**פרוייקט גמר ברשתות תקשורת**

**תומר שור – 325511541**

**אדם סין – 322453689**

**מתן קליין – 214968240**

**נועם לוין – 326662574**

**שאלות פתוחות:**

**שאלה 1 –**

1. **בעיה ראשונה, הקשר בין CC (Congestion control) לבין שליחה אמינה:** מטרת ה-CC הינה לשלוט בכמות הפאקטות שמועברות ברשת וב-TCP הוא בעצם "ננעל" על מימוש של חלון שליחה שתוכנן במקור לצד המקבל בכדי לבצע בקרת זרימה על הצד השולח ובכך לוודא שיש שליחה אמינה. מכיוון שהוא "נעול" על מימוש ספציפי, כל איבוד של חבילה (פאקטה) יגביל את ההתקדמות והגדילה של החלון עד שהחבילות שאבדו יגיעו מחדש. בזמן שאנו נזהה את האובדן ונשלח מחדש את המידע, רוב החבילות שבחלון היו יכולות כבר להתקבל אצל הצד המקבל, כלומר "יצאו מהרשת".נתאר דוגמה שתמחיש לנו את הבעיה: נניח שהמקבל קובע את חלון בקרת הזרימה שלו ל-8 חבילות ושגם חלון ה-CC הינו בגודל 8. כאשר חבילה מספר 1 תגיע החלון של השליחה יתקדם לטווח שבין חבילה 2 ל-9. אם למשל כעת חבילה 2 נאבדה אז זה מונע מאיתנו להמשיך לקדם את החלון גם אם חבילות 3 עד 9 הגיעו ולא אבדו בדרך. מכך נוצר מצב בו כמות החבילות שלא שלחנו עליהן ACK לא משקפת את כמות החבילות שנמצאות ברשת שכן חלקן התקבלו כבר ולא צריך לשלוח אותן מחדש.
2. **בעיה שנייה, Head of line blocking:** בגלל ש-TCP מבטיח העברה רציפה של מידע, האובדן של חבילה אחת בלבד תחסום את הקבלה של כל החבילות הבאות עד שהחבילה שאבדה תגיע מחדש. נסתכל על דוגמה שתמחיש את הבעיה: נניח ששלחנו את חבילות 1 עד 6. חבילה 2 הגיעה אל המקבל אך חבילה 1 נאבדה בדרך. המידע שיש בחבילה 2 לא יכול לעבור לשיכבת האפליקציה עד שחבילה 1 תשלח מחדש, תתקבל ותישלח קודם לשיכבת האפליקציה כדי להבטיח העברה ששומרת על הסדר. הבעיה הזו דומה מאוד לבעיה הראשונה שהצגנו אך פה התייחסנו לבעיה שמתרחשת אצל המקבל ומקודם התייחסנו לבעיה אצל השולח.
3. **עיכוב (delay) בעקבות הקמת קשר:** ב-TCP כל פעם ששתי נקודות קצה רוצות לתקשר בניהן חייבת להתקיים לחיצת יד משולשת. אם בנוסף לכך נרצה לאבטח את הקשר על ידי TLS אנו נזדקק ל-RT נוסף בכדי להחליף אישורי אבטחה בין שתי הנקודות. הקמת הקשר בצורה כזו לוקחת זמן רב שמעכב את שליחת המידע.
4. **הגבלות שנובעות מ-header קבוע ל-TCP:** ה-header של TCP הינו אוסף של שדות שקבועים בגודלם. 3 שדות ספציפיים ב-header של TCP הושפעו ישירות מהעלייה במהירות הרשת לאורך זמן – seq# ו-ACK ששניהם בגודל של 4 בתים, וגודל חלון בקרת הזרימה שגודלו הינו 2 בתים. הגדלים הקטנים האלו מגבילים את הביצועים של TCP במהירות גבוהה ברשת. ה-seq# וה-ACK "נעטפים" מהר מידי מה שהופך אותם לכבר לא ייחודיים, וגודל חלון הזרימה מגביל בצורה ישירה את תפוקת החיבור של TCP אשר חסומה על ידי גודל החלון כפול ה-RTT.
5. **מזהה ייחודי לחיבור ולכתובת ה-IP:** כתובת ה-IP של כל אחת מנקודות הקצה בחיבור TCP עלולה להשתנות המהלך חייו של החיבור בעקבות שלל סיבות – אירוח של מספר משתמשים, ניידות או ריצה מאחורי NAT. בגלל ש-TCP משתמש בשילוב של כתובות ה-IP ומספרי ה-port של שתי נקודות הקצה כמזהה לחיבור, כל שינוי בכתובת ה-IP של אחת מנקודות הקצה תשבור את החיבור הקיים מה שיגרום לכל המידע שהועבר על כה "להיזרק". בכדי להתאושש ממצב זה אנו נזדקק ללחיצת יד משולשת חדשה בכדי לפתוח קשר חדש.

