~~10/12/19~~

24/11/2020

בקרת רשתות - הרצאה 6

* תזכורת - טאבו פוסטר - ליאפונוב

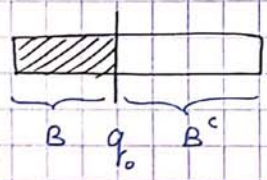
תהי $\{X_k\}$ שרשרת מרקוב אי-פריקה ולא מתנודדת (כלומר קיימת והסתברות מעברים סטציונרית והתפלגות אלא בורגאלית). מרחב מצבים $\hat{S}$.

ונניח קיימת פונקציה $V: \hat{S} \to R^+$ ומקבוצה סופית $\hat{B} \in \hat{S}$ שמקיימים:

1) $E\left[\overbrace{V(X_{k+1}) - V(X)}^{drift} \mid X_k = x\right] \leq -\varepsilon$ if $x \in \hat{B}^c$ for some $\varepsilon > 0$

2) $E\left[V(X_{k+1}) - V(X) \mid X_k = x\right] \leq A$ if $x \in \hat{B}$ for some $A < \infty$

$\Leftarrow$ אזי השרשרת "תוצרת היובית" (כלומר בזמן סופי נחזור לאזור מצב).



* אלגוריתם מקסימום משקל (תזכורת) - בכל רגע t נבחר לשדר

למשתמש i שמקיים:

$$\boxed{i = \underset{\{j\}}{\arg\max}\ C_{m(t),j} \cdot q_j(t)}$$

קיבול של משתמש j במצב $m(t)$

כמה פקטות יש בתור j בזמן t

* נרצה להראות שמקס משקל מקיים יציבות אופטימלית.

הערה: בעבר הראינו שאם קצבי הגעה אינם באזור הקיבול אזי אין אלגוריתם שיתמוך בהם. כעת נראה שאם קצבי הגעה בתוך אזור הקיבול אזי אלגוריתם מקסימום משקלותן סכום תורים שהיא שרשרת חוזרת חיובית ולכן תומך בהם.

* נרצה להראות שרשרת מרקוב $q(t) = \sum_j q_j(t)$ הינו תוצרת היובית

$$\boxed{\lim_{D \to \infty} \lim_{t \to \infty} P_r\left(|q(t)| > D\right) = 0} \longrightarrow \text{יציבות אופטימלית}$$

given q(t)=q

* Lema: נניח $q(t) = q$ ותחת מקס משקל מתקיים: $E\left[\sum_i q_i \mu_i(t)\right] \geq \sum_i q_i \gamma_i$ for all $\gamma \in C$

קצב שירות i קיבל

$$\gamma_i = \sum_{m=1}^{M} \alpha_{m,i} \cdot C_{m,i} \cdot \pi_m$$

הוכחה על הלוח...

נניח $q = q(t)$ מתאר מדיניות-משקל עמיתים: $E\left(\sum_i q_i r_i(t)\right) \geq \sum_i q_i \gamma_i$ $\forall \hat{c}$

הוכחה:

מהגדרה של $\hat{c}$, לכל $\hat{c}$ קיים α כך ש: $\gamma_i \leq \sum_{m=1}^{M} \alpha_{m,i} c_{m,i} \pi_m$.

לכן:

$$\sum_i q_i \gamma_i \leq \sum_i q_i \left(\sum_m \alpha_{m,i} c_{m,i} \pi_m\right) = \sum_m \pi_m \left(\sum_i q_i \alpha_{m,i} c_{m,i}\right) \underset{\sum_i \alpha_{m,i} \leq 1}{\leq} \sum_m \pi_m \left(\max_i q_i c_{m,i}\right) \quad (*)$$

מקרה 2 בלבד מאמרנו משקלים

(7-1)

כאשר נשלח מדיניות-משקל כמתכים את הנשאים $q_i c_{m,i}$ המקסימלי ולכן:

$$E\left(\sum_i q_i r_i(t)\right) \underset{\uparrow}{=} \sum_{m=1}^{M} \pi_m \left(\max_i q_i c_{m,i}\right) \underset{(*)}{\geq} \sum_i q_i \gamma_i$$

$r_{i^*} = c_{m,i^*}$ כאשר i^* שאותו מקבל כל הכי הרבה.

$i \neq i^*$ מקבלים כל הכי אפס.

$c(t) = c$, $q(t) = q$ לשמן

והוכחנו את הלמה.

* נרצה להוכיח $q(t)=\sum_j q_j(t)$ שרשרת מרקוב חוזרת חיובית.

