τον οποίο το YouTube χρησιμοποιεί τα HTTP/3 και QUIC

Το Youtube αξιοποιεί το DASH μέσω HTTP. Το πρωτόκολλο αυτό αφορά ένα πρότυπο ροής που επιτρέπει τη ροή πολυμέσων από την πλευρά του πελάτη, κατά το οποίο ο διαδικτυακός ρυθμός μετάδοσης προσαρμόζεται με γνώμονα τους περιορισμούς Δικτύου του πελάτη. Το πολυμέσο προερχόμενο από τον διακομιστή ιστού HTTP χωρίζεται σε επιμέρους κομμάτια, τα οποία στη συνέχεια υποβάλλονται σε ανάλυση και κάθε αντίστοιχο κομμάτι εκμεινεί τη δική του κωδικοποίηση με ξεχωριστό ρυθμό μετάδοσης. Ανάλογα με την κατάσταση του δικτύου, τα κομμάτια αυτά μεταμορφώνονται και δεσμεύονται στο buffer του δέκτη. Δεδομένου ότι το DASH αφορά ένα πρότυπο, κάθε λογισμικό ροής πολυμέσων δύναται να κατέχει κάποια αντίστοιχη κάθε φορά εφαρμογή του.

Τα HTTP Request και Response περιέχουν ενσωματωμένες παραμέτρους DASH, ενώ παράλληλα, το πρότυπο αυτό λειτουργεί πάνω από το H3. Ανάλογα την κατάσταση του δικτύου, ο ρυθμός μετάδοσης των bit προσδιορίζεται από έναν πελάτη DASH, πράγμα που γίνεται μέσω μιας τεχνολογίας προσαρμογής του ρυθμού. Παρόλο που διάφορες μελέτες έχουν επιχειρήσει την «μετάλλαξη» του ABR στο Youtube σε έναν πιο ωφέλιμο αλγόριθμο, θα πρέπει να σημειωθεί, ότι το Youtube αξιοποιεί τη δική του ιδιόκτητη μέθοδο προσαρμογής ρυθμού. Με το που προσδιοριστεί αυτός ο ρυθμός αναπαραγωγής, ο πελάτης προτύπου με βάση το buffer κάνει αίτημα για το επόμενο κομμάτι πολυμέσου χρησιμοποιώντας ένα HTTP – REQUEST το οποίο πραγματοποιεί ενσωμάτωση των πληροφοριών του κομματιού και τα απαραίτητα δεδομένα ρυθμού bit. Ύστερα οι πληροφορίες κομματιού στέλνονται με τη βοήθεια ενός HTTP – RESPONSE

4.2 Στρατηγικές ενσωμάτωσης

Λόγω της συνεχόμενης αύξησης της «κατανάλωσης» πολυμέσων στο YOUTUBE, την οποία «συντροφεύει» μια αντίστοιχη ανάγκη για βέλτιστη ποιότητα, η τεχνολογία ABR αποτελεί μία από τις πιο σημαντικές στρατηγικές στο QUIC-H3. Η τεχνολογία αυτή έχει ως σκοπό την βελτιστοποίηση της επιλογής του «bitrate» και του QoE, παίρνοντας υπόψιν τις εκάστοτε δικτυακές συνθήκες. Για τον σκοπό αυτό, δημιουργήθηκαν αρκετές τεχνολογίες ABR, εκ των οποίων σχεδιάστηκαν αρκετοί αλγόριθμοι ABR με στόχο την παροχή υψηλότερης ποιότητας βίντεο και την ελαχιστοποίηση των πάγκων:

A) «**Απόδοση**»: Το εύρος ζώνης υπολογίζεται μέσω της αξιοποίησης ενός «συρόμενου παραθύρου», ή αλλιώς της τιμής EWMA. Η επιλογή του bitrate τελείται με γνώμονα το εύρος ζώνης ανά περίπτωση.

B) «**BOLA**»: Πρόκειται για μια τεχνική με buffer και αξιοποιεί την τεχνική βελτιστοποίησης «Lyapunov». Εδώ, τελείται η ανάπτυξη ενός δευτερεύοντος προγράμματος με στόχο να παραχθεί α) ένα ναδίρ «rebuffering» και ένα ζενίθ «μέσου bitrate».

Γ) «**Δυναμικό ABR**»: Εδώ χρησιμοποιείται μια τεχνολογία που συνδυάζει την τεχνολογία A) και μια τεχνολογία buffer με στόχο να επιλεχθεί το «bitrate». Εδώ υπάρχουν δυο περιπτώσεις : (α) περίπτωση χαμηλών επιπέδων buffer(εκκίνηση/αναζήτηση) και β) περίπτωση υψηλών (σταθερότητα). Στην περίπτωση (α), γίνεται επιλογή να εκτελεστεί ο αλγόριθμος A) που αναλύσαμε πιο πάνω ενώ στην περίπτωση (β) γίνεται αλλαγή στον αλγόριθμο B).

Δ) **L2A**: Αφορά τεχνολογία μικρής καθυστέρησης στην οποία παίρνει μέρος η τεχνική «Online Convex Optimization». Αξιοποιούνται «ιστορικές τιμές» για να επιλεχθεί το «bitrate».

E) «**LoL**»: Η τεχνολογία αυτή αξιοποιεί τον αλγόριθμο τεχνητής νοημοσύνης «SOM». Πραγματοποιείται εκχώρηση βαρών στη μονάδα SOM. Τα μετρικά που συνυπολογίζονται με στόχο την εύρεση του βέλτιστου bitrate είναι «η απόδοση, το διάνυμα βάρους, το QoE, και η ταχύτητα αναπαραγωγής».

4.3 Επιπτώσεις στη συνολική απόδοση και την εμπειρία του χρήστη του Youtube

Στο έργο τους, οι «Tanya Shreedhar et al», διεξήγαγαν μία έρευνα σχετικά με την ενσωμάτωση του QUIC και H3 στην πλατφόρμα του Youtube και την ανάλυση αυτής, σε πολλά επίπεδα, εκ των οποίων και αυτό της απόδοσής τους.

A) Καθυστέρηση εκκίνησης: Αναφέρεται στη μέτρηση χρονικό διαστήματος από το στάδιο αιτήματος έως και την εκκίνηση αναπαραγωγής του βίντεο. Σε αυτό το επίπεδο συμπεριλαμβάνονται οι αναλύσεις των «DNS και χρονικά διαστήματα χειραγίας. Βρέθηκε μετά από μετρήσεις πως η απώλεια και η καθυστέρηση εκκίνησης είναι ποσά ανάλογα. Με άλλα λόγια, όσο μεγαλύτερη είναι η απώλεια σε ένα δίκτυο, η καθυστέρηση εκκίνησης αντίστοιχα αυξάνεται. Σε περιπτώσεις με μηδενικές απώλειες, η επίδοση του QUIC-H3 στο YOUTUBE κρίνεται παρόμοια με την αντίστοιχη προηγούμενων πρωτόκολλων. Από την άλλη, στην περίπτωση που έχουμε απώλειες πακέτων το QUIC-H3 ξεπερνά κατά πολύ τους «προγόνους του» Συγκεκριμένα, οι ερευνητές βρήκαν ότι για απώλεια ποσοστού πέντε τις εκατό το TLS/TCP είναι 60% πιο αργό από το QUIC-H3 στην εκκίνηση του βίντεο. Για απώλεια διπλή από την προηγούμενη, το TLS/TCP είναι κατά 0,94 ms πιο αργό. Αυτή η συμπεριφορά του QUIC σε περιπτώσεις με απώλεια πακέτων οφείλεται α) στους υψηλότερους χρόνους σύνδεσης του TLS/TCP, β) στους χειρότερους μηχανισμούς ανάκτησης απωλειών αυτού.