**שאלה 2 –**

1. **הגדרת מזהה לחיבור של הקשר ומזהה למידע שעובר –** על מנת שנדע לזהות ולהבדיל בין חיבורים שונים ובין מידע שונה.
2. **ניהול חיבורי התעבורה –** שזה בין היתר להגדיר מזהה חיבור ייחודי שמקשר בין 2 רכיבי קצה, שליטה במידע שמוחלף, הגדרת מצב חיבור וניתוק ותמיכה בשינוי ה- IP של המארח.
3. **העברת מידע באופן אמין –** מזהה מידע ייחודי על מנת להעביר את המידע באופן אמין בין רכיבי הקצה, ושליטה בחלון זרימה בשביל העברה אמינה על מנת שלא ניתקע בבעיה שהפאקטה הראשונה בתור נתקעת וע"י כך מונעת מפאקטות אחרות שאחריה לעבור עיבוד או להישלח(נקראת head of line blocking problem).
4. **בקרת עומסים –** שליטה שבפאקטות שבתוך הרשת על מנת שלא להעמיס על רכיבי הקצה ועל הרשת עצמה.
5. **אבטחה –** חיבורים מוצפנים והעברת מידע באופן מאובטח.

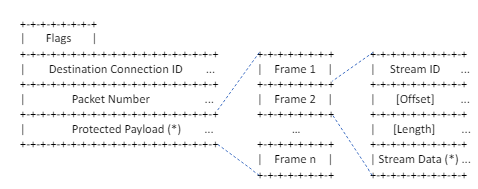
**שאלה 3 –**

הפרוטוקול QUIC משלב העברת מידע ולחיצת יד ובכך משיג את המידע הנדרש ב-RTT אחד בלבד. למעשה, זה כולל ביצוע אמין של החלפת מפתח (בין נקודות הקצה) של TLS 1.3 באותו הזמן עם החלפה אמינה של פרמטרים לטובת העברת מידע. הצורה הזו של לחיצת היד מקטינה את העיכוב בהקמת קשר מאובטח כמו שדיברנו עליו בליחת היד של TCP. בעוד ש-TCP מפריד בין לחיצת היד לבין ביסוס האבטחה בין שתי נקודות הקצה, אשר גורר כמו שציינו בשאלה 1 לפחות שני RTT, QUIC מקטין זאת ל-RTT אחד. QUIC משתמש בפאקטה (חבילה) התחלתית בכדי לדון ב-ConnectionID על מנת לפתוח חיבור (קשר) חדש. כל נקודת קצה תאכלס את השדה שלה של ה-C-ID בערך שנבחר וערך זה ישמש כל צד כ-ID ליעד בשליחת הפאקטות בהמשך. בקבלת הפאקטה ההתחלתית השרת יכול לבחור לאמת את כתובת הלקוח בעזרת שליחה של פאקטה חוזרת (Retry packet) שמכילה token רנדומלי, אשר אמור להתקבל בחזרה על ידי הלקוח בפאקטה התחלתית חדשה על מנת להמשיך בתהליך לחיצת היד. גם ההודעות שקשורות ל-TCP 1.3 מוטמעות בפאקטות ההתחלתיות כך שהן יכולות לשמש כביסוס של "סוד משותף" על מנת לשמור על אבטחה ואמינות של פאקטות עתידיות שישלחו, ב-RTT יחיד. ה-C-ID שנבחר יכלל בפרמטרים של ההעברה והוא יאומת במהלך תהליך לחיצת היד של ה-TLS. בכך ש-QUIC דן על ה-C-ID, הוא תומך ביצירה אמינה של קשר חדש בצורה דומה לפונקציונאליות שאנו מקבלים מ-TCP. QUIC מאפשר ללקוח לשלוח ב-0-RTT מידע מוצפן בפאקטה הראשונה שהוא שולח על ידי שימוש חוזר בפרמטרים מהחיבור הקודם, ומפתח ל-TLS 1.3 שנחשף מוקדם יותר על ידי השרת. בעיה קטנה היא שמידע שמועבר ב-0-RTT אינו מוגן מפני התקפות replay. בתמיכה בשליחה של מידע ב-0-RTT, QUIC יכול גם להתמודד עם מקרים בהם נדרש T/TCP.

