Communication Networks (0368-3030) / Spring 2011

The Blavatnik School of Computer Science, Tel-Aviv University

Allon Wagner

Rehearsal

את"א מועדים א+ב 2006

- ב - public key cryptography חשוב שמפתח ההצפנה הפומבי והפרטי יהיו שונים. נכון / לא נכון, נמק.
  - ברור! זה כל הרעיון
- משתמש רוצה לשמור מידע אודות קובץ שיאפשר לו לוודא שלא חלו בו שינויים. מה הכי מתאים?
  - הצפנה
  - פענוח
  - חתימה
  - Hash קריפטוגרפי

את"א מועדים א+ב 2006

- משתמש רוצה לשמור מידע אודות קובץ כך שרק הוא יוכל לקרוא את תוכנו. מהי הפרוצדורה המתאימה?
  - הצפנה
  - פענוח
  - חתימה
  - Hash קריפטוגרפי
- הסבר כיצד נוצרת התקפת DDoS.
  - ראינו בתרגיל
- האם firewall מגן מפני התקפת DDoS?
  - Firewall "קלאסי" לא יודע לעשות זאת – הוא יודע להבדיל בין תעבורה שהשרת מצפה לה (למשל שרת HTTP מצפה לקבל TCP SYNs על פורט 80) לכאלו שלא מצפים להן. הוא לא מכיל מנגנון שמנסה לאתר האם לקוח ששולח פקטה חוקית ותקינה הוא לגיטימי או חלק ממתקפת DoS.

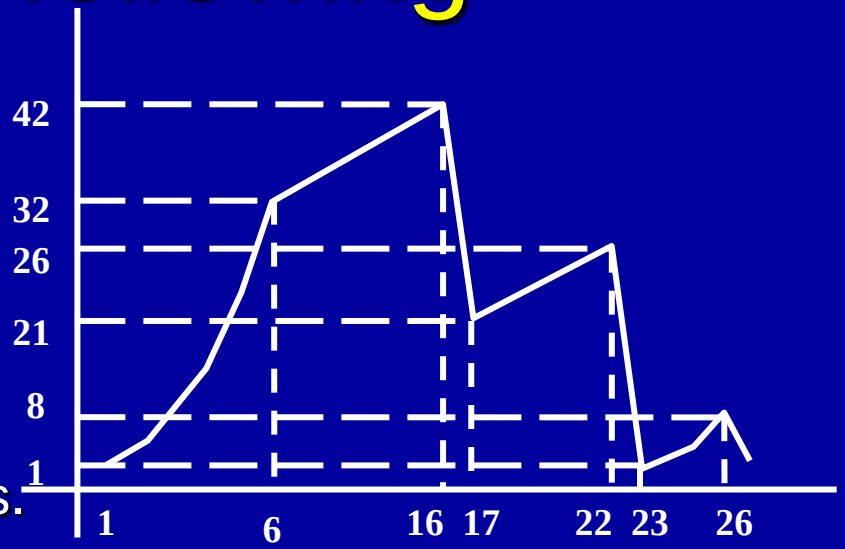
את"א מועדים א+ב 2006

- כדי לשמור על פרטיות הלקוחות מציעים להצפין את הכתובות בכל IP Header. האם זה יעבוד?
  - לא. כל ראוטר בדרך יצטרך להיות שותף להצפנה כדי לפענח את הכתובות ולדעת איך לנתב הלאה. בתשתית האינטרנט כיום אי אפשר לשלוט בצורה מלאה בנתיב שבו הפקטות יעברו.
- כדי לשמור על פרטיות הלקוחות מציעים להצפין את הפורטים בכל TCP header. פרט יתרונות וחסרונות
  - יתרונות: מספק מידה מסויימת של פרטיות, בייחוד מול מי שעושה רק header inspection (כמו חומרות שצריכות להתמודד עם הקצבים של ליבת הרשת)

את"א מועדים א+ב 2006

- כדי לשמור על פרטיות הלקוחות מציעים להצפין את הפורטים בכל TCP header. פרט יתרונות וחסרונות
  - חסרונות:
    - לא תורם כלום מול יריב שעושה deep packet inspection
    - עומס חישובי על ציוד הקצה
    - איך הלקוח מוצא את פורט השרת הנכון מלכתחילה? דורש תשתית לתיאום בין לקוח ושרת שאינם מכירים זה את זה בכל פתיחת session.

