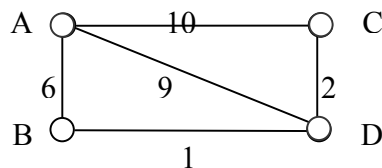


פתרון שאלות נבחרות בבחינה בקורס מבוא לתקשורת 2002 – מועד ב'

המרצה: דני ביקסון
תאריך הבחינה: 2.9.02

1. א. (5 נקודות) הסבר מהו IP fragmentation ומדוע הוא דרוש.
תשובה: זהו פיצול של הודעה למספר הודעות קטנות יותר. הדבר דרוש כאשר אנו מעוניינים לשדר הודעה לתוך link אשר קיימת בו מגבלה על אורך ההודעה, וההודעה שאנו מעוניינים לשדר ארוכה יותר.
 ב. (8 נקודות) הסבר מי מבצע את ה- fragmentation מי מבצע את האיחוי (defragmentation). ומתי.
תשובה: את הפיצול מבצע ה-router כאשר הוא נתקל ב-link "צר" מדי שלא מאפשר להכיל את ההודעה כיחידה אחת. את האיחוי מבצע היעד, זאת כדי לחסוך זמן ועבודה ל-routers בדרך. יתכן כי אם היינו מאחים את ההודעה בכל תחנה בדרך, היינו מיד צריכים לפצל אותה שוב וזהו בזבוז רב של זמן ועבודה. תחנה הקצה בכל מקרה תצטרך לאחות את החלקים לפני שהיא מעלה אותם לשכבת ה-transport ולכן זה טבעי שהיא תבצע את התפקיד.
 ג. (10 נקודות) אלו שדות ב-IP Header משמשים אותנו לביצוע ה-fragmentation וכיצד? (יש לפרט גם כיצד מתבצע החישוב).
תשובה: כולם ענו נכון.
 ד. (6 נקודות) הסבר מהו MSS (Maximum segment size) ואיזה בעיה הוא בא לפתור.
תשובה: זהו יחידת מידה המקיימת שתי תכונות: היא היחידה המקסימלית שניתן לקחת מבין המינמום על מגבלות אורך ההודעה בכל הרשתות הנפוצות. בד"כ זהו מספר בסביבות 560 בתים. המטרה היא ליצור הודעה מספיק קטנה שתעבור בכל ה-links בלי צורך בביצוע fragmentation, ומצד שני לא תהיה קטנה מדי כי בכך אנו מפסידים ביעילות השידור (ראה חומר שלמדנו על silly window syndrome). לסיכום: אנו מנסים לעקוף את הבעיה.
 ה. (4 נקודות) הסבר מהם החסרונות של ביצוע fragmentation.
תשובה: מוסיף סיבוכיות למערכת, למשל: שדות נוספים ב-header – מגדיל את נפח התקשורת. מחייב החזרת buffer המשמש לסידור ההודעות לפי הסדר לפני האיחוי – יותר זיכרון. מחייב החזקת timer ע"מ לוודא שכל ההודעות הגיעו תוך פרק זמן מסוים. דורש עבודה נוספת מה נתבים ומתחנת היעד. יותר הודעות נשלחות ברשת – עלול ליצור יותר פגיעות לאיבוד הודעות. במקרה שחלק קטן אובד – כל ההודעה צריכה להשלח מחדש.
2. א. (23 נקודות) ברצוננו להשתמש בקוד CRC ע"מ לשלוח את ההודעה הבאה (משמאל לימין): 110110110. הפולינום היוצר הינו $X^4 + X + 1$. חשב את השידור ואת הפיענוח.
תשובה: הרוב ענו נכון. יש לשים לב ש-10000 מתחלק ב-10011 כי זהו חילוק פולינומים.
 ב. (5 נקודות) תן דוגמא לפרוטוקול שלמדנו המשתמש בקוד CRC והסבר לשם מה.
תשובה: כולם ענו נכון.
 ג. (5 נקודות) תן דוגמא למצב בו תיתכן טעות בהודעה אך לא נגלה זאת ע"י קוד CRC.
תשובה: תיתכן טעות כאשר המספר המשודר ישתנה למספר אחר שהוא כפולה של הפולינום היוצר. ניתן היה לתת פה גם דוגמא מספרית למצב המתואר.