נמשיך בהוכחת הטענה:

נגדיר פונקציית ליאפונוב $V(q(t)) = \sum_{i=1}^{N} q_i^2(t)$

נחשב את ה-drift:

$$E\left[V(q(t+1)) - V(q(t)) \,\middle|\, q(t)=q\right] = E\left[\sum_i \left(q_i^2(t+1) - q_i^2(t)\right) \,\middle|\, q(t)=q\right]$$

$$= E\left[\sum_{i=1}^{N} \left(\left[q_i(t)+a_i(t)-\mu_i(t)\right]^+\right)^2 - q_i^2(t) \,\middle|\, q(t)=q\right] \leq$$

$$\leq E\left[\sum_{i=1}^{N} \left(q_i(t)+a_i(t)-\mu_i(t)\right)^2 - q_i^2(t) \,\middle|\, q(t)=q\right]$$

$$= E\left[\sum_{i=1}^{N} \left(a_i(t)-\mu_i(t)\right)^2 + 2q_i(t)\left(a_i(t)-\mu_i(t)\right) \,\middle|\, q(t)=q\right]$$

נשתמש בלינאריות בתוחלת ובמרכז שנתן ונקבל

$$= \underbrace{E\left[\sum_{i=1}^{N} \left(a_i(t)-\mu_i(t)\right)^2 \,\middle|\, q(t)=q\right]}_{\mathrm{I}} + 2\sum_{i=1}^{N} q_i \Big(\underbrace{\lambda_i}_{E(a_i)} - \underbrace{E\left[\mu_i(t) \,\middle|\, q(t)=q\right]}_{\mathrm{II}}$$

(I) $$E\left[\sum_{i=1}^{N} a_i^2(t) - 2a_i(t)\mu_i(t) + \mu_i^2(t) \,\middle|\, q(t)=q\right] \leq$$

$$\leq \sum_{i=1}^{N} \underbrace{\sigma_i^2 + \lambda_i^2}_{E(a_i^2)} + C_{max}^2$$

(II) $$\sum_i q_i E\left[\mu_i(t) \,\middle|\, q(t)=q\right] \underset{\text{Lema}}{\geq} \sum_i q_i (1+\varepsilon)\lambda_i$$

$(1+\varepsilon)\lambda_i \in \hat{C} \quad \forall \varepsilon > 0$

(סדר גודל בדיוק הנקבל)

$$E\left[V(q(t+1)) - V(q(t)) \,\middle|\, q(t)=q\right] \leq \overbrace{\sum_{i=1}^{N} \sigma_i^2 + \lambda_i^2 + C_{max}^2}^{A} - 2\varepsilon \sum_{i=1}^{N} q_i \lambda_i$$

we can choose finite q_0 sufficiently large such that:

$$\leq \begin{cases} -\tilde{\varepsilon} & , q > q_0 \\ A & , q \leq q_0 \end{cases}$$

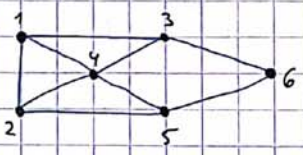
$\Leftarrow$ שרשרת חוזרת חיובית לפי פרסלר-ליאפונוב

$\Leftarrow$ מרקוביאנים משקל מקיים ניצבות מרקוביאנית/חיובית.

10/12/19

BS → users : download אך לרשתות הורדות על ישות

ניתן להרחיב את המודל לגבול הפרעות



כל צומת מייצג לינק

* הרעיון כללי נרצה לשדר על יצי לינקים שבה לו שכנים (שכנות פיזית ולכרות הפרעה הדדית)

מקסימום משקל בהקבה זה יהיה בכל רגע את הלינקים המקיים $\sum_i q_i \mu_i$ מקסימלי.

מקיים ניצולת אופטימלית.

* ישנו אלגוריתם מבוזר שקרוי Q-CSMA

Queue - Carrier Sensing Multiple Access

ניתן להוכיח שהוא מתכנס אוטומטית למקס-משקל.

הצפנה

הצפנה ישומית

אפליקציה ← presentation layer ← הצפנה

תעבורה

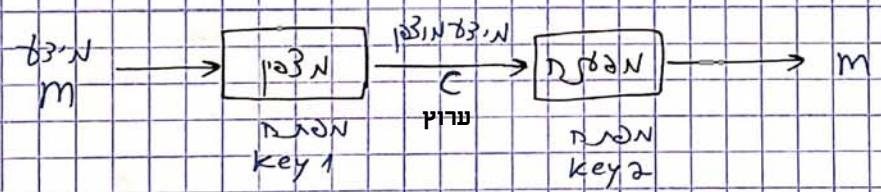
רשת

לינק (MAC)

Cipher text = C

message = m

הערוץ פתוח.



