מטלה 4 – תקשורת

מגישים :

יעקב חודורקובסקי – 207045063

דולב דובלון –

חלק א׳ – DoH

תשובות :

1. Doh מאפשר להשתמש בכל ההיררכיה והמנגנון של DNS , ולהשתמש בו בשילוב כל הפיצ'רים מ HTTP , לדוגמא : Redirect , Compression ,Caching and Authentications . מומלץ להשתמש ב DoH על גבי HTTP/2 כדי לנצל באופן מלא את האפשריות השונות כגון דחישה של המידע העובר על הטווח ו HTTP pipline .
2. א. DNS הינו צריך להיות מהיר , פרוטוקול DNS משתמש ב UDP שהוא בשביל פקטות מהירות הדורשות פחות אמינות , כך שאם פקטה משתבשת פשוט אחת אחרת נשלחת , ב DoH הפרוטוקול הוא TCP , אשר מאט את יצירת החיבור , ומשפיע על המהירות , בנוסף יש את ההצפנה המשפיעה על הביצועים.

ב. DoH מספק לנו הגנה מפני ספקי תקשורת , ומאפשר רק לשרת ה DoH שלנו לראות למי אנו פונים מה שלא בהכרח טוב לארגונים פרטיים שרוצים לנתר מידע . מערכות רבות מסמכות על מהמידע ש DNS אינו מוצפן , הן יכולות לראות לאן אנו ניגשים , לשמור את זה , ובהתאם לחסום או לדווח על כך .

1. נראה פתרון עבור חסרון 2.ב. :

כאמור אמרנו שהבעיה לא טובה עבור ארגונים פרטיים בכך שאינם יכולים לנתר את המידע בבקרה על עובדיה . פתרון אפשרי היא שהחברה תמצא פתרון שמתאים עבורה בצורה שלא משתמשת רק ב DNS או בדרך מימוש אחרת ש ל DoH עצמו .

1. a ⇔b : ב – a המימוש מתבצע דרך ה דפדפן ( בפירפוקס לדוגמא ניתן להפעיל DoH בהגדרות ) ו ה DNS-quaries מאובטחות ע״י הספק אינטרנט שלך . ב –b המימוש מתבע באותו דרך רק על הדפדפן והוא מצריך שרת נוסף שמבצע עוד פעם את התהליך , בנוסף שרתי proxy גם לרוב יש להם עלות כספית . עדיף את a .

a ⇔c : ב- a המימוש מתבצע רק תחת הגדרות הדפדפן למרות ה DNS-quarries מאובטחות ע״י ספק האינטרנט , ספקי DoH עדיין יכולים לקשת לנתונים . ב – c עם שרת local Proxy מקומי אנו שולחים את הבקשות בצורה מסווה מראש ולכן אנו יותר מוגנים מספקי ה DoH . בכך עדיפות ל c .

a ⇔d : ב – a המימוש הוא בדפדפן ו ב d מדובר בשימוש על תוכנות שמותקנות במחשב שצורכות תקשורת. העדיפות ניתנת בהתאם לצורך .

b⇔c : ב- b השרתים מוצעים ע״י ספקי האינטרנט ואבטחת ה DNS-quarries ברמת הדפדפן . ב – c מימוש ה DoH הוא עם Proxy Server מקומי שהשליטה בו נעשת על ידינו ולכן הוא יותר אמין ומוגן ובנוסף הוא יכול לתמוך בתוכנות אחרות מחוץ לדפדפן , לכן עדיף c .

d⇔b : ב -b המימוש DoH הוא דרך הדפדפן , ב -d המימוש DoH הוא על תוכנות שעל המחשב . העידפות היא תלוי בצרכים .

d⇔c ב -d המימוש DoH הוא על תוכנות שעל המחשב . ב – c מימוש ה DoH הוא עם Proxy Server מקומי שיכול לממש DoH על כל DNS query , עדיף c .

לסיכום : c הדרך הכי טובה לדעתנו , גם הכי אמינה ומאובטחת וגם הכי הרבה שליטה.

1. Do35 משתמש בפרוטוקול UDP . בעוד ש DoH משתמש ב TCP שנותן לו גישה למדיניות של TCP fast retransition לכן DoH יכול לשחזר פקטות שאבדו במהירות גבוהה יותר , מה שלא יכול לקרות ב Do35.

חלק ב : Congestion control -- NEED TO ADD WIRESHARK ANALYZE

TCP-Reno- uses slow start , congestion audience and fast retransmit triggered by triple dubplicate ACKs ,each time there is a packet loss , the sending rate is cut in half and then increases the sending rate by 1 mss every RTT until another less is detected.