3. נתונה הרשת הבאה: A, B, C, D הינם routers. משקלי הצלעות המחברות ביניהם הם לפי התרשים הבא:



א. (10 נקודות) הרץ את אלגוריתם בלמן פורד על התרשים, כולל כל השלבים, תוך פירוט טבלאות הניתוב בכל קודקוד, ואת ההודעות הנשלחות (בציון מי שולח למי בכל שלב).

תשובה: הרוב ענו נכון. על טעויות בחישוב הורדו 1-4 נקודות בהתאם לכמות הטעויות. מי שהיה חסר לו שלב בתשובה, הורדו 1-4 נקודות. (סה"כ ישנם 4 שלבים).

ב. (5 נקודות) מהו תנאי העצירה של האלגוריתם?

תשובה: ישנה התייצבות כאשר בשלב כלשהוא, לא נוצר מינימום חדש באף שורה בכל הטבלאות. כלומר, לא נמצא אף מסלול טוב יותר ממה שידוע לנו עד כה.

ג. (5 נקודות) מהם המקרים בהם קודקוד צריך לשלוח הודעה לקודקוד שכן?
תשובה: ישנם שני מקרים:

1. כאשר נוצר מינימום חדש בשורה, כלומר מצאנו מסלול קצר יותר ממה שהיה ידוע עד כה.

2. כאשר משתנה משקל של צלע ישירה.

ד. (3 נקודות) נניח כי הצלע בעלת משקל 9 שונתה להיות בעלת משקל 0. האם ניתן להמשיך ולהשתמש באלגוריתם במצב כזה?

תשובה: ניתן להמשיך להשתמש באלגוריתם, משום שאלגוריתם בלמן פורד פועל כל עוד אין מעגלים שליליים בגרף. (כלומר גם צלעות שליליות אפשריות, ובפרט 0 שהינו חיובי).

ה. (7 נקודות) הסבר מהו poisoned reverse ואיזו בעיה הוא בא לפתור.

תשובה: זהו שכלול של האלגוריתם שנועד למנוע מעגלים (routing loops) באורך 2. הגדרנו אותו בצורה הבאה: קודקוד שלומד על מינימום חדש, ישלח את ההודעה לכולם, למעט הקודקוד השכן שדרכו המסלול החדש יוצא. לקודקוד זה "נשקר" ונשלח את המסלול השני המינימלי.

ו. (3 נקודות) הסבר מהו החיסרון של poisoned reverse (כלומר באילו מקרים הוא לא פועל).

תשובה: כפי שצוין בסעיף הקודם, יתכנו מעגלים באורך יותר מ-2, שאותם poisoned reverse לא יפתור.

פרס התשובה המקורית: החיסרון הוא כאשר משקלי הצלעות הינם מספרים אי-ראציונליים ואז הפיתרון לא יפעל.

4. לגבי פרוטוקול Token Ring.

א. (5 נקודות) הסבר מדוע נקרא בשם זה.

תשובה: Ring מכיוון שהתחנות מחוברות ברשת בצורת טבעת. Token כי עוברת הודעה הנקרת token באופן מעגלי בטבעת המסדירה את רשות השידור.

ב. (5 נקודות) האם פרוטוקול זה תומך ב-broadcast? אם לא, הסבר מדוע. אם כן, הסבר כיצד.

