

## תרגיל בית עיוני מס. 4

להגשה עד 28/1/2009

### הקדמה

- שימו לב, תרגיל זה קטן בהיקפו מהרגיל, והזמן המוקצה לו קטן בהתאם.

### א. Sliding Window

- נתונים הרצפים הבאים של sequence numbers עבור הודעות שיוצאות מתחנה כלשהי (יש לקרוא משמאל לימין):
  - 1, 1, 0
  - 7, 1, 1, 0
  - 7, 0, 1
  - 7, 0, 1, 1, 0עבור כל אחד מהרצפים – באיזה פרוטוקול מבין Stop-and-Wait, Go-back-N, Selective Repeat הוא אפשרי? מה יכול להיות טווח ה-sequence numbers?

### ב. Congestion Control

- אנחנו מעבירים ב-TCP קובץ בגודל 64K. נניח שלחיבור ה-TCP שלנו יש את הפרמטרים הבאים:
  - Reno – Congestion control
  - 2Kb – MSS
  - 1 MSS – תחילי cwnd
  - 32K – תחילי ssthreshold
  - 40 msec – timeout (קבוע)
  - 20 msec – RTT (קבוע)
  - חלון הקבלה גדול מאד.
  - חבילה שמגיעה מחוץ לסדר מושמטת.
  - כל חבילה שמינית משודרת, הולכת לאיבוד, פרט לכך הערוץ אמין לגמרי.
  - פרטו את סבבי השידור (מהו cwnd בכל סבב). תוך כמה זמן יסתיים השידור?

### ג. RSA

- קודדו ב-RSA עם המספרים הראשוניים  $p=3$ ,  $q=11$  את ההודעה "NETWORK". הניחו שהמחרוזת מקודדת בקידוד ASCII. ניתן להיעזר בכל כלי עזר לביצוע חישובים במספרים גדולים, אך יש לפרט בתשובה את כל החישובים שבוצעו.