**שאלה 4 –**

ל-QUIC יש שני סוגים של headers. סוג אחד בשביל הקמת החיבור וסוג שני (וקצר יותר) לאחר הקמת החיבור ("לחיצת יד").

להלן תמונה של הפאקטה הקצרה יותר-



כלומר, בכל פאקטה אפשר להכניס frame אחד או יותר.

כמו כן, הפאקטה ששולחת selective ACK יכולה לשלוח עד 256 ACK-ים לעומת 3 ב TCP.

השיפורים שבאים לידי ביטוי בין היתר: הפאקטה ששולחים אחרי שהקשר נוצר הרבה יותר קצרה מב-TCP ובכך מונעת שליחה מבוזבזת של מידע. הפאקטה תומכת ב-streams ובכך מונעת את בעיית ה-Head of line.

**שאלה 5 –**

ראשית, נתחיל בזיהוי של איחור או איבוד ב-QUIC על ידי ACK. כל חבילה של QUIC מכילה בתוכה "frames" כך שאנו יכולים להתייחס לכל "frame" כפאקטת IP. QUIC מזהה איבוד חבילות על בסיס פאקטות אלו. על כל חבילה שקיבלה ACK, כל ה-"frames" שהיו באותה החבילה נחשבים ככאלו שהגיעו בהצלחה. "frames" נחשבים ככאלו שאבדו אם החבילה שבתוכה הם נשלחו עדיין לא קיבלה ACK כאשר חבילה שנשלחה אחרי כבר קיבלה ואנו עוברים איזה סף מסויים. ל-QUIC יש שני סוגים של סף לקביעת איבוד חבילות – אחד, על פי מספר החבילה: כל החבילות שנשלחו והמספר הסידורי שלהן (seq#) קטן בכמות מסויימת מהחבילה שקיבלנו עלייה ACK. שתיים, על פי זמן: החבילה שנשלחה כבר נשלחה לפני יותר מה-RTT המקסימלי שמדדנו על כה, לפני החבילה שכבר קיבלנו עליה ACK. סוגי הסף האלו מספקים לנו קצת "זמן של חסד" לפני קביעה של איבוד חבילה בכדי שלא יווצר לנו מצב בו אנו שולחים מחדש חבילות ללא צורך אמיתי. בנוסף הם באים גם למנוע ירידה בביצועים שנגרמת מה-CC כאשר יש זיהוי של איבוד חבילה. בכדי לזהות איבוד של "חבילות זנב", QUIC מאתחל טיימר בכל פעם שחבילה שאמורה לקבל ACK נשלחת, כאשר הוא כולל את ה-RTT המשוער, את השונות בין דגימות ה-RTT, ואת הזמן המקסימלי שהמקבל עשוי לחכות עד שהוא שולח ACK. כאשר הטיימר שלנו מתאפס (נגמר), השולח יישלח חבילה חדשה שדורשת ACK לבדיקה כך שאפשר גם כבר להתחיל לכלול בה מידע שאנו צריכים לשלוח שוב ובכך להוריד את כמות השליחות מחדש. כעת נראה כיצד QUIC מתאושש מאיבוד חבילות. לאחר שזוהה איבוד, ה-"frames" האבודים מוכנסים לחבילה חדשה שתקבל מספר שונה ללא קשר לחבילות שנאבדו. סך הכל אנו רואים ש-QUIC מספק לנו סדר אמין של שליחה וקבלה של מידע בדומה למה ש-TCP מספק לנו.