תשובה: הפרוטוקול מדמה broadcast בצורה הבאה: כל תחנה מחוברת בקו נ"ץ לתחנה שאחריה. כאשר הודעה משודרת היא עוברת בין כל התחנות במעגל, כאשר כל תחנה שמקבלת frame מהתחנה שלפניה, מבצעת את השלבים הבאים: א. במידה והכתובת (destination address)

של החבילה הינו הכתובת שלה עצמה או כתובת broadcast היא מעביר את ההודעה לשכבת ה-network. במידה וכתובת ה-source address אינה הכתובת שלה עצמה, היא מעביר את החבילה לתחנה שאחריה בטבעת. אחרת, היא מפסיקה להעביר את ההודעה הלאה. כלומר, כל הודעה שנשלחת, עוברת את כל התחנות במעגל וחוזרת לתחנה שיזמה אותה.

ג. (7 נקודות) הסבר כיצד מתבצע סדר השידור בין התחנות.

תשובה: ישנו מחשב הנקרא monitor שאחראי לייצר את האסימון (token) כל פרק זמן מסוים. האסימון הינו הודעה המכילה header ללא data בעלת פורמט מסוים. המוניתור משדר את האסימון לתחנה שבאה אחריה והתחנות מעבירות אותו בטבעת לפי סדר הטבעת. כל תחנה המקבלת את המוניתור רשאית להחזיק בו למשך זמן מסוים הנקרא token holding time ובו היא רשאית לשדר מספר בתים ככל שתספיק. כך זכות השידור עוברת באופן שווה בין כל התחנות.

ד. (3 נקודות) האם כאשר תחנה משדרת בפרוטוקול זה יש לה דרך לדעת האם ההודעה הגיעה ליעד? אם כן, פרט כיצד. אם לא, פרט מדוע.

תשובה: כן. ישנו שדה ב- header הנקרא FS כלומר frame status. בתוכו ישנם שני ביטים: A ו- C. A מציין האם התחנה קיימת בטבעת, ו- C מציין, האם קיימת, וכן הצליחה לקרוא את השידור מהרשת. (יתכן מצב תיאורטי שהתחנה עמוסה ולא הצליחה לקרוא את השידור). במידה ושני הביטים הנ"ל דלוקים, אנו יודעים שהתחנה קיבלה את ההודעה בודאות. גם מי שהסביר את העיקרון ולא פירט את שמות השדות קיבל את הנקודות.

ה. (3 נקודות) מה קורה אם אחד המשתמשים מכבה בלילה את המחשב שלו המחובר לרשת? תשובה: כרטיס הרשת הינו חיצוני למחשב ומקבל את המתח הדרוש לפעולתו בצורה עצמאית. ולכן הרשת תמשיך לפעול.

פרס התשובה המקורית: הרשת תקרוס, ובבוקר יחפשו אותו המשתמשים העצבניים ויסגרו איתו חשבון.

ו. (5 נקודות) השווה בין היעילות בשידור של רשת Token ring לעומת Ethernet.

תשובה: בעומס נמוך Ethernet עדיפה משום שיהיו מעט התנגשויות, ואילו ב- TR – התחנות יאלצו לחכות זמן רב לאסימון לפני שיכולו לשדר. בעומס גבוה ל- TR ישנה עדיפות משום שרוב התחנות ישדרו בזו אחר זו ללא התנגשויות רבות שיקרו ב- Ethernet ויפחיתו מיעילות השידור.

ז. (5 נקודות) נניח שהינך hacker המעוניין לגרום נזק לרשת. ביכולתך לפגוע באחת התחנות ברשת. באיזה תחנה היית בוחר? מה היה קורה ברשת לאחר שתחנה זו היתה מפסיקה

לתפקד? כיצד מתגברים על בעיה זאת ברשת token ring?

תשובה: כמובן שנפגע ב- monitor. כך לא ייוצר האסימון, ולכן אף תחנה לא תוכל לשדר. לכן מוגדר standby monitor שמתחיל לפעול כאשר ה- Monitor קורס. בכל מקרה, אם תוך פרק זמן מסוים התחנות לא מקבלות את האסימון שם אחראיות ליזום תהליך של בחירת monitor חדש.