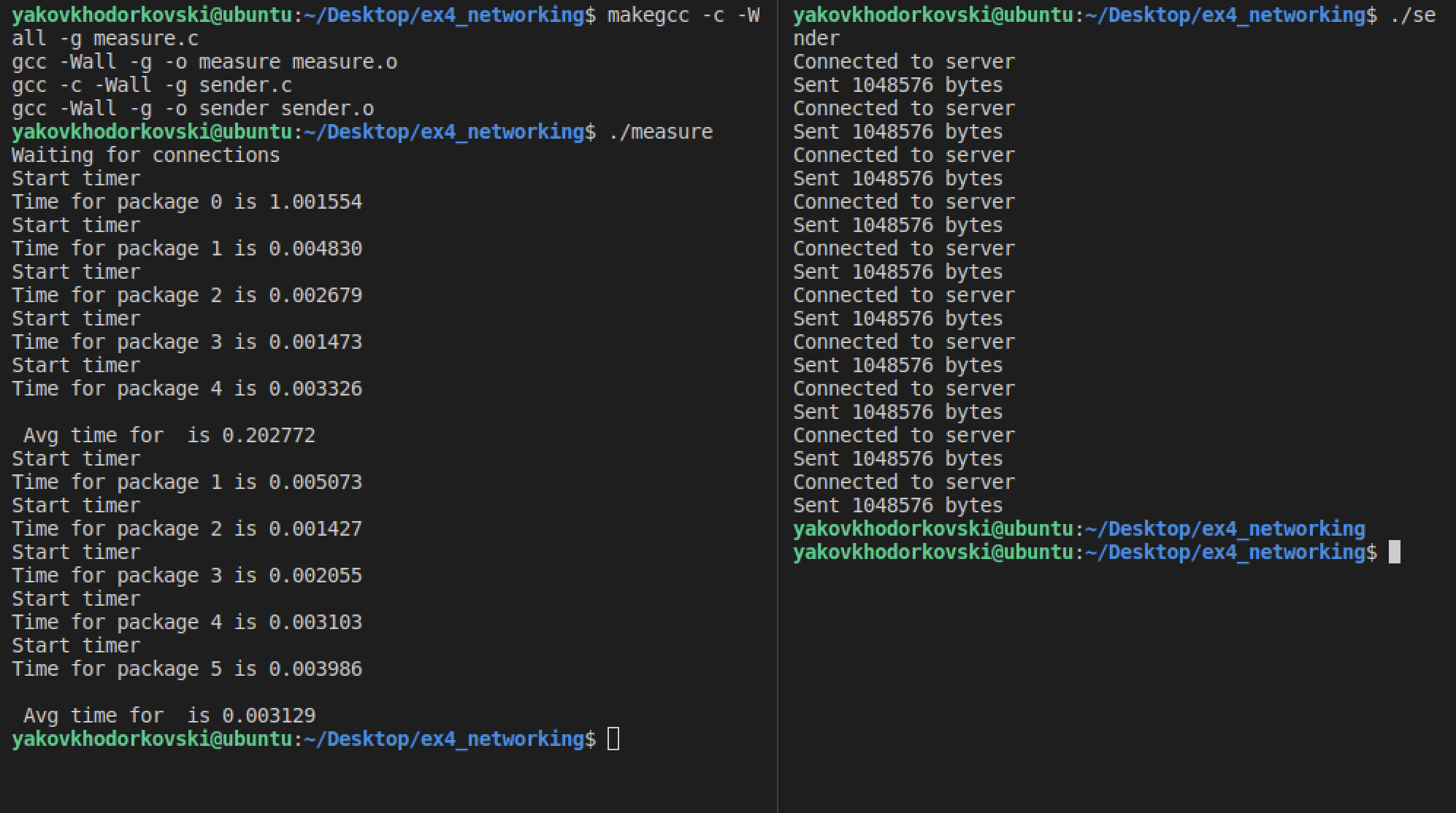
TCP- CUBIC : also cutting the densing rate by half each time a loss was tesected , initially it ramps to wmax faster , but then approanches wmax mor slowly .

We can say that events of higher packet loss CUBIC is much faster because he can reach Wmax faster then rano .

Here are the resualts of using 1MB file :

|  |  |  |
| --- | --- | --- |
|  | Cubic | Reno |
| 0% | 0.200979 | 0.0011 |
| 10% | 0.396905 | 0.209518 |
| 15% | 1.182074 | 2.069763 |
| 20% | 1.383675 | 9.79906 |
| 25% | 9.817438 | 43.507946 |
| 30% | 40.345156 | 81 |

here screen shots of running the terminal :



now for each packet loss :

|  |  |  |
| --- | --- | --- |
| Packet loss percent | Cubic | Reno |
| 0 |  |  |
| 10 |  |  |
| 15 |  |  |
| 20 |  |  |
| 25 |  |  |
| 30 |  |  |