**שאלה 6 –**

QUIC משתמש במספר פאקטה לבקרת עומסים ול-offset ב-frames של ה-streams לצורך בקרת אמינות. כמו TCP יש ל QUIC חלון שמגביל את המקסימום בתים שהשולח יכול להעביר בכל רגע נתון. QUIC לא מחפש ליצור אלגוריתמים של בקרת עומסים או לממש קיימים, הוא מספק קווים כלליים לבקרת עומסים ונותנת לשולח חופש למשש בעצמו. בשביל למנוע צמצום לא הכרחי של החלון הוא מקריס את החלון רק אם הוא מזהה עומס קבוע: במידה ושני פאקטות אבדו וגם אף אחת מהחבילות שנשלחו ביניהם לא אושרו. השולח יאט את השליחה בשביל לצמצם את הסיכויים לגרימת עומס בטווח הקצר ע"י שליחת הפאקטות שיעלו על הזמן של החישובים שמבוססים על ה RTT הממוצע, גודל החלון וגודל הפאקטה.

**חלק "רטוב"**

נציג לפניכם את הסטטיסטיקות עם כמה דגשים:

1) בשלבי המימוש של השולח והמקבל, נתקלנו בבעיה הנובעת מחוסר התקשורת בין השולח והמקבל:

בעוד המקבל מחכה לחבילה, מקבל אותה ועושה פעולות של שמירת הנתונים במקום הנחוץ, וחישוב סטטיסטיקות לפני שיוכל לקבל את החבילה הבאה,

השולח ממשיך לשלוח חבילות בקצב שגורר חבילות רבות שנשלחו למקבל אבל הוא היה עסוק מכדי לקבל אותם.

נוצר מצב של איבוד של כ65%~ מהחבילות!

אנו ניגשנו לפתור את הבעיה הזאת על ידי הקצעת זמן בו השולח יחכה לאחר ששלח חבילה, מהפעם שיוכל לשלוח את החבילה הבאה. עם קצת ניסוי וטעיה בחיפוש אחר הזמן המינימלי שיבטיח חוסר מוחלט באיבוד חבילות מצאנו ש0.0005 הוא הזמן האידיאלי.

ברור שזה משפיע על הריצה הכוללת של השולח והמקבל אבל לא משפיע על הסטטיסטיקות שכן זה לא היה בטווח הקוד אותו אנחנו מודדים.

2) משום שהמטרה של QUIC היא למנוע שליחת כל המידע בחבילה אחת, דבר העשוי לעכב קבצים מסוימים כאשר חבילה נאבדת גם אם הן לה קשר לקובץ, החלטנו שבכל שליחת חבילה נבחר 60% מהקבצים הקיימים. כך שבתיאוריה, גם אם תאבד חבילה, הקבצים שלא נשלחו בחבילה הנאבדת יוכלו להמשיך ולהישלח.

3) דגש נוסף הוא אי בירור כיצד לפרש את ממוצע הביטים/חבילות לשנייה. ישנם 2 דרכים שונים להסתכל על חישוב זה:

א) חישוב מספר הביטים לשנייה לכל חבילה, וחישוב הממוצע בין כל החבילות.

ב) חישוב מספר הביטים הכולל, והזמן הכולל שלקח, וחילוק ביניהם.

דוגמה:

חבילה 1: 100 בתים, חושבה ב0.01 שניות

חבילה 2: 150 בתים, חושבה ב0.03 שניות

חבילה 3: 200 בתים, חושבה ב0.06 שניות

ממוצע החבילות = 611.11 = (דרך א')

ממוצע החבילות = 450 = (דרך ב')

בשביל להיות בטוחים, הצגנו סטטיסטיקות לשתי הדרכים.