נושאי יסוד

1) השיטה של ההצפנה וההפענוח ידועה (קיימים תקנים)

2) נרצה מערכת לתקשורת תחת יכולת שיטת ההצפנה וההפענוח הוא ניתנת להשגה כי המפתחות אינם ידועים.

(קיימים תקנים גם למפתחות אך הערך המספרי אינו ידוע)

סוגי התקפות

1) **סקס מוצפן בלבד** - נרצה מערכת שמידע בפני מתקיף שיודע את C

כך שלא יוכל לחלץ את המפתח ואת ההודעה.

דוגמה: הצפנה פרמוטציה של אותיות

* צופן ויג'נר (Vigener Cypher) **כל אות מחליפים באות במרחק מסוים:**

a b c d e f g h i j k l m n o p q r s t u v w x y z

למשל נתון מפתח בגודל 4

$$\begin{matrix} m & & c \\ \begin{bmatrix} h \\ o \\ m \\ e \end{bmatrix} & \longrightarrow & \begin{bmatrix} i \\ r \\ o \\ l \end{bmatrix} \end{matrix} \qquad \begin{bmatrix} 1 \\ 3 \\ 2 \\ 7 \end{bmatrix}$$

זהו מפתח רב-אלפבית. מרחקים לא קבועים

* שיטת קסיסקי לשבירת הצופן (kasisky)

נתבסס תכונת של הצפנים כדי לגלות את גודל המפתח

$$\underbrace{ABC \cdots\cdots}_{r-|k|}\ \underbrace{ABC \cdots\cdots}_{j-|k|}\ ABC$$

נגלה את k

נפתח שיטה סטטיסטית לגלות את סדר המפתח.

למשל "יתרונות שפה טבעית".

דוגמא נוספת

$$\begin{cases} m = \text{וקטור בינארי באורך } n \\ k \text{ מטריצת מפתח} \end{cases}$$

$$(m)(k) = (c)$$

$$(c)(k^{-1}) = (m)$$

המשך סוגי התקפות

(2) יכולת לקסט עבור (m)

הנחה ל-c גם m יכולה

מניחים שמתקיים יכולה הרבה צורות (m,c)

למשל בדוגמה של המטריצה $(m)(k) = (c)$ $k \in R^{n \times n}$

במטריצה k יש n^2 נעלמים

מכל זוג (m,c) נוכל לבנות n משוואות

אם יש לי n זוגות (m,c) נוכל לשבור את הצופן.

10/12/19

סוגי התקפות

3) טקסט נבחר בתור

התוקף יכול לבחור איזה צמד (m,c) לקבל

* תכונה נוספת שנרצה: אלגוריתם "מפתח השלם"

אם יש שני m שונים המקבלים אותו c נרצה ש-c שלהם

יהיו שונים מאוד. כלומר לכל שינוי ב-k

לאותו הטקסט המוצפן צריכה להיות מאוד לא לינארית.

הצפנה מושלמת (perfect secrecy) Shannon 1940

1) גודל המפתח כגודל הטקסט
2) מפתח אקראי לגמרי
3) מפתח חד פעמי
4) השיטה תהיה XOR ביט-ביט בין ההודעה למפתח בהצפנה ובפענוח.

בעיות: הצורך לזכור מספרים, המפתח גדול מאוד.

הצפנה סימטרית ואסימטרית

* סימטרית: $k_1 = k_2$ אם ניתן לבצע מפתח אחד לפי השני (למשל: ובאופן יותר כללי:)
* אסימטרית: לפתוח את אחד והמפתחות לא ניתן לגזור.

הדרכה קושי בשבירת מפתח

$$m \longrightarrow \boxed{\text{הצפנה}} \xrightarrow{k} c$$

גם יודעים צמד (m,c) ניתן לגזור את k על ידי Brute Force

עבור על כל האפשרויות של המפתח k עד שנגיע

הסיבוכיות תלויה בכל שגודל המפתח גדול. סטנדרט: 128 bit או יותר

במקרה זה צריך לבדוק 2^{128} אפשרויות!

דרישה לשבירה של מפתח שלם:

* לא נרצה שיהיה אפשר לשבור את המפתח בחלקים.

כי אז הסיבוכיות לינארית במספר החלקים.