B) Ποσοστό και Διάρκεια Διακοπής: Η διακοπή τελείται στην περίπτωση της μη λήψης ενός καρέ ακριβώς πριν το «playout». Το χρονικό διάστημα που «συμβαίνει» η διακοπή, έχουμε αντίστοιχη διακοπή στην αναπαραγωγή του βίντεο με το buffer να σημειώνει 0s. Σε περιπτώσεις πολλών απωλειών πακέτων, παρατηρείται αντίστοιχα μεγαλύτερος αριθμός διακοπών. Όσον αφορά τη διάρκεια μια τέτοια διακοπής, παρατηρήθηκε ότι σε απώλεια δέκα τις εκατό το QUIC-H3 παρουσιάζει μικρότερη διάρκεια σε σύγκριση με τα προγενέστερα πρωτόκολλα. Αυτό σημαίνει φυσικά, ότι το QUIC-H3 προσφέρει εν γένει, μια πιο βέλτιστη QoE, παρόλο που το TLS/TCP κρίνεται καλύτερο αποδοτικά. Όταν έχουμε να κάνουμε με μεγάλα ποσοστά απώλειας, η παραπάνω συμπεριφορά εντείνεται.

Γ) «Διακοπή Καλής Ποιότητας» Παρατηρήθηκε αντιστοιχία, αναφορικά με την απώλεια, τη διακοπή και την καλή ποιότητα των βίντεο. Όπως θα έχει παρατηρήσει και ένας μέσος χρήστης της πλατφόρμας YOUTUBE, όσο αυξάνονται τα «απολεσθέντα» πακέτα, τόσο

αυξάνεται όπως είπαμε και στο Β) πιο πάνω το ποσοστό και η διάρκεια διακοπής, και με τη σειρά του τόσο αυξάνονται τα συμβάντα διακοπής καλής ποιότητας. Σε περιπτώσεις με μεγάλη απώλεια, το QUIC-H3 παρουσιάζει περισσότερες διακοπές όσον αφορά την ποιότητα. Αντίθετα, σε περιπτώσεις με μικρή έως και καθόλου απώλεια, απαντώνται οι ποιότητες βίντεο 720p και 480p. Εδώ επίσης αξίζει να σημειωθεί πως το QoE διατηρείται βέλτιστο, με αποτέλεσμα η ανάλυση να αναβαθμίζεται στο βέλτιστο δυνατό και οι διακοπές να παραμένουν όσο γίνεται λιγότερες. Για απώλειες από πέντε έως δέκα τις εκατό η χειρίστη ποιότητα αντιστοιχεί στα 144p. Με την αύξηση της απώλειας πακέτων, η αλλαγή από καλή σε κακή ποιότητα γίνεται αντιστοίχως πιο συχνή, γεγονός που δεν έγκειται στο πρωτόκολλο μεταφοράς καθαυτό. Έχοντας αυτό υπόψιν, συμπερασματικά αποδεικνύεται πως το QUIC-H3 σημειώνει πιο βέλτιστη QoE σε σύγκριση με άλλα πρωτόκολλα, πράγμα που οφείλεται στον μικρότερο αριθμό της μέσης διάρκειας διακοπής. Αυτό δύναται να οφείλεται στους καλύτερους «μηχανισμούς ανάκτησης» και σε προσέγγισης όπως το «F-RTO, TCP-RACK».

Κεφάλαιο 5

Συγκριτική ανάλυση της QoE

5.1 Ανασκόπηση των υφιστάμενων μελετών σχετικά με το QoE των χρηστών του YouTube με το HTTP/3 και το QUIC

Περίπου το 85% της συνολικής διαδικτυακής κίνησης συνιστά αναπαραγωγή βίντεο [40]. Μεγάλοι ISPs αναζητούν συνεχώς νέες μεθόδους, πιο αξιόπιστες τεχνολογίες που θα οδηγήσουν σε ενεργή βελτίωση της λεγόμενης «Ποιότητας Εμπειρίας Χρηστών» (PEX – QoE). Στην τρέχουσα ενότητα, ακολουθεί μια βιβλιογραφική ανασκόπηση αντίστοιχων ερευνητικών μελετών.

Έχουν πραγματοποιηθεί αρκετές μελέτες κατά τις οποίες η PEX αξιολογείται σε ένα περιβάλλον με συγκεκριμένες μεταβλητές και μια ποικιλία δικτυακών καταστάσεων. Αρχικά στο [8] οι μελετητές πραγματοποίησαν μια σύγκριση όσον αφορά την εμπειρία χρήστη, μέσω της εφαρμογής διαφορετικών αλγοριθμικών τεχνολογιών «DASH», με τη βοήθεια του «Amazon EC2». Στο [24] οι μελετητές αξιολογούν το QoE με γνώμονα δύο

μεταβλητών, εκ των οποίων το bitrate και τα συμβάντα διακοπής καλής ποιότητας κατά τη διάρκεια ενός βίντεο. Στα έργα [1] και [2] οι μελετητές τελούν μια συγκριτική μέτρηση TCP – QUIC της ποιότητας και των διακοπών που λαμβάνουν μέρος κατά τα βίντεο, ωστόσο, παρά της μετρήσεις αυτές, τα ευρήματα δεν κρίνονται αρκετά ώστε να προταθούν συγκεκριμένα μέτρα για τη βελτίωση της PEX για τα βίντεο QUIC. Στο [9] συμπεραίνεται πως το QUIC δεν είναι αρκετά ευαίσθητο ως προς τη μεταβλητότητα που απαρτίζει το δικτυακό εύρος ζώνης. Στο [25], τελείται η αξιολόγηση του πρωτοκόλλου QUIC μέσω της αξιοποίησης του ιστοτόπου «MONROE». Μετά από δοκιμές, οι συγγραφείς καταλήγουν στο συμπέρασμα ότι η συνεισφορά του πρωτοκόλλου στη γενική ποιότητα εμπειρία χρήστη δεν κρίνεται μεγάλης σημασίας. Στο [26] πραγματοποιήθηκε μια συγκριτική μελέτη μεταξύ των QUIC και TCP με σκοπό την ποιοτική αξιολόγηση της απόδοσής τους από τη μεριά του χρήστη. Και εδώ, οι διαφορές όσον αφορά την υποκειμενική άποψη περί της ποιότητας από τη μεριά του χρήστη, δεν έγιναν αντιληπτές. Στο [3] οι συγγραφείς προβήκαν στη δημιουργία τεχνικών «παθητικής και ενεργητικής παρακολούθησης». Οι πληροφορίες που συλλέχθηκαν αφορούσαν τα επίπεδα εφαρμογής και δικτύου, εκ των οποίων το «εύρος ζώνης, δικτυακή απώλεια, διακοπή, και buffer». Για τα δύο αυτά επίπεδα, εισήχθη μια μέθοδος αξιολόγησης, η «VQI» με στόχο την ενιαία αξιολόγηση της PEX. Η μέθοδος αυτή, κατάφερε την ακριβή μέτρηση της PEX για τα πρωτόκολλα HTTP και QUIC. Στο [19] οι συγγραφείς τέλεσαν μια συγκριτική μελέτη της συνεισφοράς των TCP – QUIC στη βελτίωση της PEX. Οι μετρικές που χρησιμοποιήθηκαν αφορούσαν το χρόνο φόρτωσης και τη ροή YOUTUBE. Τα πορίσματα που βγήκαν από αυτή τη μελέτη ήταν ι) η απόδοση του QUIC όσον αφορά την PEX κρίνεται σχεδόν εξ ολοκλήρου καλύτερη από αυτήν του TCP, κυρίως λόγω της εγκατεστημένης 0-RTT και της δυνατότητας γοργής επαναφοράς απωλειών. ιι) Σε περιπτώσεις με μεταβλητό εύρος ζώνης, το TCP κρίνεται πιο τελέσφορο λόγω της δυνατότητας εξάλειψης του «ACK», ιιι) μια γενική παρατήρηση είναι ότι από τη μία, το QUIC λειτουργεί σχεδόν το ίδιο αποδοτικά με το TCP, και από την άλλη λειτουργεί πιο βέλτιστα όταν εφαρμόζεται σε ροή καλής ανάλυσης.