Answer the following



- Identify Slow Start rounds.
- Identify Congestion Avoidance rounds.
- At 16th round, is it timeout or triple duplicate ACK?
- At 22nd round, is it timeout or triple duplicate?
- What is the Slow Start Threshold at round 1?
- What is the Slow Start Threshold at round 24?
- If a packet loss is detected after the 26th round by the receipt of a triple duplicate ACK, what will be the value of the congestion-window size?

Answers

- First note: since we see here a loss event followed by CA state (rounds 16-17) we conclude this is not the Tahoe variant.
- On the other hand, the behavior given in the chart conforms to Reno's behavior (which is the only variant we studied other than Tahoe).
- Identify Slow Start rounds.
  - 1-6 and 23-26: where we see exponential increase of cwnd
- Identify Congestion Avoidance rounds
  - 6-16, 17-22: where we see linear increase of cwnd

Answers

- At 16th round, is it timeout or triple duplicate ACK?
  - triple dup: causes Reno to cut ssthresh and start again from CA (and, as said before, this can't be Tahoe; Tahoe returns to SS after every loss event).
- At 22nd round, is it timeout or triple duplicate?
  - timeout: causes both Reno and Tahoe to return to SS.
- What is the Slow Start Threshold at round 1?
  - We see that on round 6 we transitioned from SS to CA.
  - There are no loss events between rounds 1 and 6, so ssthresh of round 1 does not change (at least) until round 6.
  - Thus, ssthresh of round 1 is 32.

Answers

- What is the Slow Start Threshold at round 24?
  - Every loss event causes ssthresh to become half the size of cwnd on the time the loss event was detected (by timeout or 3rd dup ack).
  - Thus, ssthresh on round 23 is 26 / 2 = 13.
  - There is no loss in round 23 so this is also the thresh of round 24.
- If a packet loss is detected after the 26th round by the receipt of a triple duplicate ACK, what will be the value of the congestion-window size?
  - Again, we set ssthresh to half the size of cwnd on the time the loss event was detected, namely 8 / 2 = 4.

את"א מועד א 2002

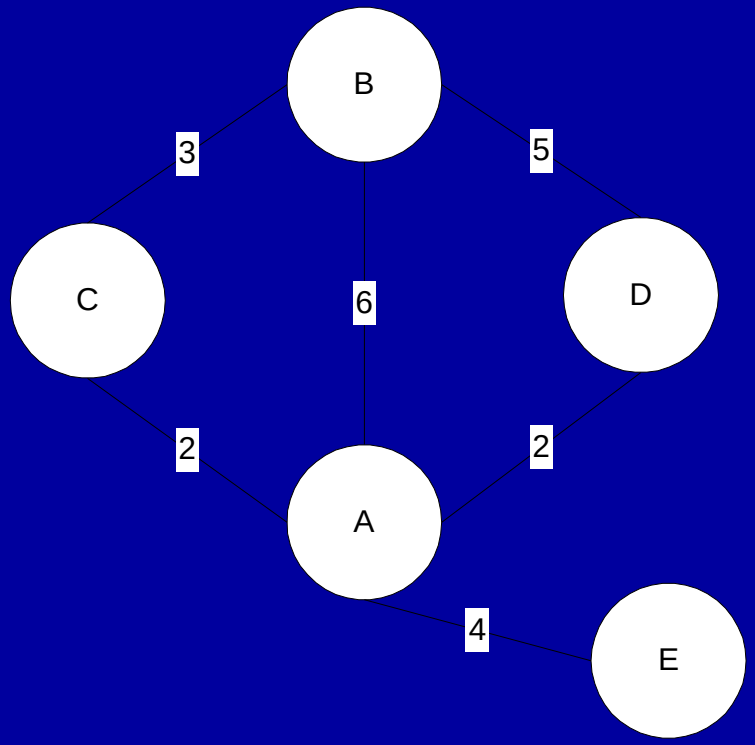
- תן דוגמה למצב שבו receiver שולח הודעת TCP עם receiver window = 0
  - זו שאלה על TCP Flow control
  - השולח "מציף" את המקבל במידע, והאפליקציה במקבל לא קוראת את המידע הזה בקצב מהיר מספיק
  - ה – buffer של המקבל מתמלא, ואז הוא שולח rwnd = 0
  - **<u>פיתוח לשאלה:</u>** נניח שאין למקבל שום דבר לשלוח. הוא לעולם לא ישלח חלון מעודכן! (כי לא יווצרו acks חדשים, כי השולח לא שולח כלום). מה עושים?
  - זו הסיבה ש – TCP אומר שגם אם rwnd = 0 השולח מגשש וכל כמה זמן שולח בית אחד של מידע חדש. אם התפנה מקום אצל המקבל, A יקבל ack עם rwnd מעודכן והקישור יחזור למצב נורמלי.