הצפנה סימטרית

Data Encrypting Standart	(1976)	DES	(1)
Advanced Encryption Standart	(2000)	AES	(2)

Subtitution	(S)	**התמרה**
Permutation	(P)	**פרמוטציה**

אנו נתמקד ב AES

חוזרים על תהליך התמרה ופרמוטציה על המידע.

כללים מתמטיים נדרשים:

- **XOR**: כי XOR הוכנס לדוגמא:

M	K	C
0	0	0
0	1	1
1	0	1
1	1	0

$\Rightarrow$

C	K	M
0	0	0
1	0	0
1	0	1
0	1	1

$M \oplus K = C \Rightarrow C \oplus K = M$

- **מודולו**

נתבקש בתרגיל בלינגמן: $x^7+x^5+x^4+x^3+1 \bmod x^4+1$

נבצע כך:

$$
\begin{array}{l|l}
 & x^3 + x + x^0 \\
\hline
x^7+0\cdot x^6+x^5+x^4+x^3+0\cdot x^2+0\cdot x^1+x^0 & x^4+1 \\
-\ x^7 \qquad\qquad +x^3 & \\
\hline
x^5+x^4 \qquad\qquad +x^0 & \\
-\ x^5 \qquad\qquad +x^1 & \\
\hline
x^4 \qquad -x^1+x^0 & \\
-\ x^4 \qquad +x^0 & \\
\hline
-x^1 &
\end{array}
$$

כיבלנו: $x^3+x^1+x^0+\dfrac{-x^1}{x^4+1}$

נעדיף השארית תמיד $\underline{\underline{-x}}$. כשארית לכל הוויתר בתרגיל x^3 מעיין אבל תקרה אבל זה יתן את 3 מעלה ולא יהיה כשבר.

$$
\begin{array}{l|l}
 & x^3 \\
\hline
x^7+x^3 & x^4 \\
x^7 & \\
\hline
x^3 &
\end{array}
= x^3 + \frac{x^3}{x^4}
$$

שארית

דרך נוספת

חזרה נוספת: שדה גלואה $GF(2^8)$

Galois Field

כלומר 8 קבוצת: $x^0, x^1, \dots, x^7$

$GF(2^8) \Rightarrow$ קבוצת כל הפולינומים מעל 2 ופחות עם מקדמים בינאריים

ישנם 2^8 פולינומים כאלו (כי:

2^8 אפשרויות

שדה - קבוצה אלגברית שניתן לבצע עליה פעולות חשבוניות

(קבוצה בה סגורה תחת פעולה כלשהי. (חיבור, חיסור, כפל וחילוק)

דרוש להגדיר חיבור, חיסור, כפל וחילוק.

לפי גלואה: חיבור = חיסור. בא XOR על וקטורים בינאריים

כפל: שני ביטים שמוכפלים דרך לקבל ביט.

$g(x)$ - פולינום יחיד של הדרגה מעולה 8 (הוא קבוע)

אם a, b הם אלמנטים של שדה, הגדרה על הכפל:

$$a \cdot b \triangleq a \cdot b \bmod g(x)$$

וכך נקבל פולינום מעולה 7

(הערה: ~~אחרת~~ ענית $c = a \cdot b \Rightarrow a = c \cdot b^{-1}$)

כאן הלוקח ב- b.

נדון על הנכונו מודולו בהמשך)

17/12/19

הצפנות רשתות - הרצאה 7

* שבוע שעבר דיברנו על הצפנה ישראלית.

הצפנה סימטרית

פרוטוקול AES (Advanced Encryption Standart)

* יעיל בהרבה מהקודם
* אורך מפתח בחלק: 128, 192, 256
* עושה שימוש ברעיון פעולות S, P (Substitution, Permutation)
* עובד על מערך בתים (לפי עמודה) Column Major order $4 \times N_b$

למשל עבור המערך $[b_0, b_1, \dots, b_{15}]$ נעבור כך:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

* יש כמה סיבובים, בכל סיבוב משתמשים

שלבי עיבוד להמרה plain text (טקסט מקורי). ל- Cyper text (טקסט מוצפן). **שתלויים במפתח.**

* הנלמדים נרשמים בסדר הפוך במפתח כדי לתאר לטקסט המקורי.

* עובדים בשדה גלואה $GF(2^8)$: כל הפולינומים עד דרגה 7.