5.2 Μετρικές που χρησιμοποιούνται για την αξιολόγηση της QoE

Μετρικές εκ των οποίων η καθυστέρηση έναρξης, το buffer, η καλή/καλή ποιότητα κρίνονται μεγάλης σημαντικότητας όσον αφορά την «καθήλωση» των χρηστών. Σε προηγούμενες μελέτες, αναλύθηκε πως η πιθανότητα καθυστερημένης έναρξης ενός βίντεο στο Youtube, είναι αντιστοίχως ανάλογη με την πιθανότητα αλλαγής βίντεο, ή ακόμη και πλατφόρμας από την πλευρά των χρηστών. Το ίδιο ισχύει και στα συμβάντα (συχνής και μη) διακοπής ροής. Συνεπώς, κρίνεται πολύ σημαντική η παρακολούθηση αντίστοιχων μετρικών ΠΕΧ, από την πλευρά των δημιουργών αλλά και των δικτυακών χειριστών, με στόχο την βελτιστοποίηση της σχέσης μεταξύ χρηστών και youtube. Παρακάτω, παραθέτουμε, τις πιο σημαντικές μετρικές που χρησιμοποιούνται για την αξιολόγηση της ΠΕΧ.

- Μέσο Bitrate: Αρχικά υπολογίζεται αθροίζοντας το μονό bitrate των «κομματιών» του βίντεο . Το άθροισμα αυτό στη συνέχεια διαιρείται με το σύνολο όλων των κομματιών. Η μετρική αυτή αντανakλά την καλή ή κακή ποιότητα του μεταδιδόμενου βίντεο. Στην περίπτωση αφθονίας του εύρους ζώνης και πληρότητας του buffer, ο ABR αιτείται ένα κομμάτι υψηλού bitrate. Αυτό σημαίνει βίντεο πολύ καλής ποιότητας
- Αριθμός Διακοπών του Bitrate: Ο υπολογισμός γίνεται με γνώμονα μη όμοια bitrate τα οποία ακολουθούνται από αντίστοιχες δικτυακές καταστάσεις. Η μη μεταβλητή ποιότητα συνιστά χαμηλή τιμή του αριθμού αυτού. Στην περίπτωση χαμηλού εύρους ζώνης ή εξάντλησης του buffer, γίνεται αίτημα από την πλευρά του πελάτη για χαμηλό bitrate, με σκοπό την αποτροπή της διακοπής ροής. Η μεταβλητότητα του bitrate σίγουρα κρίνεται επιβλαβής για το ΠΕΧ.
- Μέση Απόδοση: Ο υπολογισμός αυτής της μετρικής με τη μέση τιμή της απόδοσης μεμονωμένων κομματιών . Ο υπολογισμός γίνεται καθ' όλη τη διάρκεια της ροής.
- Μέση πληρότητα του Buffer.

5.3 Βασικά ευρήματα και τάσεις όσον αφορά τον αντίκτυπο στους χρόνους φόρτωσης βίντεο, τη ρυθμιστική μνήμη και τη συνολική ικανοποίηση των χρηστών

- Το H3 – QUIC καταφέρνει έναν βέλτιστο μέσο bitrate, όταν η λειτουργία της αλγοριθμικής τεχνολογίας L2A τελείται σε εύρος ζώνης 100MBPS. Το LoL+ καταφέρει το βέλτιστο μέσο bitrate, όταν η λειτουργία του τελείται βάσει σεναρίου απώλειας πακέτων 2% του δικτύου και εύρους ζώνης 100MBPS.
- Σε κατάσταση εύρους ζώνης 100MBPS, το L2A παρουσιάζει διακοπές ελάχιστου bitrate. Σε κατάσταση εύρους ζώνης 100MBPS, δικτυακής απώλειας πακέτων 2% και κατάσταση εύρους ζώνης 100MBPS, δικτυακής απώλειας πακέτων 2% και καθυστέρηση του βαθμού των δύο χιλιά δευτερολέπτων, το L2A παρουσιάζει τον μικρότερο αριθμό διακοπών του bitrate. Σε όλες τις δικτυακές καταστάσεις, ο αλγόριθμος αυτός παρουσιάζει τη λιγότερη μεταβλητότητα όσον αφορά την ποιότητα.
- Η μέγιστη απόδοση απαντάται σε σενάρια 100MBPS μέσω των L2A και Throughput. Σε κατάσταση εύρους ζώνης 100MBPS, δικτυακής απώλειας πακέτων 2% η βέλτιστη μέση απόδοση επιτυγχάνεται με τα LoL και L2A. Εν γένει, οι αλγοριθμικές τεχνολογίες που επιδεικνύουν χαμηλά ποσοστά καθυστέρησης επιφέρουν βέλτιστο μέσο όρο απόδοσης.
- Σε κατάσταση οριακής εξάντλησης του buffer, η πιθανότητα διακοπής αυξάνεται. Αντίθετα, σε κατάσταση πλήρους buffer, ο bitrate δύναται να αυξηθεί κατά πολύ. Σε κατάσταση εύρους ζώνης 100MBPS, οι BOLA και Throughput καταφέρνουν το βέλτιστο buffer ως προς την πληρότητά του. Σε κατάσταση εύρους ζώνης 100MBPS και δικτυακής απώλειας πακέτων 2%, ο Throughput καταφέρει τον μεγαλύτερο μέσο όρο πλήρους buffer. Σε κατάσταση εύρους ζώνης 100MBPS, δικτυακής απώλειας πακέτων 2% και κατάσταση εύρους ζώνης 100MBPS, το μέγιστο του μέσου όρου του πλήρους buffer επιτυγχάνεται από τον BOLA.

ΚΕΦΑΛΑΙΟ 6

Εκτέλεση πειραμάτων

6.1 Μεθοδολογία

Προκειμένου να μελετηθεί η επίδραση του HTTP3 στο Youtube Video Streaming, πραγματοποιήθηκαν μετρήσεις με χρήση ενός Ubuntu 22.04.4 LTS Workstation που έχει εγκατασταθεί σε εικονική μηχανή που εκτελείται σε εξυπηρετητή που βρίσκεται στο Κέντρο Διαχείρισης Δικτύου στη Λάρισα. Σε αυτό εγκαταστάθηκε ένα docker image του CURL με Boring SSL για χρήση του TLS1.3 και της βιβλιοθήκης της Cloudflare quiche (έκδοση 0.17.2). Οι οδηγίες για την εγκατάσταση του docker image βρίσκονται εδώ:

<https://github.com/yurymuski/curl-http3?tab=readme-ov-file>

Η βιβλιοθήκη quiche είναι η υλοποίηση της Cloudflare για το QUIC και μπορεί να βρεθεί στο σύνδεσμο που ακολουθεί:

<https://github.com/cloudflare/quiche>

Στη συνέχεια, από τη δικτυακή θέση:

https://en.wikipedia.org/wiki/List_of_most-viewed_Youtube_videos

που περιέχει τη λίστα με τα 30 δημοφιλέστερα video του Youtube όλων των εποχών, χρησιμοποιήθηκαν οι δικτυακές θέσεις αυτών των video για να πραγματοποιηθούν μετρήσεις του χρόνου πρόσβασης (άρα της καθυστέρησης έναρξης αναπαραγωγής) για τα video αυτά με χρήση των πρωτοκόλλων HTTP/2-TCP και HTTP/3-QUIC. Η προσομοίωση των αιτήσεων των πρωτοκόλλων HTTP/2 και HTTP/3 γίνεται μέσω του CURL. Τα αποτελέσματα που επιστρέφονται από το CURL χρησιμοποιούνται από το σενάριο (script) Python httpstat για την εξαγωγή χρήσιμων πληροφοριών: Το httpstat, το οποίο μπορεί να εγκατασταθεί και ως εντολή στο Linux, χρησιμοποιείται για την εμφάνιση και αποθήκευση πληροφοριών που συλλέγονται με το CURL. Είναι ένα και μόνο αρχείο το οποίο δεν έχει εξαρτήσεις για να εγκατασταθεί σε ένα υπολογιστικό σύστημα.

Πληροφορίες για την εγκατάσταση και χρήση του CURL και του httpstat βρίσκονται στους συνδέσμους <https://curl.se/> και <https://github.com/reorx/httpstat>.

Οι μετρήσεις του χρόνου πρόσβασης με χρήση των πρωτοκόλλων HTTP/2-TCP και HTTP/3-QUIC, έγιναν με τη χρήση της τιμής που περιέχει το πεδίο Content Transfer όπως αυτό προκύπτει από την εκτέλεση της ακόλουθης εντολής για το video που βρίσκεται στη θέση <https://www.youtube.com/watch?v=XqZsoesa55w>:

```
sudo docker run -it --rm ymuski/curl-http3 ./httpstat.sh -  
ILv https://www.youtube.com/watch?v=XqZsoesa55w --http2
```

Ο χρόνος πρόσβασης με χρήση του HTTP/3 για το ίδιο video προκύπτει ως εξής:

```
sudo docker run -it --rm ymuski/curl-http3 ./httpstat.sh -  
ILv https://www.youtube.com/watch?v=XqZsoesa55w --http3
```

Στις εικόνες που ακολουθούν παρουσιάζονται τα αποτελέσματα της εκτέλεσης του CURL για τη δημιουργία αιτήσεων HTTP/2 και HTTP/3 και της εμφάνιση των αποτελεσμάτων που περιέχουν το χρόνο πρόσβασης με τη χρήση του httpstat.

```
osak@plam-lab-desktop:~$ sudo docker run -it --rm ymuski/curl-http3 ./httpstat.sh -ILv https://youtube.com --http2
HTTP/2 301
content-type: application/binary
x-content-type-options: nosniff
expires: Fri, 10 Jan 2025 07:55:24 GMT
date: Fri, 10 Jan 2025 07:55:24 GMT
cache-control: private, max-age=31536000
location: https://www.youtube.com/
content-length: 0
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000; includeSubDomains; preload
content-security-policy: require-trusted-types-for 'script'
permissions-policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua
report-to: {"group":"youtube_main","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/youtu
origin-trial: AmhMBR6zCLzDDxpW+HfpP67BqWIKnWnyMOX00GfzYswFmJe+fgaIE6XZgAzcx0rzNtP7hEDs0o1jdjFnVr2IdxQ4AAAB4eyJvcmlnaW4iOi
ZXByZWVhdGlvbiIsImV4cGlyeSI6MTc1ODAzNzE5OSwlaXNTdWJkb21hZW4iOnRydWV9
cross-origin-opener-policy: same-origin-allow-popups; report-to="youtube_main"
server: ESF
x-xss-protection: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

HTTP/2 200
content-type: text/html; charset=utf-8
x-content-type-options: nosniff
cache-control: no-cache, no-store, max-age=0, must-revalidate
pragma: no-cache
expires: Mon, 01 Jan 1990 00:00:00 GMT
date: Fri, 10 Jan 2025 07:55:24 GMT
content-length: 576913
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000
permissions-policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua
content-security-policy: require-trusted-types-for 'script'
cross-origin-opener-policy: same-origin-allow-popups; report-to="youtube_main"
report-to: {"group":"youtube_main","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/youtu
origin-trial: AmhMBR6zCLzDDxpW+HfpP67BqWIKnWnyMOX00GfzYswFmJe+fgaIE6XZgAzcx0rzNtP7hEDs0o1jdjFnVr2IdxQ4AAAB4eyJvcmlnaW4iOi
ZXByZWVhdGlvbiIsImV4cGlyeSI6MTc1ODAzNzE5OSwlaXNTdWJkb21hZW4iOnRydWV9
p3p: CP="This is not a P3P policy! See http://support.google.com/accounts/answer/151657?hl=en for more info."
server: ESF
x-xss-protection: 0
set-cookie: YSC=4zeitj9GUrK; Domain=.youtube.com; Path=/; Secure; HttpOnly; SameSite=none
set-cookie: __Secure-YES=CgTWULdBQWhVNzJTYjyspI08BJIiCgJHUHicEhgSFhMLFBUWFwYGRobHB0eHw4PIBAREiEgDQ%3D%3D; Domain=.youtu
lte=lax
set-cookie: VISITOR_PRIVACY_METADATA=CgJHUHicEhgSFhMLFBUWFwYGRobHB0eHw4PIBAREiEgDQ%3D%3D; Domain=.youtube.com; Expires=
set-cookie: VISITOR_INFO_LIVE=; Domain=.youtube.com; Expires=Sat, 16-Apr-2022 07:55:24 GMT; Path=/; Secure; HttpOnly; S
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

Body stored in: /tmp/httpstat-body.1175331736495724

[ DNS Lookup | TCP Connection | SSL Handshake | Server Processing | Content Transfer |
 67ms | 73ms | 478ms | 272ms | 2ms |
  namelookup:67ms | connect:140ms | pretransfer:618ms | starttransfer:890ms | total:892ms ]
```

Εικόνα 16. Εκτέλεση του CURL με χρήση του HTTP/2 για το δικτυακό τόπο youtube.com και εμφάνιση αποτελεσμάτων με την httpstat.

```
osak@plam-lab-desktop:~$ sudo docker run -it --rm ymuski/curl-http3 ./httpstat.sh -ILv https://youtube.com --http3
HTTP/3 301
content-type: application/binary
x-content-type-options: nosniff
expires: Fri, 10 Jan 2025 07:52:12 GMT
date: Fri, 10 Jan 2025 07:52:12 GMT
cache-control: private, max-age=31536000
location: https://www.youtube.com/
content-length: 0
strict-transport-security: max-age=31536000; includeSubDomains; preload
x-frame-options: SAMEORIGIN
report-to: {"group":"youtube_main","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/youtube_m
permissions-policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow
content-security-policy: require-trusted-types-for 'script'
origin-trial: AmhMBR6zCLzDDxpW+HfpP67BqWIkNwNyMOX0Q6fzYswFmJe+fgaI6XZgAzcx0rzNtP7hEDs0o1jdjFnVr2IdxQ4AAB4eyJvcmlnaW4iOiJodH
ZXByZWdhbGlvbiIsImV4cGlyeSI6MTc1ODAzNzES0SwiaXNTdWJkb21haw4iOnRydWV9
cross-origin-opener-policy: same-origin-allow-popups; report-to="youtube_main"
server: ESF
x-xss-protection: 0
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

HTTP/3 200
content-type: text/html; charset=utf-8
x-content-type-options: nosniff
cache-control: no-cache, no-store, max-age=0, must-revalidate
pragma: no-cache
expires: Mon, 01 Jan 1990 00:00:00 GMT
date: Fri, 10 Jan 2025 07:52:12 GMT
content-length: 593533
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000
origin-trial: AmhMBR6zCLzDDxpW+HfpP67BqWIkNwNyMOX0Q6fzYswFmJe+fgaI6XZgAzcx0rzNtP7hEDs0o1jdjFnVr2IdxQ4AAB4eyJvcmlnaW4iOiJodH
ZXByZWdhbGlvbiIsImV4cGlyeSI6MTc1ODAzNzES0SwiaXNTdWJkb21haw4iOnRydWV9
content-security-policy: require-trusted-types-for 'script'
permissions-policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow
cross-origin-opener-policy: same-origin-allow-popups; report-to="youtube_main"
report-to: {"group":"youtube_main","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/youtube_m
p3p: CP="This is not a P3P policy! See http://support.google.com/accounts/answer/151657?hl=el for more info."
server: ESF
x-xss-protection: 0
set-cookie: YSC=taNjLK0peJo; Domain=.youtube.com; Path=/; Secure; HttpOnly; SameSite=none
set-cookie: __Secure-YEC=CgsxdnJTtEtQTGdySSiso408BjIiCgJHUhIcEhgSFhMLFBUWFwwYGRobHB0eHw4PIBAREiEgGg%3D%3D; Domain=.youtube.c
tte=lax
set-cookie: VISITOR_PRIVACY_METADATA=CgJHUhIcEhgSFhMLFBUWFwwYGRobHB0eHw4PIBAREiEgGg%3D%3D; Domain=.youtube.com; Expires=Mon,
set-cookie: VISITOR_INFO_LIVE=; Domain=.youtube.com; Expires=Sat, 16-Apr-2022 07:52:12 GMT; Path=/; Secure; HttpOnly; SameS
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

Body stored in: /tmp/httpstat-body.183731736495532

DNS Lookup 10ms | TCP Connection 9ms | SSL Handshake 227ms | Server Processing 214ms | Content Transfer 2ms |
[ namelookup:10ms | connect:0ms | pretransfer:227ms | starttransfer:440ms | total:442ms ]

osak@plam-lab-desktop:~$
```

Εικόνα 17. Εκτέλεση του CURL με χρήση του HTTP/3 για το δικτυακό τόπο youtube.com και εμφάνιση αποτελεσμάτων με την httpstat.

Τα αποτελέσματα των αιτήσεων HTTP/2 και HTTP/3, όπως φαίνεται στις Εικόνες 16 και 17, αποθηκεύονται σε αρχεία στο φάκελο /tmp. Από εκεί λαμβάνονται και επεξεργάζονται οι τιμές όπως περιγράφεται στην ενότητα που ακολουθεί.

6.2 Αποτελέσματα

Στον πίνακα που ακολουθεί εμφανίζονται οι μέσοι όροι των χρόνων πρόσβασης στα 30 δημοφιλέστερα video του Youtube με χρήση του HTTP2/TCP και του HTTP/QUIC. Οι μέσοι όροι υπολογίστηκαν σε ένα δείγμα 10 μετρήσεων που πραγματοποιούνταν κάθε 10 ώρες με χρήση του εργαλείου crontab του Linux¹. Με χρήση του crontab «πυροδοτείται»

¹ Πληροφορίες για τον τρόπο χρήσης του crontab εδώ: <https://linuxhandbook.com/crontab/>

η εκτέλεση των σεναρίων h2_youtube.sh και h3_youtube.sh εναλλάξ. Οι μετρήσεις ξεκίνησαν το Σάββατο 30/11 στις 16:00. Τα αποτελέσματα της εκτέλεσης των σεναρίων, όπως φαίνεται και από τις εκτελέσεις του CURL παραπάνω, αποθηκεύονται σε αρχεία στο φάκελο tmp του συστήματος. Από εκεί αντιγράφηκαν οι τιμές που αντιστοιχούν στο Content Transfer και υπολογίστηκε ο μέσος όρος από τις δέκα προσβάσεις στο κάθε video.

Στον πίνακα που ακολουθεί παρουσιάζονται οι μέσοι όροι των χρόνων πρόσβασης στα 30 δημοφιλέστερα video του Youtube με χρήση HTTP/2-TCP και HTTP/3-QUIC.

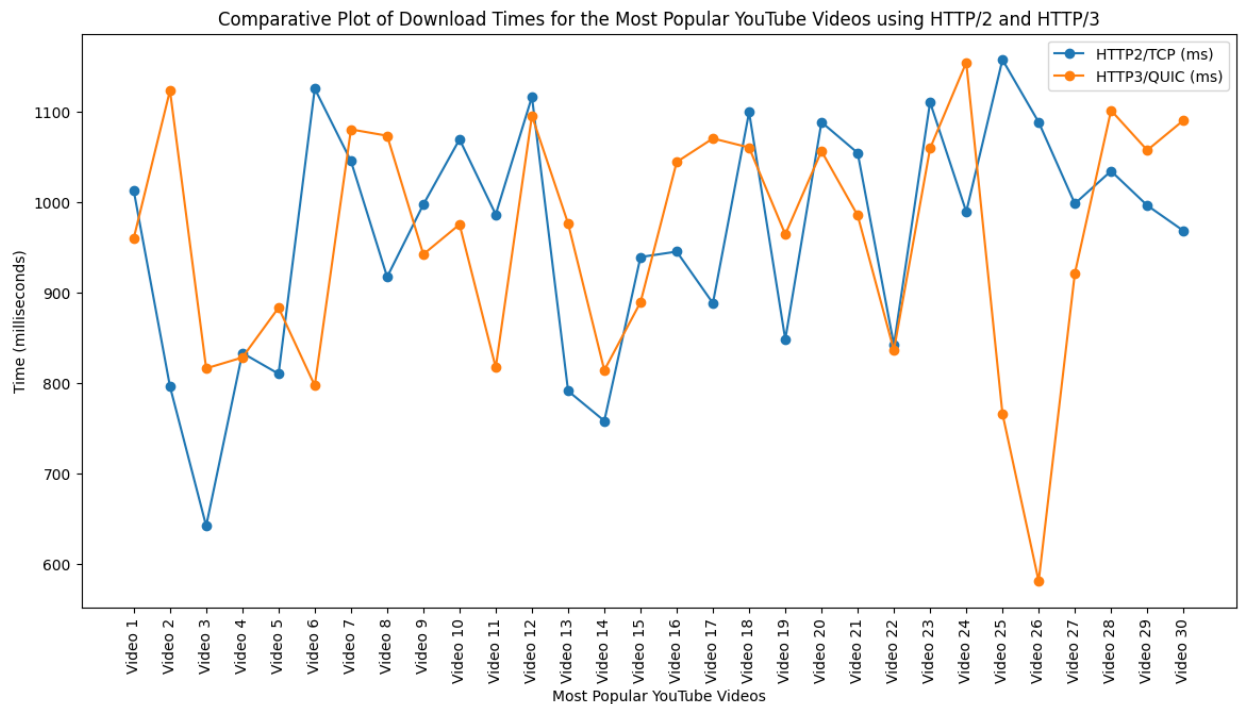
Video	HTTP2/TCP (ms)	HTTP3/QUIC (ms)
1	1012	960
2	796	1123
3	642	816
4	833	828
5	810	883
6	1125	797
7	1045	1080
8	917	1073
9	997	942
10	1069	975
11	986	817
12	1116	1095
13	791	976
14	758	814
15	939	889
16	945	1044
17	888	1070
18	1099	1060
19	848	964
20	1088	1056
21	1054	985
22	842	836

23	1110	1059
24	989	1154
25	1157	766
26	1088	581
27	998	921
28	1034	1101
29	996	1057
30	968	1090

Πίνακας 1. Μέσοι όροι από τις 10 απόπειρες πρόσβασης με HTTP/2-TCP και HTTP/3-QUIC στα 30 δημοφιλέστερα video του Youtube.

Οι μετρήσεις γίνονται εναλλάξ για το HTTP/2 και το HTTP/3, δηλαδή τη μια φορά ξεκινάνε οι μετρήσεις με το HTTP/2 και την άλλη με το HTTP/3. Αυτό συμβαίνει για να μη χρεωθεί η καθυστέρηση σε ένα πρωτόκολλο στην περίπτωση που το video δεν βρίσκεται στον cache cluster που κατευθύνεται ο χρήστης και χρειάζεται να μεταφερθεί μέσω του backbone της Google/Youtube. Όπως προκύπτει από τον παραπάνω πίνακα, η χρήση του HTTP/3-QUIC δεν φαίνεται να βελτιώνει σαφώς το χρόνο πρόσβασης στο video, αφού σε 16 από τις 30 περιπτώσεις ο χρόνος πρόσβασης στα video με το HTTP3/QUIC είναι μικρότερος από τον χρόνο πρόσβασης στο ίδιο video με χρήση του HTTP/TCP. Σύμφωνα και με όσα αναφέρονται στη βιβλιογραφία, το HTTP/3 βελτιώνει το χρόνο πρόσβασης στα video κυρίως σε συνδέσεις μικρής ταχύτητας λόγω του 0-RTT και της ενσωμάτωσης της χειραψίας (handshake) που πραγματοποιεί το TCP και το TLS σε λιγότερα βήματα στο QUIC. Ωστόσο η σύνδεση της εικονικής μηχανής που χρησιμοποιήθηκε στο Internet είναι μεγάλης ταχύτητας, κατά συνέπεια οι μετρήσεις που πραγματοποιήθηκαν επιβεβαιώνουν αντίστοιχα ευρήματα αφού είναι από ότι μετρήθηκε η χρήση του QUIC δεν έχει σημαντικές επιπτώσεις στο χρόνο πρόσβασης στα video.

Στο διάγραμμα που ακολουθεί παρουσιάζεται συγκριτικά η καταγραφή των μέσων χρόνων απόκρισης για τα 30 δημοφιλέστερα video του Youtube, όταν η πρόσβαση γίνεται μέσω του HTTP/2-TCP και του HTTP/3-QUIC.



Εικόνα 18. Συγκριτική παρουσίαση των χρόνων πρόσβασης στα 30 δημοφιλέστερα video του Youtube με χρήση HTTP/2-TCP και HTTP/3-QUIC

Οι μικρές διαφορές στους χρόνους απόκρισης στις περισσότερες περιπτώσεις είναι πιθανό να εξηγούνται εξαιτίας της δημιουργίας πολλών αντιγράφων των δημοφιλών video σε πολλά Youtube cache clusters, αφού τα video αυτά εντοπίζονται πιθανότατα στον cache cluster που μας κατευθύνει η Youtube. Για το λόγο αυτό καλό θα ήταν να πραγματοποιηθούν πειράματα με video που -με μεγάλη πιθανότητα- δεν βρίσκονται στον cache cluster που κατευθύνουν τους Έλληνες χρήστες οι DNS servers της Youtube και από περισσότερους από έναν δικτυακούς τόπους με μεγάλη απόσταση μεταξύ τους, διαφορετικές ταχύτητες σύνδεσης και διαφορετικές δυνατότητες επεξεργασίας, ώστε να κατευθυνθούν σε διαφορετικούς cache clusters και να μελετηθεί η επίδραση του HTTP/3QUIC στο χρόνο πρόσβασης στα video. Ωστόσο κάτι τέτοιο αποτελεί επέκταση της παρούσας εργασίας, όπως και η καταγραφή και άλλων μετρικών για την ΠΕΧ, όπως η μέση πληρότητα του buffer και τα γεγονότα διακοπής της αναπαραγωγής του video.

Κεφάλαιο 7

Συμπεράσματα

7.1 Σύνοψη των βασικών ευρημάτων

Μέσω της σύγκρισης διάφορων ευρημάτων παλαιότερων ερευνών, και τη σχετική βιβλιογραφική ανασκόπηση που πήρε μέρος, σε αυτή τη μελέτη αναλύθηκαν τα πρωτόκολλα H3 και QUIC, η απόδοση, η Ποιότητα Εμπειρίας Χρήστη, οι μετρικές τους, κ.α. Εν γένει, το QUIC, δεν αποτελεί πάντα τη βέλτιστη επιλογή. Αυτό ισχύει περισσότερο σε καταστάσεις μη υψηλού εύρους ζώνης. Μάλιστα σε τέτοιες καταστάσεις, παρατηρείται «επιστροφή» στο TCP. Το σίγουρο είναι ότι κρίνεται αναγκαίο να επανεξεταστεί το πρωτόκολλο αυτό από το δημιουργό του. Η πολυπλεξία και το 0-RTT αποτελούν δύο πολύ δυνατά «χαρτιά» για τη συνέργεια των πρωτοκόλλων αυτών καθώς έτσι ενισχύονται κατά πολύ αποδοτικά. Από την άλλη, στην περίπτωση ανάγκης πολλαπλής αναμετάδοσης των πακέτων εγκατάστασης σύνδεσης, το 0-RTT, κρίνεται ατελέσφορη. Έτσι κρίνεται βασικής αναγκαιότητας ο σχεδιασμός αντίστοιχων πολιτικών που θα υποστηρίξουν αντίστοιχες ροές μέσω μεσαίων κουτιών, ενώ παράλληλα να διασφαλίζεται και η βέλτιστη απόδοση των πρωτοκόλλων αυτών.

Επίσης, κρίνεται σημαντικό να επανεξεταστούν οι αλγοριθμικές τεχνολογίες ABR, με γνώμονα τη βελτίωση της εμπειρίας χρήστη. Παρατηρήσαμε στο κεφάλαιο 5, πως κάποιες από αυτές τις τεχνολογίες οδηγούν σε βέλτιστα ΠΕΧ σε δικτυακές καταστάσεις με απώλειες, πραγματοποιώντας μείωση των ροών. Το βέλτιστο bitrate επιτυγχάνεται με τη βοήθεια των τεχνολογιών μικρής καθυστέρησης, οι οποίοι επιτυγχάνουν αριθμητική μείωση των διακοπών της ποιότητας κατά την αναπαραγωγή πολυμέσων, κατά διαφορετικές δικτυακές καταστάσεις. Τέτοιοι αλγόριθμοι εκ των οποίων οι LA2 και LoL+, δύναται να επιφέρουν μια βελτιωμένη Ποιότητα όσον αφορά την Εμπειρία Χρήστη.