**דרך א':**

העברנו את הדפסות הקוד לטבלה בה ניתן לראות את הנתונים של כל זרימה בכל הרצה. הרצה 1 מסמלת את ההרצה בה שלחנו קובץ יחיד והרצה 10 את ההרצה בה שלחנו 10 קבצים ב10 זרימות שונות:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Run 10** | **…** | **Run 2** | **Run 1** |  |  |
| 19270310.70843328 |  | 92684082.55670367 | 134065944.1803061 | Average num of bytes per second | **Total** |
| 10497.162315154495 |  | 50403.37801019834 | 72907.57237589273 | Average num of packets per second |
| 1048589 |  | 1048589 | 1048589 | total num of bytes | **Stream 1** |
| 3411 |  | 571 | 571 | total num of packets |
| 3293468.3564966125 |  | 93605678.9528709 | 134065944.1803061 | average num of bytes per second |
| 10757.560164237088 |  | 50904.28057964331 | 72907.57237589273 | average num of packets per second |
| 1048589 |  | 1048589 | **X** | total num of bytes | **Stream 2** |
| 3397 |  | 571 | total num of packets |
| 3182121.620446689 |  | 91762486.16053617 | average num of bytes per second |
| 10387.733818945178 |  | 49902.47544075348 | average num of packets per second |
|  |  |  |  |  | **…** |
| 1048589 |  | **X** | **X** | total num of bytes | **Stream 10** |
| 3427 |  | total num of packets |
| 3266751.3697198206 |  | average num of bytes per second |
| 10675.71368535687 |  | average num of packets per second |

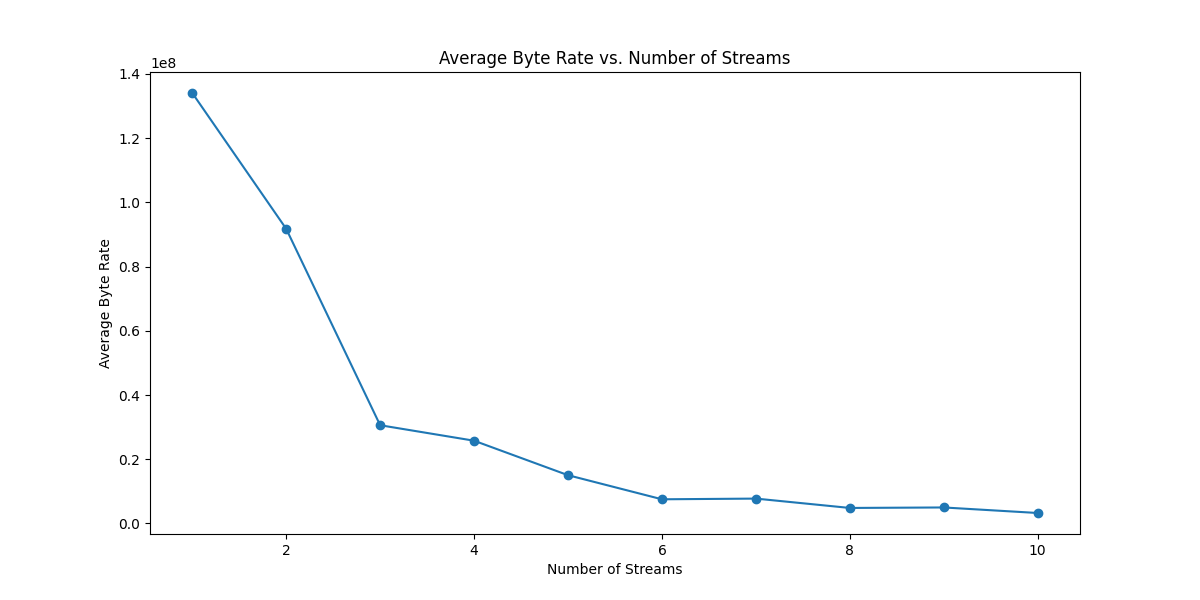
חשוב לציין שבגלל הגדרתנו לשלוח 60% מהקבצים בכל שליחת חבילה בין הרצות מסוימות יכול להיות שמספר החבילות הנשלחות בין כל זרימה יהיה זהה.