את"א מועד א 2002

- האם ייתכן שפקטת IP תעבור דרך אותו router יותר מפעם אחת במסלול שלה?
  - כן – אם יש לולאה ברשת ולכן הפקטה תמשיך לעבור בלולאה הזו עד אינסוף
  - ראינו ששדה ה – TTL ב – IP Header מונע מפקטה שמסתובבת בלולאה לחיות ברשת לנצח
  - ראינו דוגמה להווצרות לולאה ברשת במהלך ההתכנסות של פרוטוקול DV לניתוב (אפילו אם משתמשים ב – poisoned reverse)

Routing Tables

- Consider the following network running the distance vector routing protocol. In the diagram, vertices represent routers and edges (arcs) represent links between routers. The numerical annotation on the links represents link costs. Higher costs indicate worse links
  - Show the routing table at node A when the distance vector routing algorithm stabilizes
  - Suppose the link between node A and node E fails. Will the algorithm stabilize in this case?



Via →	B	C	D	E
B	6	**5**	7	13
C	9	**2**	6	10
D	11	6	**2**	10
E	15	8	8	**4**

Assuming no split horizon/poison reverse

Via→	B	C	D	E
B	6	**5**	7	∞
C	9	**2**	∞	∞
D	11	∞	**2**	∞
E	∞	∞	∞	**4**

With split horizon/poison reverse

CSMA

- נתונה רשת CSMA|CD עם N תחנות. נניח שנמצא מנגנון מופלא שיקבע, עבור כל התנגשות, בדיוק כמה תחנות שידרו ותרמו לאותה התנגשות.

א. נניח מתרחש התסריט הבא:

  - מספר התחנות שתרמו להתנגשות הוא X
  - בחריץ (SLOT) הזמן הבא כל אחת מהן תשדר בהסתברות 1/X
  - אף אחת משאר התחנות לא תשדר באותו חריץ.

- מה ההסתברות לשידור מוצלח בחריץ (SLOT) הזמן שלאחר ההתנגשות ? הסבר!

- תשובה סופית: $\left(1-\frac{1}{X}\right)^{X-1}$
- כדי שתחנה אחת מתוך ה-X תצליח לשדר, היא צריכה להחליט לשדר ולקוות שהאחרות לא ישדרו.
  ההסתברות לכך היא $\frac{1}{X}\left(1-\frac{1}{X}\right)^{X-1}$
- כדי שתחנה כלשהי תצליח לשדר, צריך להתקיים אחת מ-X מאורעות זרים, שההסתברות של כל אחד מהם היא כלעיל

ב. נניח מתרחש התסריט הבא:

- מספר התחנות שתרמו להתנגשות הוא X
- בחריץ (SLOT) הזמן הבא כל אחת מהן תשדר בהסתברות 1/X
- בחריץ הזמן הבא **אחת** מהתחנות שלא השתתפו בהתנגשות תשדר תמיד (בהסתברות 1)

- מה ההסתברות לשידור מוצלח בחריץ (SLOT) הזמן שלאחר ההתנגשות ? הסבר!

- תשובה: $\left(1-\frac{1}{X}\right)^X$

- מבין מי שלא השתתף בהתנגשות, יש בדיוק תחנה אחת שמשדרת.
- לכן השידור מצליח אם"ם כל X התחנות שכן השתתפו בהתנגשות לא ישדרו.

ג. נניח מתרחש התסריט הבא:

- מספר התחנות שתרמו להתנגשות הוא X
- בחריץ (SLOT) הזמן הבא כל אחת מהן תשדר בהסתברות 1/X
- בחריץ הזמן הבא **שתיים** מהתחנות שלא השתתפו בהתנגשות ישדרו תמיד (בהסתברות 1)

- מה ההסתברות לשידור מוצלח בחריץ (SLOT) הזמן שלאחר ההתנגשות ? הסבר!
- תשובה: 0, כבר יש התנגשות אם שתים משדרות.