7.2 Προτάσεις για μελλοντική έρευνα στον τομέα αυτό

Σε αυτό το σημείο αξίζει να σημειώσουμε, πως τα πρωτόκολλα αυτά δεν έχουν ακόμη οριστικοποιηθεί από την «IETF». Έτσι, κρίνεται σημαντική η διεξαγωγή μια μελλοντικής μελέτης και έρευνας (πρακτικής) εκ νέου περί της απόδοσής τους σε διαφορετικούς ιστότοπους υπό διαφορετικές συνθήκες δικτύου, εύρους ζώνης, κ.τ.λ. Αυτό βέβαια σημαίνει και μια περαιτέρω έρευνα στην οποία θα λάβουν μέρος πραγματικοί τελικοί χρήστες, με σκοπό την μεγαλύτερη αντικειμενικότητα των ερευνητικών ευρημάτων. Παράλληλα, πραγματοποιείται εγχείρημα από την «IETF» για τη δημιουργία ενός «API QUIC». Σύμφωνα με αυτό, η σύνδεση πολλαπλών υλοποιήσεων και εφαρμογών των δύο πρωτοκόλλων θα δύναται εφικτή από τις εφαρμογές. Με αυτόν τον τρόπο βέβαια, οι προηγούμενες μελέτες, έρευνες θα έχουν τη δυνατότητα να επαναλάβουν τα πειράματά τους, αυτή τη φορά με ένα μεγαλύτερο εύρος υλοποιήσεων και δεδομένων.

Παρά το γεγονός ότι έχει διεξαχθεί μια σχετική έρευνα περί της ασφάλειας που προσφέρουν τα πρωτόκολλα QUIC και HTTP/3, αξίζει να σημειωθεί ότι υπάρχει ακόμη μεγάλο περιθώριο για αντίστοιχη πρόοδο. Έτσι κρίνεται σημαντική η διεκπεραίωση μιας διεξοδικής έρευνας αναφορικά με την ανθεκτικότητα του QUIC απέναντι στις «επιθέσεις πλαστογράφησης IP και πλημμύρας». Αν και η προστασία επικύρωσης διεύθυνσης εφαρμόζεται από την QUIC, θα πρέπει να διερευνηθεί περαιτέρω για να διαπιστωθεί εάν αυτή η προστασία είναι λειτουργική έναντι όλων των υλοποιήσεων QUIC ή όχι. Επιπλέον, εξίσου σημαντική δύναται να αποδειχθεί μια μελέτη περί της εξισορρόπησης της ασφάλειας και της απόδοσης. Η χειραψία 0-RTT με ασφάλεια προς τα εμπρός [39] παρουσιάζει αρκετά υψηλό κόστος απόδοσης, ενώ η χειραψία 0-RTT που χρησιμοποιείται από την QUIC δεν μπορεί να εξασφαλίσει ασφάλεια προς τα εμπρός. Αντίθετα, για να αποκτήσει ισχυρότερη ασφάλεια από τα τρέχοντα πρότυπα ασφαλείας, η QUIC χρησιμοποιεί το TLS1.3. Ως αποτέλεσμα, οι απαιτήσεις επεξεργασίας του QUIC στην CPU έχουν αυξηθεί σημαντικά λόγω του φόρτου κρυπτογράφησης και αποκρυπτογράφησης που επιβάλλεται από την QUIC. Ως εκ τούτου, είναι σημαντικό να διερευνηθεί και να διερευνηθεί πώς να εξισορροπηθεί η ασφάλεια και τα γενικά έξοδα υπολογισμού.

Παράλληλα, μελλοντικά θα ήταν σημαντικό επίσης να διερευνηθεί το ζήτημα των επιθέσεων δηλητηρίασης κρυφής μνήμης. Οι επιθέσεις δηλητηρίασης κρυφής μνήμης που έχουν στόχο εφαρμογές που βασίζονται σε HTTP μπορεί να αποβούν αρκετά

προβληματικές. Ωστόσο, καμία μελέτη δεν έχει ακόμη εξετάσει παρόμοιες επιθέσεις εναντίον του πρωτόκολλου QUIC. Η μελλοντική έρευνα μπορεί να μελετήσει αντίστοιχες επιθέσεις ε τέτοιες υποδομές, επειδή το QUIC εφαρμόζεται σε πολλούς διακομιστές μεσολάβησης και εξισορροπητές φορτίου. Επίσης, όπως είδαμε, οι συνδέσεις QUIC είναι πράγματι ευάλωτες σε επιτιθέμενους συνδεδεμένους και μη στο Ιντερνετ. Για να προσδιορίσουμε καλύτερα τις ενέργειες ενός κακόβουλου χρήστη και να βελτιώσουμε την ασφάλεια των συνδέσεων, μπορούμε να διερευνήσουμε πώς να βελτιώσουμε το πρωτόκολλο για να παρέχουμε πρόσθετους μηχανισμούς εγγύησης στις συνδέσεις QUIC.

Τέλος, μελλοντικά, κρίνεται σημαντικό να αξιολογηθούν οι επιπτώσεις αναφορικά με την ασφάλεια της επανεγκατάστασης αναγνωριστικού σύνδεσης σε περιπτώσεις πελατών κινητών, όπως και η αξιολόγηση έντονης δικτυακής σύνδεσης σε περιπτώσεις πολλαπλών ταυτόχρονων συνδέσεων. Έχοντας αυτά υπόψιν, μελλοντικά τα δεδομένα αυτά θα καθορίσουν την περεταίρω ανάπτυξη των H3 και QUIC.

Αναφορές – Πηγές

[1] Michael Seufert, Raimund Schatz, Nikolas Wehner, Bruno Gardlo, Pedro Casas, “Is QUIC becoming the New TCP? On the Potential Impact of a New Protocol on Networked Multimedia QoE”. 2019

[2] Michael Seufert, Raimund Schatz, Nikolas Wehner, Pedro Casas, “QUICker or not? - an Empirical Analysis of QUIC vs TCP for Video Streaming QoE Provisioning”, 2019

[3] M. Hammad Mazhar, Zubair Shafiq, “Real-time Video Quality of Experience Monitoring for HTTPS and QUIC” 2018

- [4] Thomas Zinner, Stefan Geissler, Fabian Helmschrott, Valentin Burger , “Comparison of the Initial Delay for Video Payout Start for Different HTTP-based Transport Protocols”, 2017
- [5] Mirko Palmer, Thorben Krüger, Balakrishnan Chandrasekaran, Anja Feldmann, “The QUIC Fix for Optimal Video Streaming”, 2018
- [6] Vaibhav Bajpai, Saba Ahsan, J“urgen Sch“onw“alder and J“org Ott, “Measuring YouTube over IPv6” , 2017.
- [7] Adam Langley, Alistair Riddoch, Alyssa Wilk, Antonio Vicente, Charles Krasie, Dan Zhang, Fan Yang, Fedor Kouranov, Ian Swett, Janardhan Iyengar, Jeff Bailey, Jeremy Dorfman, Jim Roskind, Joanna Kulik, Patrik Westin, Raman Tenneti, Robbie Shade, Ryan Hamilton, Victor Vasiliev, Wan-Teh Chang, Zhongyi Shi, “The QUIC Transport Protocol: Design and Internet-Scale Deployment”, 2017.
- [8] D. Bhat, A. Rizk, and M. Zink, “Not so QUIC: A Performance Study of DASH over QUIC,” in Proceedings of the 27th Workshop on Network and Operating Systems Support for Digital Audio and Video, NOSSDAV 2017, Taipei, Taiwan, June 20-23, 2017, ser. NOSSDAV Workshop. New York, NY, USA: ACM, 2017, pp. 13–18. [Online]. Available: <https://doi.org/10.1145/3083165.3083175>.
- [9] Ibrahim Ayad, Youngbin Im, Eric Keller, Sangtae Ha, “A Practical Evaluation of Rate Adaptation Algorithms in HTTP-based Adaptive Streaming”, 2018.
- [10] Sapna Chaudhary , Prince Sachdeva , Abhijit Mondal , Mukulika Maity , and Sandip Chakraborty , “YouTube over Google’s QUIC vs Internet Middleboxes: A Tug of War between Protocol Sustainability and Application QoE”, 2022.
- [11] Martino Trevisan, Danilo Giordano, Ali Safari Khatouni. Measuring HTTP/3: Adoption and Performance. 19th Mediterranean Communication and Computer Networking Conference (2021).
- [12] Yann Bachy, Vincent Nicomette, Eric Alata, Mohamed Ka“âniche, Jean-Christophe Courr“ege. Security of ISP Access Networks: practical experiments. 11th European Dependable Computing Conference - Dependability in Practice (EDCC 2015), Sep 2015, Paris, France. fihal-01190054f
- [13] D. Saif, C.-H. Lung, and A. Matrawy, “An early benchmark of quality of experience between http/2 and http/3 using lighthouse,” arXiv preprint arXiv:2004.01978, 2020
- [14] R. Marx, J. Herbots, W. Lamotte, and P. Quax, “Same standards, different decisions: A study of quic and http/3 implementation diversity,” in Proceedings of the Workshop on the Evolution, Performance, and Interoperability of QUIC, pp. 14–20, 2020
- [15] S. Tellakula, “Comparing HTTP/3 vs. HTTP/2 Performance.” <https://blog.cloudflare.com/http-3-vs-http-2/>, 2020.
- [16] L. Guillen, S. Izumi, T. Abe, and T. Suganuma, “Sand/3: Sdn-assisted novel qoe control method for dynamic adaptive streaming over http/3,” Electronics, vol. 8, no. 8, p. 864, 2019.
- [17] K. Wolsing, J. Ruth, K. Wehrle, and O. Hohlfeld, “A performance “ perspective on web optimized protocol stacks: Tcp+ tls+ http/2 vs. quic,” in Proceedings of the Applied Networking Research Workshop, pp. 1–7, 2019

- [18] G. Carlucci, L. De Cicco, and S. Mascolo, "Http over udp: An experimental investigation of quic," in Proceedings of the 30th Annual ACM Symposium on Applied Computing, SAC '15, (New York, NY, USA), p. 609–614, Association for Computing Machinery, 2015
- [19] A. M. Kakhki, S. Jero, D. Choffnes, C. Nita-Rotaru, and A. Mislove, "Taking a long look at quic: an approach for rigorous evaluation of rapidly evolving transport protocols," in Proceedings of the 2017 Internet Measurement Conference, pp. 290–303, 2017
- [20] M. Kosek, T. Shreedhar, and V. Bajpai, "Beyond quic v1—a first look at recent transport layer ietf standardization efforts," arXiv preprint arXiv:2102.07527, 2021.
- [21] M. Bishop, "Hypertext Transfer Protocol Version 3 (HTTP/3)," InternetDraft draft-ietf-quic-http-33, Internet Engineering Task Force, Feb. 2021.
- [22] J. Iyengar and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport," Internet-Draft draft-ietf-quic-transport-33, Internet Engineering Task Force, Dec. 2020.
- [23] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3." RFC 8446, Aug. 2018.
- [24] D. Bhat, R. Deshmukh, and M. Zink, "Improving QoE of ABR Streaming Sessions through QUIC Retransmissions," in Proceedings of the 26th ACM International Conference on Multimedia, ser. MM '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 1616–1624. [Online]. Available: <https://doi.org/10.1145/3240508.3240664>
- [25] M. Rajiullah, A. Lutu, A. S. Khatouni, M.-R. Fida, M. Mellia, A. Brunstrom, O. Alay, S. Alfredsson, and V. Mancuso, "Web Experience in Mobile Networks: Lessons from Two Million Page Visits," ser. WWW Conference, 2019, p. 1532–1543. [Online]. Available: <https://doi.org/10.1145/3308558.3313606>
- [26] M. Rajiullah, A. Lutu, A. S. Khatouni, M.-R. Fida, M. Mellia, A. Brunstrom, O. Alay, S. Alfredsson, and V. Mancuso, "Web Experience in Mobile Networks: Lessons from Two Million Page Visits," ser. WWW Conference, 2019, p. 1532–1543. [Online]. Available: <https://doi.org/10.1145/3308558.3313606>
- [27] V. Aggarwal, E. Halepovic, J. Pang, S. Venkataraman, and H. Yan. Prometheus: Toward Quality-of-experience Estimation for Mobile Apps from Passive Network Measurements. In ACM HotMobile, 2014
- [28] Justus Wendroth, Benedikt Jaeger: A Brief Overview on HTTP. 2022 https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2022-11-1/NET-2022-11-1_11.pdf
- [28] Xumiao Zhang, Shuwei Jin, Yi He, Ahmad Hassan, Z. Morley Mao, Feng Qian, Zhi-Li Zhang: QUIC is not Quick Enough over Fast Internet. 2023 <https://arxiv.org/pdf/2310.09423>
- [29] Tauqeer M, Gohar M, Koh SJ, Alquhayz H. Use of QUIC for Mobile-Oriented Future Internet (Q-MOFI). *Electronics*. 2024; 13(2):431. <https://doi.org/10.3390/electronics13020431>
- [30] Jayasree Sengupta , Mike Kosek , Justus Fries , Simone Ferlin , and Vaibhav Bajpai: QUIC is not Quick Enough over Fast Internet. 2024 <https://arxiv.org/pdf/2306.11643>
- [31] Alexander Yu, Theophilus A. Benson: Dissecting Performance of Production QUIC. 2021 https://cs.brown.edu/~tab/papers/QUIC_WWW21.pdf

- [32] Constantin Sander, Ike Kunze, Klaus Wehrle: Analyzing the Influence of Resource Prioritization on HTTP/3 HOL Blocking and Performance . 2022 <https://www.comsys.rwth-aachen.de/fileadmin/papers/2022/2022-sander-h3-prio-hol.pdf>
- [33] Tanya Shreedhar , Rohit Panda, Sergey Podanev, Vaibhav Bajpai: Evaluating QUIC Performance over Web, Cloud Storage and Video Workloads. 2021 <https://vaibhavbajpai.com/documents/papers/proceedings/quic-tism-2022.pdf>
- [34] Sindhu Chellappa and Radim Bartos: Is QUIC Quicker with HTTP/3? An Empirical Analysis of Quality of Experience with DASH Video Streaming. <https://www.cs.unh.edu/cnrg/publications/quic-ants-2022.pdf>
- [35] Kazuho Oku and Lucas Pardue: Extensible Prioritization Scheme for HTTP. 2022 <https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-priority>
- [36] Martin Thomson and Cory Benfield: Hypertext Transfer Protocol Version 2 (HTTP/2). 2022 <https://datatracker.ietf.org/doc/draft-ietf-httpbis-http2bis/>
- [37] R. Lychev, S. Jero, A. Boldyreva, and C. Nita-Rotaru, How Secure and Quick is QUIC? Provable Security and Performance Analyses. 2022 <https://datatracker.ietf.org/doc/draft-ietf-httpbis-http2bis/>
- [38] L. Xuebing, C. Yang, Z. Mengying, and W. Xin, Internet Data Transfer Protocol QUIC: A Survey, 2020. <https://crad.ict.ac.cn/EN/10.7544/issn1000-1239.2020.20190693>
- [39] F. Günther, B. Hale, T. Jager, and S. Lauer, “0-RTT Key Exchange with Full Forward Secrecy,” 2017
- [40] CISCO, “Global - 2021 forecast highlights.”. Available: https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf
- [41] W3Techs -Usage statistics of HTTP/3 for website. <https://w3techs.com/technologies/details/ce-http3#:~:text=HTTP%2F3%20is%20used%20by%206.5%25%20of%20all%20the%20website>