כלומר בהרצות מספר 1 ו2 ניתן לראות אותו מספר חבילות לכל זרימה. זאת בגלל שכאשר ניקח 60% מהזרימות (ונעגל) נראה שנשלח כל פעם חבילה אחרת, ובגלל הגדלים הזהים של הקבצים המספר מתחלק שווה בשווה

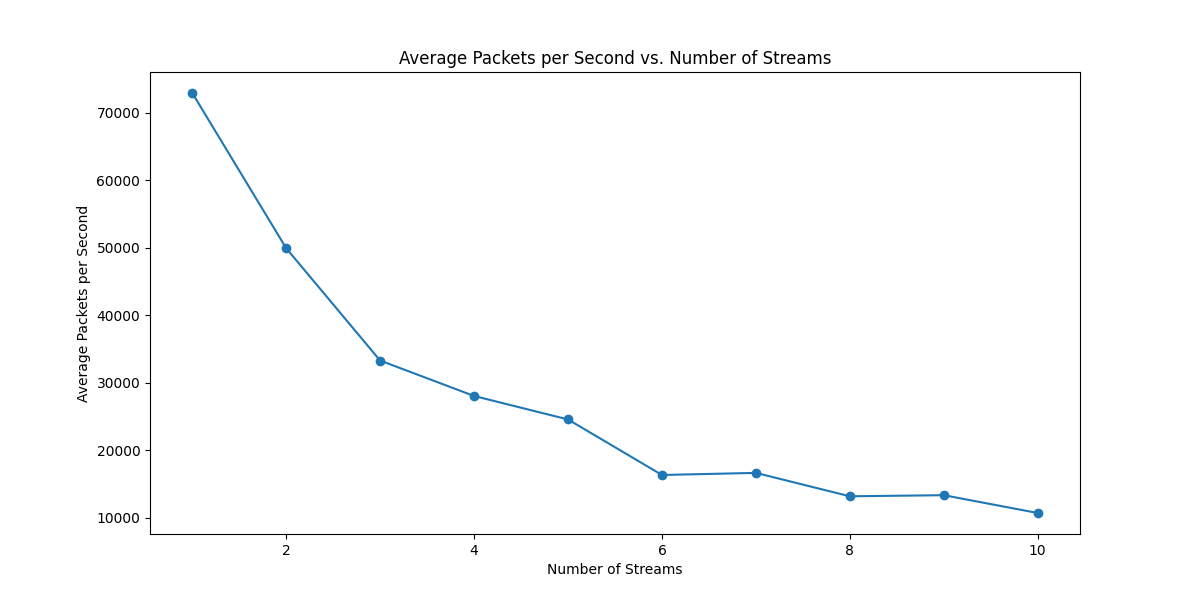
ככל, מספר החבילות הנשלחות בכל זרימה הולך וגדל ככל שאנחנו שולחים יותר קבצים, כי ה60% הנשלחים הם מספר קבצים רב יותר, ובכך חילוק המקום בחבילה מתחלק לפריימים בגדלים קטנים יותר.

הגרף הבא מציג את מספר הביטים לשנייה הממוצע בכל הרצה (1-10).

ניתן לראות בבירור שיש השפעה של מספר הקבצים הנשלחים לבין הקצב בוא הביטים נרשמים אצל המקבל. ככל פעם שמגדילים את מס' הזרימות קצב הנתונים הכולל יורד, כי



מאותה סיבה בדיוק, אנו רואים ירידה במספר החבילות הנשלחות בשנייה יורד גם כן:



**דרך ב':**

כל הערה ותובנה מדרך א' תופסות גם כאן, אלו התוצאות:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Run 10** | **…** | **Run 2** | **Run 1** |  |  |
| 4727826.335523504 |  | 24828018.113064244 | 34834992.057436 | Average num of bytes per second | **Total** |
| 2996.966557175855 |  | 15745.57051922891 | 22091.84887329062 | Average num of packets per second |
| 1048589 |  | 1048589 | 1048589 | total num of bytes | **Stream 1** |
| 3966 |  | 665 | 665 | total num of packets |
| 798726.0770087006 |  | 22717334.5389247 | 34834992.057436 | average num of bytes per second |
| 3020.96209422043 |  | 14407.005479158111 | 22091.84887329062 | average num of packets per second |
| 1048589 |  | 1048589 | **X** | total num of bytes | **Stream 2** |
| 3926 |  | 665 | total num of packets |
| 805550.4743482079 |  | 27371084.91704115 | average num of bytes per second |
| 3016.044572555181 |  | 17358.34675915193 | average num of packets per second |
|  |  |  |  |  | **…** |
| 1048589 |  | **X** | **X** | total num of bytes | **Stream 10** |
| 3973 |  | total num of packets |
| 797273.4876928602 |  | average num of bytes per second |
| 3020.790382698782 |  | average num of packets per second |