$\underbrace{0/1 \ \cdots \ \cdots \ 0/1}$

$0/1 \to$ מקדם של x^7, $0/1 \to$ מקדם של x^0

* **צופן ריינדל** נגדיר:

$$A(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + \dots + a_0x^0$$

$$a_i \in GF(2) \ \cancel{\{0,1\}} = \{0,1\}$$

פעולה חיבור: XOR $\quad C(x) = A(x) + B(x) = \sum_{i=0}^{M-1} (a_i \oplus b_i) x^i$

פעולה כפל: $\underbrace{P(x) = x^8 + x^4 + x^3 + x + 1}$ $\quad C(x) = A(x) \cdot B(x) \bmod P(x)$

פולינום יחיד שמוגדר בתקן AES.

דוגמה למימוש בפועל של כפל פולינומים:

$A(x) = (x^6 + x + 1)$, $B(x) = (x^2 + 1)$

$$C(x) = A(x)B(x) = (x^6 + x + 1) \cdot x \cdot x + (x^6 + x + 1)$$

$$= \underbrace{(x^8 + x^3 + x^2)} + \underbrace{(x^6 + x + 1)}$$

$\underbrace{1}_{\text{overflow}}00001100$

בהגעה נכפל על יד חיסור ואחר כך נחבר

$$(x^8 + x^3 + x^2) - (x^8 + x^4 + x^3 + x + 1) = x^4 + x^2 + x + 1$$

$$(x^4 + x^2 + x + 1) + \underbrace{(x^6 + x + 1)} = x^6 + x^4 + x^2 \quad 01010100$$

האלגוריתם

נרית בלוק של טקסט

נוסדר במטריצה של $4 \times N_b$ כל איבר במטריצה הוא byte.

* שלב I - התמרה (S)

כל byte במטריצה מוחלף ב- byte אחר לפי lookup table

המבלה התמרה מתאימה לכל אחד מ- 256 מרכיבים.

- פעולה הפוכה נעשית ע"ל המפתח.

* שלב II - פרמוטציה (P)

הזזה מעגלית של השורות בהתאם לסטנדרט (תלוי בגודל הבלוק)

- פעולה הפוכה נעשית ע"ל המפתח.

* שלב III Mix Column

מכפילים כל עמודה במטריצה בפולינום קבוע $C(X)$ ומקבלים

מטריצה עם עמודות חדשות

- המפתח מבצעים פעולה הפוכה.

* שלב IV - הצפנה

הוספת מטריצה נגזרת תלויה מפתח: לוקחים מפתח בגודל

הבלוק ומבצעים XOR איבר-איבר (בשכל איבר הוא byte)

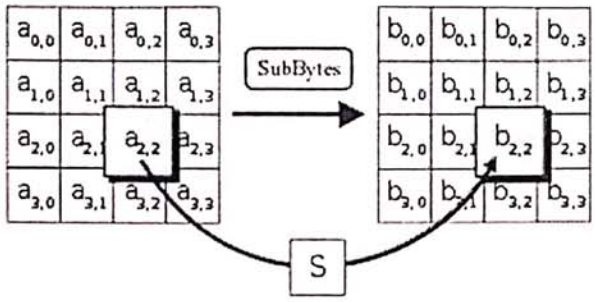
- כאן המפתח צריך לדעת את המפתח הסודי בשביל פענוח

בעיה מרכזית בהצפנה סימטרית: צריך להפיץ מפתח סודי

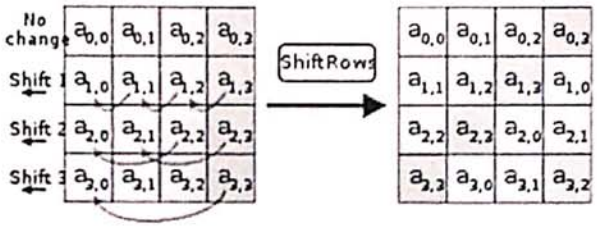
בערוץ מאובטח

AES אלגוריתם ריינדל

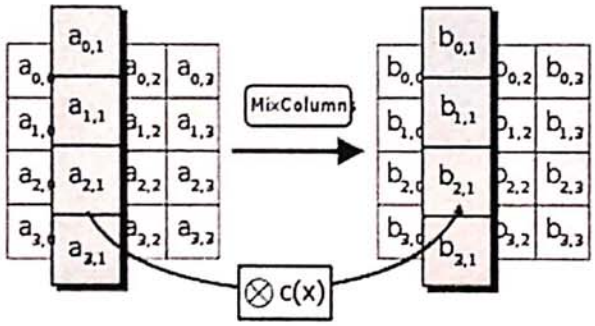
Step 1:



Step 2:



Step 3:



Step 4: