**בטיחות ברשתות – עבודת גמר  
  
*An Efficiency-Boosting Client Selection Scheme for Federated Learning With Fairness Guarantee***

**תוכן עניינים**

**תקציר 3**

**הקדמה** **4**

**מודל המערכת וניסוח הבעיה** **7**

**פתרונות לבעיה13**

**תוצאות סימולציה18**

**מסקנות וביקורת על המאמר 28**

**נספחים29**

**סימוכין 30**

**תקציר**

בעקבות קצב התפתחותה המהיר של הבינה המלאכותית והתלות הגוברת בכמויות הגדולות של המידע שהיא צורכת, נוצרה בעיה מהותית בשמירה על פרטיות המידע בתהליך האימון ומניעת זליגת מידע רגיש תוך שימוש במערכות לימוד מרוכזות.  
  
על מנת להתמודד עם הבעיה זו, נוצרה סכמת לימוד מבוזרת חדשה – Federated Learning   
(לימוד מאוחד) המאפשרת אימון מבוזר על ידי מספר לקוחות במקביל, כל לקוח מתאמן בצורה לוקאלית.  
שיטה זו מאפשרת לכל לקוח לשמור את המידע הפרטי שלו אצלו ולפרסם לשרת מתכלל רק עדכונים שוטפים הרלוונטיים לתהליך הלימוד, העדכונים החלקיים מכל הלקוחות מאוגדים יחד לכדי עדכון כולל (אגרגציה) שממנו ניתן להסיק תוצאות או להמשיך לסבב אימון נוסף.  
  
כאמור, הלימוד המאוחד מושתת על מערכת מבוזרת הכוללת בתוכה שרת מתכלל שמטרתו להפיץ את המודל ולאסוף עדכונים, ומספר (לעיתים רב של) לקוחות שמבצעים אימון ושולחים את אותם עדכונים. לכן, על מנת שהלימוד יוכל להתקיים יש להקים ערוץ תקשורת בין השרת לבין הלקוחות.   
  
מכיוון שערוץ תקשורת מתאפיין ברוחב פס חסום, רשת לימוד מאוחד מבוזרת אינה יכולה להכיל יותר ממספר סופי של עדכונים בתהליך אימון מסוים, לכן, ישנה חשיבות רבה לאופן בו שרת בוחר את צמתי האימון שבהם הוא נעזר, הן מבחינת אפקטיביות האימון ואיכות המודל והן מבחינת הוגנות הבחירה כלפי משתמשי הקצה.  
  
השאיפה היא למצוא שיטה בה רשת הלימוד המאוחד יכולה לאפשר תהליך למידה תקין, כלומר, עם אחוזי דיוק טובים לפחות כמו תהליך אימון מאוחד סטנדרטי, ובנוסף, השיטה צריכה לכלול מנגנון הבטחת הוגנות בו לא יתקיים מצב שלקוח מסוים מבצע אימון במספר סבבים גדול משמעותית מלקוח אחר   
(לא יתקיים מצב של הרעבה או ניצול יתר של לקוח מסוים).   
  
המאמר שאותו ננתח מציע אלגוריתם בשם F-RBCS לבעיית בחירת הלקוחות בתהליך הלימוד המאוחד.  
האלגוריתם מבטיח הוגנות תוך אופטימיזציה של בעיית Lyapunov בבחירת הלקוחות ובנוסף על ידי שימוש במידע מקדים מסבבי לימוד קודמים, משערך בעזרת התבססות על שיטת את זמן שליחת המודל בין כל לקוח לשרת ובכך בוחר לקוחות בצורה מיטבית בכל סבב לימוד.  
תוצאות הניסויים במאמר אף מוכיחות את ההשערות התיאורטיות ומראות שגודל החרטה – המרחק בין תוצאות הלימוד בשימוש באלגוריתם ביחס לאלגוריתם אופטימלי, חסומה ממש על ידי מספר סופי קבוע. מסקנות מהמאמר אף מראות ששמירה על בחירה הוגנת אינה משרתת רק את הלקוחות, אלא משפרת את הלימוד כתוצאה מהגדלת שונות דגימות המידע שמונעת Overfitting (אימון יתר) על מידע ספציפי וגורמת להטיות בתוצאות הלימוד.

**הקדמה**

**תיאור הבעיה:**

אחד הנושאים החמים ביותר כיום הוא בינה מלאכותית, משימות מסובכות למידול לצד פעולות יומיומיות סטנדרטיות הולכות ונעשות אוטומטיות על ידי מכונות חכמות שיכולות ללמוד ולהשתפר כתוצאה מניתוח הקלט שהן מקבלות.  
  
חלק קריטי מתהליך הלימוד של אותן מכונות הוא גישה למידע, כדי שמכונה חכמה תוכל לבצע את הפעולות שהיא מתבקשת לבצע בצורה הטובה ביותר עליה לקבל כמויות גדולות מאוד של מידע.   
התלות במידע נובעת מהצורך של המכונה להתאמן (training), ללא קלט חדש אין ביכולתה של מכונה חכמה ללמוד ולהעריך את ביצועיה (אחוזי שגיאה, שיטות ניקוד וכו'), רק כך תוכל להשתפר.  
  
כיום מידע נחשב לאחד המשאבים היקרים ביותר, לכן היכן שנמצאת כמות גדולה ממנו ימצאו גם אנשים שירצו לנסות להדליף ולגנוב אותו. עקב החשש הגדול בנושא, שלעיתים אף יכול להגיע עד כדי גניבה של מידע רגיש כגון מסמכים, פרטים אישיים, מסלולי נסיעה קבועים וכו' נוצר משבר גדול בתחום הבינה המלאכותית הנקרא Isolated "data island". כאשר המידע הרלוונטי ללימוד צריך להתקבל מלקוחות שונים ברחבי הרשת ישנה סכנה כי במהלך שליחת המידע יהיו תוקפים שינסו להאזין לו או לגנוב אותו, סכנה זו מצמצמת את מספר הלקוחות שמעוניינים לתרום לתהליך האימון ובעצם יוצרת "אי בודד" של מידע לא נגיש. לכן, על מנת להתגבר על הבעיה יש לחשוב על פתרון שימנע מהמידע לנוע ברחבי הרשת.

פתרון אפשרי לבעיית ה - Isolated "data island" הוא Federated Learning (לימוד מאוחד).  
בשיטה זו שלב האימון של המודל אינו מתקיים אצל מכונה יחידה אלא אצל מספר רב של מכונות.   
מודל הלימוד המרוכז הופך למודל מבוזר שמסוגל למקבל לימוד על מידע חלקי בכל מכונה, ועל ידי שרת מתכלל שמבצע איחוד (אגרגציה) עדכונים שוטפים מהמכונות לכיוון השרת מאוחדים יחד לעדכון מאוגד שממנו ניתן להסיק מסקנות או להמשיך לסבב לימוד נוסף. השימוש בלימוד המאוחד מאפשר לכל לקוח לבצע לימוד מקומי במכונה שלו ולשלוח עדכונים שוטפים הרלוונטיים רק לתהליך הלימוד, כך המידע הרגיש שעליו מסתמך הלימוד לא מופץ החוצה לרחבי הרשת.

כעת, כאשר הבעיה הבטיחותית נפתרה נוצרת בעיה חדשה, כאמור, הלימוד המאוחד מתבסס על עדכונים שוטפים בין לקוחות לשרת מתכלל, עדכונים אלו צריכים לקרות בזמן אמת וגם להתבצע בסנכרון אחד עם השני מכיוון שלא ניתן להתחיל סבב לימוד נוסף לפני שכל הלקוחות מסיימים את סבב האימון המקומי שלהם. כלומר, שיטת הלימוד החדשה מחייבת הקמת ערוץ תקשורת בין השרת לבין הלקוחות ומכיוון שלכל ערוץ תקשורת יש רוחב פס סופי שמוקצה לו, ובפרט מכיוון שהלימוד קורה בזמן אמת ישנו מספר מוגבל של לקוחות שיכולים להשתתף בתהליך הלימוד המאוחד.   
  
מטרת המאמר היא לפתור את בעיית בחירת זהותם של המשתתפים בלימוד המאוחד על ידי אלגוריתם לבחירת משתתפים שרץ (בתיאוריה) לפני כל סבב אימון ושמו F-RBCS. האלגוריתם מתבסס על אלגוריתמי אופטימיזציה ושערוך על מנת לבחור את המשתתפים היעילים ביותר בכל סבב לימוד תוך שמירה על בחירה הוגנת שלא מקפחת או מנצלת יתר על המידה את אף אחד מבין הלקוחות.

**תוצאות עיקריות:**

תוצאות המאמר תלויות במידה רבה בפרמטר V ובמשמעות מאחורי בחירת ערכו, על מנת שנוכל לנתח את התוצאות הסופיות ואת המשמעויות הנגזרות מהן, ראשית נרצה להסביר בצורה אינטואיטיבית על הפרמטר V ותפקידו באלגוריתם בחירת המשתתפים, אנליזה רחבה על הפרמטר ופיתוחים מתמטיים נלווים יפורטו בהמשך.  
  
הפרמטר V משמש כ – Penalty Factor (פקטור ענישה/מחיר הוגנות), מטרתו היא לאזן בין מזעור זמן ביצוע משימת הלימוד המאוחד (אופטימיזציה) לבין שמירה על הוגנות בחירת זהות המשתתפים. V הינו פרמטר הכפלתי שתפקידו למשקל את השפעת הוגנות הבחירה, הפרמטר מוכפל בפונקציית "מחיר הוגנות" המתווספת למשוואת ליאפונוב ריבועית וביחד יוצרת פונקציית אופטימיזציה אל מול הוגנות שממנה ניתן לפתח בעיית תכנות לינארי שניתן לפתור בצורה אלגוריתמית. בחירה של פקטור נמוך משמעה מזעור פונקציית מחיר ההוגנות, כלומר, מערכת הוגנת יותר.

תוצאות המאמר מראות שלפקטור הענישה V יש כמה דרגות השפעה על תהליך האימון, השפעתו של הפרמטר גדלה כתלות בהתפלגות וכמות המידע שמערכת הלימוד המאוחד מקבלת. בנוסף, מתוצאות המאמר ניתן להסיק כי עבור מטלות לימוד גדולות ביצוע משימות בצורה הוגנות עם דיוק הולם מצריכה כמות גדולה מאוד של מידע, כאמור, פתרון בחירת המשתתפים שמציע המאמר אינו הפתרון האופטימלי מבחינת זמן ריצה, זאת מכיוון שהוא מתחשב בנוסף בהוגנות הבחירה, לכן, על מנת לשמור על דיוק, מידע רב ומגוון צריך להיות מפולג בין הלקוחות השונים. לעומת זאת, למרות שניתן לראות שוני בתוצאות הן מבחינת יציבות המודל והן מבחינת זמן הריצה במהלך סבב אימון עבור לקוחות שמחזיקים במידע תלוי אל מול כאלו שמחזיקים במידע פחות תלוי או בלתי תלוי לחלוטין, תוצאות הניסויים מראות שהשפעת תלות המידע בין לקוחות שונים היא כמעט חסרת השפעה על טיבה של הוגנות בחירת המשתתפים, דבר שמוכיח את יציבותו של האלגוריתם להתמודדות עם סוגים שונים של לקוחות.  
  
בחירה במערכת הוגנת מראה עלייה משמעותית בדיוק הסופי במודלים שנבדקו ביחס למערכות פחות הוגנות, לעומת זאת עבור מספר נמוך של סבבי אימון, רמת הדיוק אינה גבוהה במיוחד.   
בחירה במערכת פחות הוגנת מראה אפקטיביות נמוכה יותר לכל סיבוב, כלומר, זמן התכנסות המודל לרמת דיוק מסוימת גדל, דבר דומה קורה גם עבור מימוש מנגנון בחירת המשתתפים ההוגנת, שתופס משקל רב יותר רק לקראת סוף סבב האימון (לוקח למערכת זמן רב יותר להגיב ולהשתפר).

**עבודות נוספות בתחום:**

ישנם מאמרים נוספים בתחום אשר מתעסקים בבעיות דומות למאמר שאנו מנתחים:   
במאמר [1] כותבי המאמר מנסים לשערך את זמן השידור בין הלקוחות לשרת ובכך לבחור בצורה מיטבית את זהות הלקוחות המשתתפים. במאמר מוצע אלגוריתם בשם FedCS שבודק את כל אפשרויות בחירת הלקוחות בכל סיבוב ובוחר את המינימלית מבחינת זמן אימון, נשתמש ב-FedCS כנקודת ייחוס לבדיקת האלגוריתם במאמר שלנו.   
במאמר [2] מעבר לשערוך זמן השידור ישנה גם התחשבות בצריכת האנרגיה ואף מוצעת דרך יעילה לחילוק רוחב הפס בין לקוחות שונים. שני המאמרים מציעים פתרון ישים ויכולים לשפר את ביצועי הלימוד המאוחד, אך נראה שמאמרים אלו מתבססים על שתי הנחות שהן לא בהכרח נכונות או רצויות.

ראשית, ההנחה הרווחת במאמרים אלו היא שניתן לשערך את זמן שידור הלקוחות בהתבסס על זמן אימון לוקאלי ידוע, זהו לא בהכרח המצב שקורה בפועל שכן זמן אימון יכול להשתנות בין סבבי אימון שונים.  
ושנית, עקב ההנחה שהעדיפות היא תמיד עבור לקוחות עם קצב שידור מהיר, נוצר מצב בו לקוחות מסוימים נבחרים תמיד ואחרים לא נבחרים בכלל, דבר אשר פוגע משמעותית בהוגנות בין לקוחות שונים ואף יכול להוביל ל- Overfitting על מידע מסוים שנמצא אצל לקוחות ספציפיים.

המאמר מתמודד עם בעיות חדשות בפתרון בעיית בחירת הלקוחות המשתתפים בתהליך הלימוד, כאשר כעת הפתרון הרצוי הוא ללא הנחות מקלות, שיערוך זמן השידור של הלקוחות אינו מסתמך על זמן לוקאלי קבוע אלא מתחשב גם בזמינות הלקוחות, זמני אימון אקראיים וערוץ תקשורת דינאמי.   
בנוסף לכך, בניגוד למאמרים קודמים המאמר מציע פתרון המשלב הוגנות ביחד עם שערוך דינאמי בזמן אמת של זמני העדכונים ושליחת הפרמטרים ללקוחות, שקורה מחדש בכל סבב אימון.

בנוסף לשני המאמרים לעיל, בשנים האחרונות נעשו מספר ניסיונות להתגבר על בעיית גניבת המידע בתהליך הלימוד של הבינה המלאכותית גם בדרכים אחרות מזו שבמאמר.   
כפי שניתן לראות במאמרים [4], [5], [6], נעשו ניסיונות לשלב בין בינה מלאכותית לבין  
Edge Computing – שיטה בה ממקמים את הלקוחות המשתתפים בלימוד ברשת מקומית סגורה יחד עם השרת שמבצע את הלימוד בצורה מרוכזת, בלימוד מסוג זה ניתן לבזר את הלימוד בין צמתים שונים ולהאיץ את הלימוד ובנוסף פוחת החשש מגניבת מידע שכן על מנת לגשת אליו יהיה על תוקף לקבל גישה אל תוך רשת מקומית מאובטחת שהמידע הרגיש בתוכה ולא יכול (ולא צריך) לצאת ממנה.   
מאמר פורץ דרך בתחום הוא Neurosurgeon [7] , שם ישנו שימוש ב- Edge Computing לחילוק רשת נוירונים עמוקה לחלקים קטנים יותר ובכך למקבל לימוד על רשת נוירונים בין כמה מחשבים שונים. אמנם Edge Computing היא שיטה יעילה שמשפרת את ביצועי הלימוד ושומרת על סודיות המידע עד רמה מסוימת (מופץ מידע רגיש בתוך הרשת המקומית) אך כאמור השיטה המוצעת במאמר שומרת לחלוטין על סודיות המידע (שלא מופץ בכלל, רק עדכוני לימוד מופצים) ואף מנצלת כמו שנעשה ב- Edge Computing את העקרון החישוב המבוזר.  
  
שיטה נוספת להתגבר על הבעיה היא שילוב לימוד מכונה מבוזר ביחד עם למידה לוקאלית כפי שניתן לראות במאמרים [8],[9], [10], [11] ובצורה מתוחכמת יותר על ידי שימוש באגרגציה (איחוד) כפי שניתן לראות במאמרים [12], [13]. שיטה זו היא הנחת הבסיס עליה מושתת המאמר, כעת ישנה שיטה המאפשרת לשרת שרוצה לאמן בינה מלאכותית או "בעל מודל" כפי שהוא נקרא במאמר לאמן את המכונה שלו על ידי שירותם של מספר רב של לקוחות רחוקים שיכולים לבצע אימון מקומי על חלק מסוים מהמידע ולשלוח חזרה לשרת רק עדכונים רלוונטיים ללא חשיפת מידע רגיש. המאמר לוקח את השיטה הזו וחושב על השלב הבא, כעת כשקיימת היכולת למקבל את הלימוד אצל לקוחות שונים נעבור להתעסק בשאלות הקריטיות הבאות - באיזה לקוחות כדאי לבחור? איך נבחר בצורה טובה וגם הוגנת?

נעבור להתבונן במאמרים מהתקופה האחרונה, כפי שציינו לעיל, ישנם אלגוריתמים קיימים המנסים לפתור את בעיית בחירת הלקוחות המשתתפים בלימוד המאוחד, אך כאמור בכל אחד מבין המאמרים שציינו ובנוסף במאמרים [14], [15], ו-[16] ההתעסקות המרכזית היא באופן בחירת לקוחות כך שתמזער מטריקות תקשורת שונות כגון זמן שליחה, עומסים ברשת, הקצאות יעילות של רוחב פס לכל לקוח וכו' . המאמר לוקח את העקרונות המנחים ממאמרים אלו ושוב לוקח צעד קדימה כאשר כעת הוא מתעסק בנוסף בשאלת הוגנות בחירת המשתתפים, המאמר מציע אלגוריתם ששואף למצוא את השילוב המיטבי בין מזעור זמן שליחה משוער והוגנות בחירת המשתתפים בלימוד.

**מודל המערכת וניסוח הבעיה**

**ניסוח מילולי של הבעיה:**

הבעיה המרכזית במאמר מתמקדת באופן קבלת ההחלטות של השרת בשלב בחירת הלקוחות ללימוד המאוחד. כאמור נרצה לבחור לכל סבב אימון מספר לקוחות כך שישרתו אותו בצורה הטובה ביותר תוך שמירה על בחירה הוגנת בין לקוחות. הבעיה עלולה להתפרש כבעיה פשוטה אך ישנן כמה בעיות מהותיות שיש לפתור על מנת להתמודד איתה.  
  
ראשית, יש להתמודד עם השאלה מהי בחירה אופטימלית ואיך מוצאים כזו?  
נראה כי לא ניתן להתייחס לבעיית אופטימיזציה ללא הגדרת מטריקה מסוימת (פונקציית רווח או מחיר) שאותה נרצה למקסם או למזער. עבור המקרה הנ"ל המטריקה המתאימה היא שערוך   
ה - Exchange Time (זמן החלפה), הזמן שלוקח מרגע שהשרת שולח את המודל לכל הלקוחות שנבחרו עד שהוא מקבל מכולם עדכונים בחזרה, כמובן שנרצה למזער אותו על מנת לחסוך בזמן הלימוד.  
  
הקושי מאחורי שערוך זמן החלוקה נובע משתי בעיות, האחת היא שזמן החלוקה הוא משתנה אקראי, על מנת לשערך משתנה אקראי יש לדעת את הפילוג ממנו מגיע המשתנה או לחלופין לבצע דגימות או הערכות על בסיס ידע מקדים, והשנייה היא שיש לבצע שערוך על בסיס אלגוריתם רציף שפועל בזמן אמת, על האלגוריתם לפעול בזמן האימון על מנת שתתאפשר למידה של המודל.

שנית, יש להתמודד עם השאלה כיצד ממדלים בחירה הוגנת?  
נרצה לדעת להעריך מהי בחירה הוגנת ומהו האיזון הנכון בין בחירה הוגנת לבין בחירה אופטימלית, על מנת למדל מהי בחירה הוגנת נצטרך לקיים אילוץ שיבטיח את קיום ההוגנות, נרחיב עליו בחלק הבא.

**הנחות יסוד ובניית תשתית למידול המערכת:**

1. ***Model Exchange Time*** – זמן ההחלפה הינו מטריקה חשובה שיש לשערך, נחדד את הגדרתו על מנת שנוכל להגדירו בצורה מתמטית עבור המודל: זמן ההחלפה הינו הזמן שלוקח מרגע שהשרת מחליט על בחירת הלקוחות ושולח להם את המודל ועד לרגע שבו הוא מקבל מכולם עדכונים בחזרה, זמן ההחלפה נקבע לחלוטין על ידי הלקוחות המשתתפים ובפרט על ידי הלקוח האיטי ביותר שנבחר השוהה את הזמן הרב ביותר בתהליך הלמידה, שליחת וקבלת עדכונים.  
   נגדיר מתמטית את זמן ההחלפה:

*הינה קבוצת הלקוחות הנבחרים בזמן , הינו זמן ההחלפה של לקוח שנבחר.   
הנחת יסוד חשובה היא שהזמן אינו ידוע עד סוף כל סבב לימוד, לכן יש לשערך אותו.*

1. ***Long-Term Fairness Constraint*** – מטריקה חשובה בעלת השפעה קריטית על תהליך הלמידה הינה פקטור ההוגנות. על מנת להבין מדוע ההוגנות היא חשובה נתבונן במצב אידיאלי בו זמני ההחלפה ידועים מראש, היינו נוטים להאמין כי במידה וכל זמני ההחלפה ידועים, הפתרון האופטימלי הינו הפתרון החמדן, לכל סבב לימוד יש לקחת את הלקוחות המהירים ביותר ולבחור בהם. אמנם פתרון זה אכן יכול למזער את זמן הלימוד אך זו לא השאיפה העיקרית, בתהליך אימון נרצה לשאוף להגיע לדיוק מקסימלי, על מנת לקבל זאת נרצה לאמן מודל לא רק בכמות גדולה של מידע אלא גם בצורה מגוונת. במידה ונבחר בצורה חמדנית לקוחות רבים לא יבחרו עקב זמני החלפה הארוכים שלהם ונקבל אימון פחות מגוון במידע, פגיעה זו תגרע מיכולתו של המודל להתמודד עם מידע חדש ותיצור הטיה כלפי מידע שנמצא אצל הלקוחות המהירים.

על מנת לשמור על הוגנות נגדיר בצורה מתמטית אילוץ לטווח ארוך שנחייב את המערכת לקיים:

הינו קצב ממוצע מחייב לבחירת לקוחות, הינו מספר סיבובים הכולל בתהליך הלימוד   
ו- הינה פונקציה המציינת האם לקוח משתתף בסבב אימון .  
  
האילוץ מוודא כי לטווח ארוך קצב הבחירה הממוצע - כמות הפעמים בה הלקוח נבחר ליחידת זמן חסומה מלמטה על ידי , כך ניתן להבטיח כי בהסתכלות רחבה על תהליך אימון שלם כל לקוח יבחר לפחות מספר מסוים של פעמים, לכן הבחירה הוגנת יותר ולא מקפחת לקוחות מסוימים.

1. ***Availability of clients*** – מכיוון שאנו מתמודדים עם בעיית בחירת לקוחות דינאמית תחת תנאים שמדמים את המציאות, נרצה להתחשב בעובדה שלקוחות לא תמיד יהיו פנויים להשתתף בתהליך האימון לכן הנחה נוספת היא שיש לבחור את הלקוחות לסבב האימון הבא רק מאלו שדיווחו על עצמם כפנויים בסוף סבב האימון הקודם.  
   לצורך נוחות נגדיר פונקציית אינדיקטור שתציין את נכונותו של לקוח להשתתף בסבב אימון :  
     
   הערה: הפונקציה זהה מתמטית לזו שנעזרנו בה בסעיף 2 אך רעיונית הפונקציות שונות, הינה פונקציית אינדיקציה עתידית (לסבב הבא) ואילו פונקציית אינדיקציה לסבב הנוכחי (מי נבחר).
2. ***Selection Fraction*** – כאמור, אנו מתמודדים עם בעיית בחירת לקוחות דינאמית שמדמה את המציאות, לכן, כעת נרצה להתייחס גם להנחה כי יתכן מצב בו לא יהיו משתמשים פנויים שנוכל לבחור לסבב הלימוד, כלומר, יש להגדיר בצורה סגורה את גודל קבוצת המשתתפים בכל סבב אימון:

מספר המשתתפים בסבב אימון יהיה המספר המינימלי בין (מספר קבוע רצוי לאימון) לבין סכום הלקוחות הפנויים להשתתף.

**ניסוח מתמטי של הבעיה והגדרת המודל :**

כעת כאשר הבעיה הכללית מנוסחת והנחות היסוד מוגדרות בצורה סגורה, נרצה באמצעות פיתוחים מתמטיים להגיע למודל סגור שאותו יהיה ניתן לממש בקוד.  
  
ראשית, נרצה לפתח מתמטית בעיית אופטימיזציה בסיסית הפותרת את בעיית בחירת המשתתפים   
ב- Offline (לפני תחילת הלימוד).

Offline Long-Term Optimization Problem:

*משוואה זו שואפת למזער את זמן ההחלפה הממוצע לתהליך הלימוד ועושה זאת על ידי מזעור משוכלל של כל סבבי האימון יחד (לכן זו בעיית* Offline*).  
נראה בנוסף כי בהתאם למשוואות לעיל ישנן מגבלות (*constraints*)* שיש לשמור עליהן, כאשר (2) מבטיחה הוגנות ו-(3),(4) מבטיחות כי אין הנחות מקלות וזמינות המשתתפים נלקחת בחשבון בבעיית האופטימיזציה.

שנית, לאחר שהוגדרה בעיית האופטימיזציה ב – offline נרצה להשתמש בבעיית אופטימיזציה מסוג Lyapunov על מנת להמיר את הבעיה לבעיה בזמן-אמת (Online):  
  
השלב הראשון בהמרת הבעיה לזמן אמת היא הגדרת תורים ווירטואליים לכל לקוח, את תורים אלו נרצה לשערך בזמן אמת ונוכל לעשות זאת לפי המשוואה הבאה:

האינטואיציה להגדרת התורים הווירטואליים נובעת מהמשפט הבא:

Theorem 1:   
Long-term time average constraint holds if all the virtual queues   
(whose backlogs denoted by ) remain mean rate stable across the FL process.

את ההוכחה למשפט זה ניתן לראות בנספחים [1].   
אינטואיטיבית, אורך התור יתבדר לאינסוף במידה ומגבלת ההוגנות לטווח הארוך לא תתקיים, על מנת להבטיח הוגנות על התור להישאר במצב יציב. אורך התור יכול לתאר את דרגת ההוגנות של תהליך הבחירה, ככל שגודל התור גדל כך תהליך הבחירה פחות הוגן.

השלב השני הוא שימוש בטכניקות של שיטת Lyapunov על מנת לחסום את התבדרות אורך התורים הווירטואליים תוך מזעור פונקציית המטרה ב – .  
נשתמש בפונקציית Lyapunov ריבועית מהצורה הבאה:

*נרצה לחסום את הגידול של , לשם כך נגדיר את ערך ההסתה:*

נרצה למזער את זמן ההחלפה לכן נשלב את פונקציית המטרה בבעיית האופטימיזציה ביחד עם פונקציית ההסתה תוך התחשבות בפקטור ההוגנות , נקבל פונקציית הסתה ועוד מחיר:

כעת מה שנותר הוא לחסום את הפונקציה שהתקבלה על ידי החסם הבא:

לפי המשפט הבא:

Theorem 2:   
Conditioning on the queues’ backlogs , the drift-plus-cost function for our system model could be bounded into the following form, where is a constant.

את ההוכחה למשפט זה ניתן לראות בנספחים [2].  
  
נגיע לבסוף לתיאור הבעיה בזמן-אמת:

ובמידה ונתעלם מהקבועים (זו בעיית מינימיזציה אין טעם לסחוב קבועים) נקבל את הצורה הבאה:

כעת לאחר שהגדרנו את הבעיה בזמן-אמת נראה כי אין ביכולתנו לממש את בעיה זו בצורתה הנוכחית תחת ההנחה שלא ניתן לדעת את זמן ההחלפה לפני כל סבב לימוד (כך קורה במציאות) לכן נרצה לפתח את הבעיה לצורתה הסופית שאותה נוכל לממש בזמן אמת ולפי ההנחה המקשה לעיל.

נשתמש בשערוך לפי שיטת עם UCB (ניתן ל*התעמק בנושא במאמרים [17-21]) על מנת למזער את הערך הנצבר כתוצאה מפקטור הענישה עבור בחירות לא הוגנת ככל שניתן.  
נשתמש בטכניקת השיערוך על מנת לשערך את זמן ההחלפה של כל לקוח לפי היסטוריית זמני ההחלפה שלו. ניתן להתייחס לכל לקוח כ -* Arm *בשיטת ה -* Multi Arm Bandit *ובעזרת משתנה אקראי שמגלם את תכונות השידור והעיבוד של לקוח בזמן לשערך את זמן השידור האמיתי של כל לקוח:*

*– משתנה שנועד לכמת כמה המעבד\ים של לקוח פנויים (חישובית) להשתתף בסבב לימוד.  
 – משתנה אינדיקציה להשתתפות בסבב בלימוד הקודם.  
 – משתנה אינדיקציה לרוחב הפס שהמשתמש מקצה לסבב הלימוד.  
 – משתנה שמשערך את זמן הלימוד (לבדו) עבור לקוח בתפוסה חישובית מלאה.  
 – משתנה שקובע את תחילת זמן הלימוד.  
 – משתנה שמגלם את יחס האות לרעש של לקוח לפי איכות השידור שלו.  
 – קבוע שרירותי לחסימת הרעש.*

*מכפלת הווקטורים במשוואה יוצרת שיערוך טוב לזמן ההחלפה, היא כוללת בתוכה את קצב העלאת המודל (משוואת שאנון), התחשבות ביכולת העיבוד של כל לקוח , זמן התחלה ולימוד משוערכים והתייחסות נוספת למשתנה האינדיקציה במידה והלקוח השתתף בסבב הקודם, לכל זה מתווסף רעש כמשתנה אקראי אפסילון וכך ישנה התחשבות נוספת גם בשגיאות אפשריות בקו התקשורת.*

*ולאחר כמה פיתוחים מתמטיים (שלא נרחיב עליהם כאן) נקבל את הנוסחה הסופית לשערוך זמן החלפה ממוצע שבו ניתן להשתמש באלגוריתם בזמן אמת:*

*– מטריצה שמגלמת בתוכה פקטור רגרסיה לשערוך לפי זמנים קודמים (Ridge regression).  
 – וקטור דינאמי שמתעדכן בכל סבב לימוד לפי תוצאות בחירת המשתתפים.  
 – פקטור גילוי משתנה שניתן לזהות בכל סבב לימוד.*

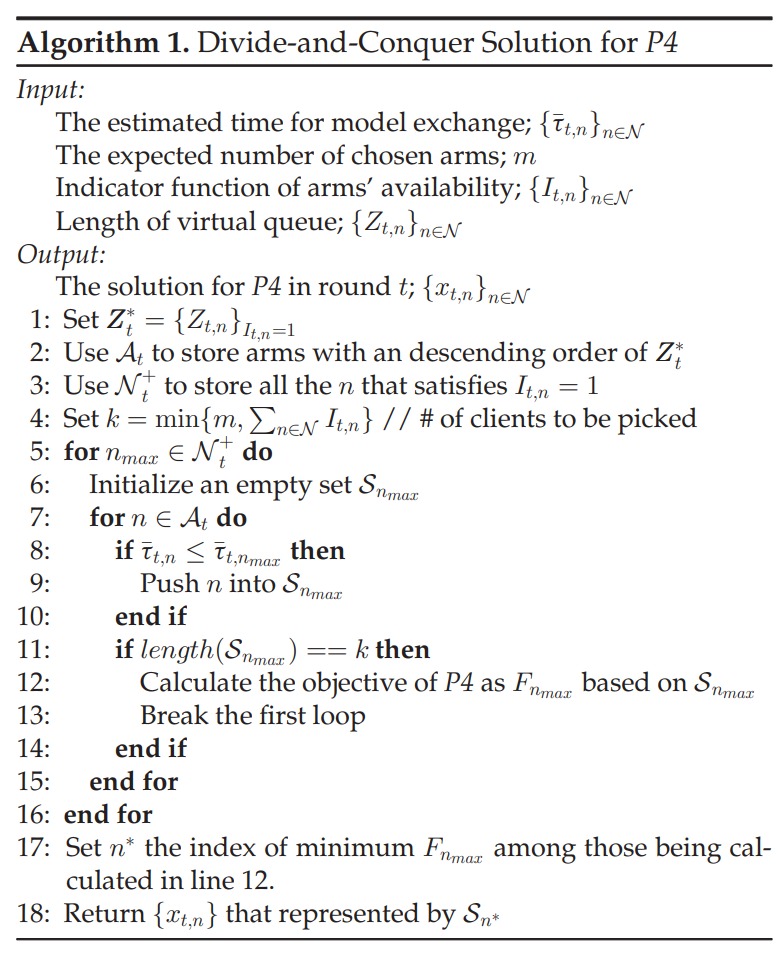
לבסוף נוכל לרשום את בעיית התכנות הלינארי בצורתה הסופית:

ובצורה יותר קלה חישובית ניתן לשפר את הבעיה לכדי צורה פשוטה יותר:

האלגוריתם שמוצע במאמר משתמש בבעיית התכנות הלינארי לעיל על מנת להגיע לבחירה מינימלית בזמני ההחלפה (הממוצעים) המשוערכים תוך שמירה על מגבלת ההוגנות לפי פקטור ההוגנות ,   
נראה זאת בחלק הבא ("פתרונות לבעיה").

**פתרונות לבעיה**

בחלק זה נציג את האלגוריתמים המוצעים במאמר ונדון בתוצאות התיאורטיות שאנו מצפים לקבל.  
כפי שראינו בחלק הקודם, בעיית בחירת המשתתפים ניתנת להמרה לבעיית תכנות לינארי עם מספר מגבלות שיש לקיים.   
נתבונן באלגוריתם הראשון שמוצע במאמרDivide-and-Conquer Solution for P4 - וננתח כיצד הוא פותר את בעיית התכנות הלינארי בצורה אלגוריתמית בקוד.  
  
**Algorithm 1 - Divide-and-Conquer Solution for**:  
  
על מנת להתמודד עם בעיית התכנות הלינארי המאמר מציע את האלגוריתם הבא:



נסביר את הקוד בקצרה:  
  
קלטים:  
נראה כי האלגוריתם מקבל ארבעה קלטים:  
 *– רשימה של זמנים המשוערכים ללימוד כל לקוח.  
 – מספר הלקוחות הרצוי ללימוד (מספר ה –* arms*).  
 – רשימה של אינדיקטורים לזמינות כל לקוח.  
 – רשימה של אורכי התורים הווירטואליים של כל לקוח.*

פלט:  
פתרון בעיית עבור סבב לימוד *– רשימת הלקוחות הנבחרים ללימוד בסבב .*

הסבר כללי על הקוד:  
*בשורות 1-4 ישנן הגדרות של משתנים על מנת להכין את התשתית לחישוב הבעיה הרצויה:  
מכל אורכי התורים שמקבל האלגוריתם נתעניין רק באלו ששייכים ללקוחות שמעוניינים להשתתף בסבב הלימוד, לכן נשמור רק אותם. בנוסף נגדיר שלושה משתנה חדשים, אחד שבו נשמור את מספרי הלקוחות לפי סדר יורד של אורכי התורים שלהם, אחד שבו נשמור את כל הלקוחות שמוכנים להשתתף בסבב הלימוד ואחרון שמייצג את מספר הלקוחות שישתתפו בלימוד בסבב ה- , המספר המינימלי בין מספר הלקוחות הרצוי לבין מספר הלקוחות שהתנדבו להשתתף.  
הגדרות אלו משמרות את המגבלות השנייה והשלישית מבעיית .  
  
בשורות 5-16 נבדקים כל הפתרונות האפשריים לפתרון בעיית התכנות הלינארי:  
נעבור באיטרציה על כל הלקוחות שהסכימו להשתתף ונגדיר סט ריק שאליו נכניס לקוחות בהמשך.  
לאחר מכן נעבור באיטרציה על כל הלקוחות לפי אורך התור שלהם ונבדוק האם המגבלה הראשונה  
של מתקיימת, במידה וכן נכניס את הלקוח לתוך הסט שהגדרנו.  
כעת נבדוק האם הסט מכיל את מספר המשתתפים הרצוי, במידה וכן נחשב את הערך של פונקציית המטרה של בעיית התכנות הלינארי המתאימה לסט שנבחר.  
  
בשורות 17-18 נפתור את בעיית המינימיזציה ונחזיר פלט רצוי:  
נבדוק מהו הערך המינימלי שמתקבל מפונקציית המטרה עבור כל הסטים שנבחרו ונחזיר את הסט הנבחר כרשימת אינדיקציה על בחירה לסבב .  
  
מידת חרטה והבטחת הוגנות באלגוריתם 1:  
במודל ה –* MAB *מידת החרטה היא מטריקה חשובה שמודדת את הפער בין יעילות בחירת המשתתפים שנבחרה לבין בחירת משתתפים לפי האלגוריתם האופטימלי, ננסה לחסום אותה ולהבטיח את התכנסותו של האלגוריתם.  
ראשית נגדיר את מידת החרטה של האלגוריתם:*

כאשר היא ההחלטה של האלגוריתם המוצע במאמר ו- היא ההחלטה של האלגוריתם האופטימלי.  
  
  
  
  
  
כעת נחסום את החרטה לפי המשפט הבא:

Theorem 3: Given any control parameter , with probability at least , the time average regret achieved by RBCS-F is upper bounded by:

Where and are both positive finite constants satisfying andfor all and and:

את ההוכחה למשפט זה ניתן לראות בנספחים [3].

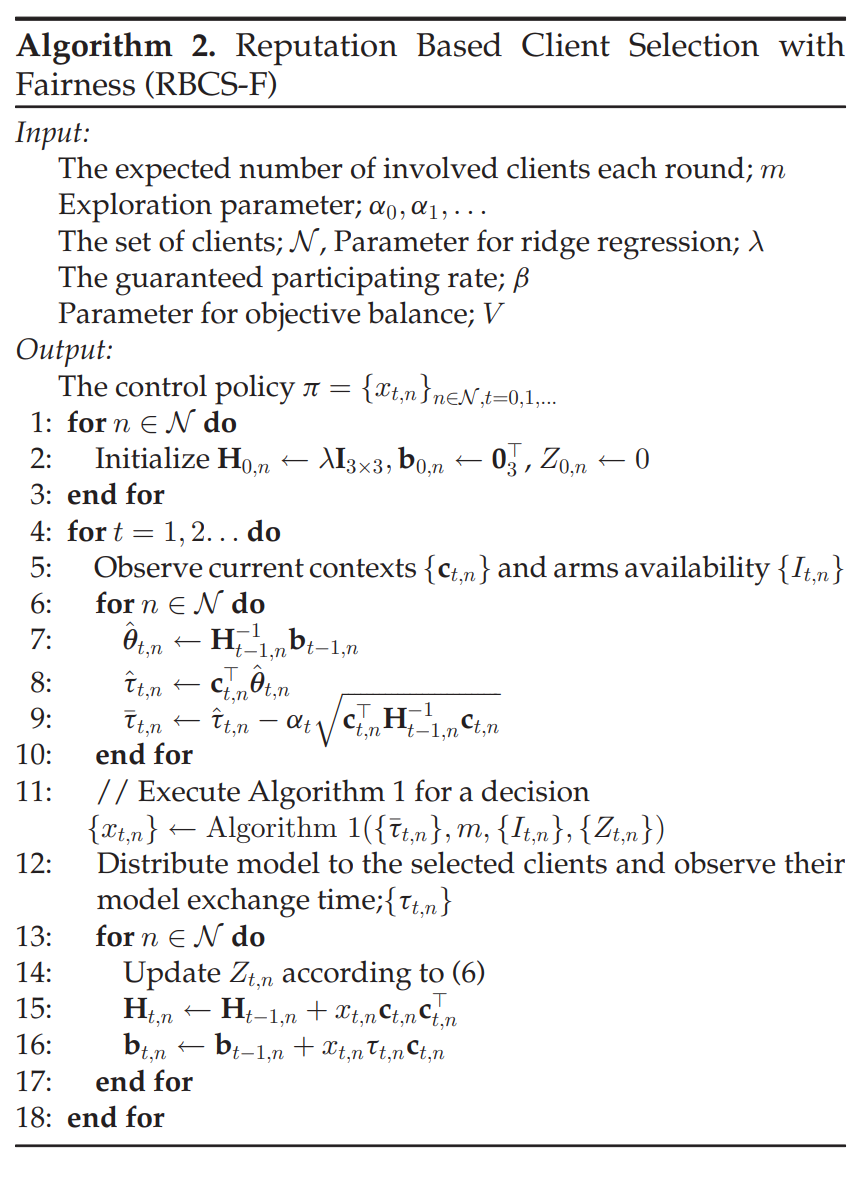
ובנוסף עם המשפט הבא:

Theorem 4: For RBCS-F, the fairness virtual queues are all mean rate stable in any setting of , thus the time average fairness is being guaranteed.

את ההוכחה למשפט זה ניתן לראות בנספחים [4].  
  
נקבל חסם למידת החרטה של האלגוריתם שמבטיח את יעילותו אל מול האלגוריתם האופטימלי, בנוסף נקבל הבטחה שאורך התורים הווירטואליים לא מתבדר ולכן האלגוריתם מחויב להתכנס לכדי תוצאה סופית ללא תלות במספר סבבי הלימוד המתקיימים בלימוד המאוחד.

ניתוח תוצאות תיאורטיות כתלות בפרמטר ההגנות :

לאור משפט 3, היינו מצפים כי לקבוע את גורם הענישה להיות גדול ככל האפשר הייתה בחירה טובה מכיוון שהיא מאפשרת לנו לבטל את השפעת האיבר הראשון בחסם החרטה שהצגנו. הבחירה נראית אף יותר אטרקטיבית נוכח העובדה שמגבלת ההגינות מתקיימת לכל ערך של כפי שראינו במשפט 4.  
אך למרות זאת, למרות שערך גדול של אכן יכול להבטיח לנו זמני החלפה רצויים לטווח הארוך תוך שמירה על מגבלת ההגינות, זמני לימוד במציאות הם סופיים שלא כמו בהנחה בה כותבי המאמר השתמשו להוכחת החסם. בנוסף לכך, הגדלת פקטור ההוגנות תגרום לקצב התכנסות ארוך יותר, תוצאה לא רצויה שיכולה לפגוע בדיוק הלמידה עבור תהליכי לימוד סופיים (אמיתיים).   
נרצה למצוא ערך (או תחום ערכים) של כך שהמערכת תהיה הוגנת אך גם שלא תתכנס בזמן ארוך מידי ובכך תפגע בדיוק הלימוד.

**Algorithm 2 - Reputation Based Client Selection with Fairness:**  
  
נציג את האלגוריתם הראשי שבוחר את זהות המשתתפים בלימוד המאוחד בזמן-אמת:

נסביר את הקוד בקצרה:  
  
קלטים:  
נראה כי האלגוריתם מקבל חמישה קלטים:  
 *– מספר הלקוחות הרצוי ללימוד (מספר ה –* arms*).  
 – רשימה של* Exploration parameters *לשערוך זמני הלימוד.  
 – רשימת כל הלקוחות של הלימוד המאוחד.   
 – פרמטר שערוך לרגרסיה לינארית ( Ridge regression).  
 – פרמטר הנועד להבטיח השתתפות (חסם תחתון ממקודם)  
 – פרמטר הוגנות*

פלט:  
*רשימת הלקוחות הנבחרים ללימוד לכל סבבי הלימוד.*

הסבר כללי על הקוד:  
*בשורות 1-3 ישנן הגדרות של משתנים על מנת להכין את התשתית לפעולתו של האלגוריתם:  
נגדיר לכל לקוח מטריצת יחידה הנכפלת בפקטור הרגרסיה, בנוסף נגדיר לכל לקוח וקטור אפסים לצורך חישובים להמשך ונגדיר את אורך התורים הווירטואליים של כל לקוח להיות אפס.   
  
כעת בשורות 4-5 נבצע איטרציה על כל הסבבים (), ובכל סבב נבדוק את המאפיינים הנוכחיים - מי מעוניין להשתתף ומה הם המאפיינים הקונטקסטואליים של השידור שלו ().*

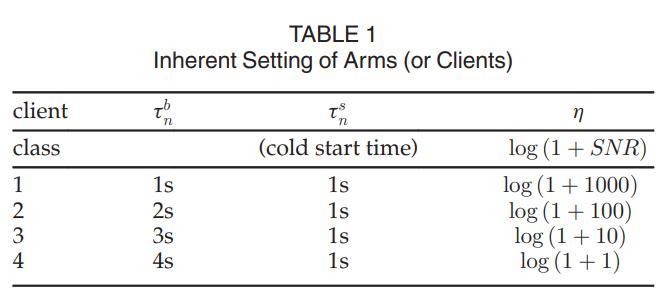
*בשורות 6-10 נעבור על כך אחד מבין מהלקוחות ונחשב את הזמן הממוצע המשוערך שלו לסיבוב הנוכחי. החישובים הנעשים בשורות אלו נובעים מהפיתוחים המתמטיים שנעשו לעיל (וגם כאלה שלא ציינו מפורשות כאן).*

*בשורות 11-12 ישנו שימוש באלגוריתם 1 על מנת לקבל פתרון לבעיית קביעת זהות המשתתפים עבור סבב t , בנוסף האלגוריתם מתבונן על זמן ההחלפה האמיתי ושומר אותו על מנת להסתמך עליו לסבבים הבאים.*

*בשורות 13-18 נכין את התשתית לסבב הבא של הלימוד בכך שנעדכן את אורכי התורים, את המטריצה והווקטור שהגדרנו לעיל תוך שימוש בזמן האמיתי שנמדד באלגוריתם בזמן-אמת.*

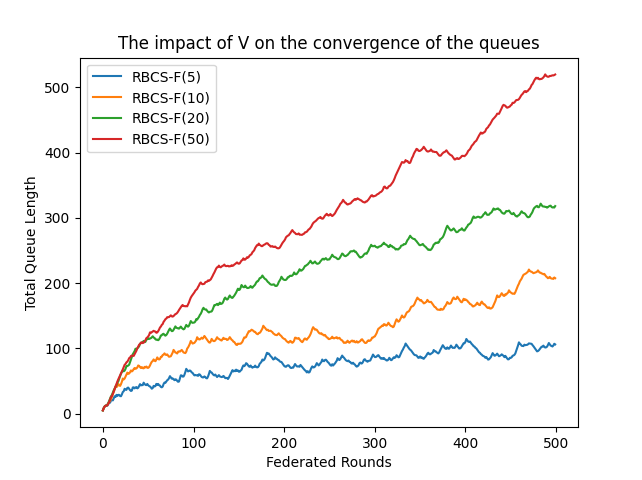
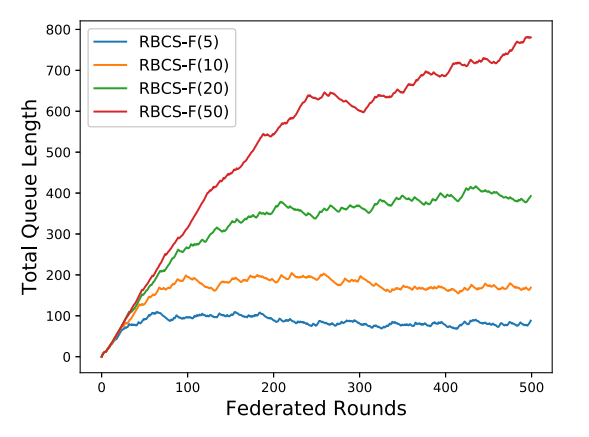
אינטואיציה:  
האלגוריתם הנ"ל משמש מאין מעטפת לאלגוריתם 1, האלגוריתם מוודא כי בכל סבב לימוד אלגוריתם 1 מקבל את כל הקלטים המעודכנים שעליו לקבל על מנת לפתור את בעיית התכנות הלינארי, לכן ישנו תפקיד חשוב לאלגוריתם והוא מדידה וחישוב של משתנים בזמן-אמת.  
חשוב לציין כי אלגוריתם זה נשען על הנחות רבות, אופן המדידה והשערוך הנעשים נשענת על יכולתו של בעל מודל למדוד את קו התקשורת בינו לבין כל לקוח ובנוסף כפופה לרצונו של לקוח לשתף מידע הכולל רוחב פס פנוי וזמינות מעבד, אך כאמור זהו מידע שולי ביחס לרגישות הפוטנציאלית של המידע שתהליך האימון יכול לקבל, לכן זוהי הנחה סבירה.

**תוצאות סימולציה**

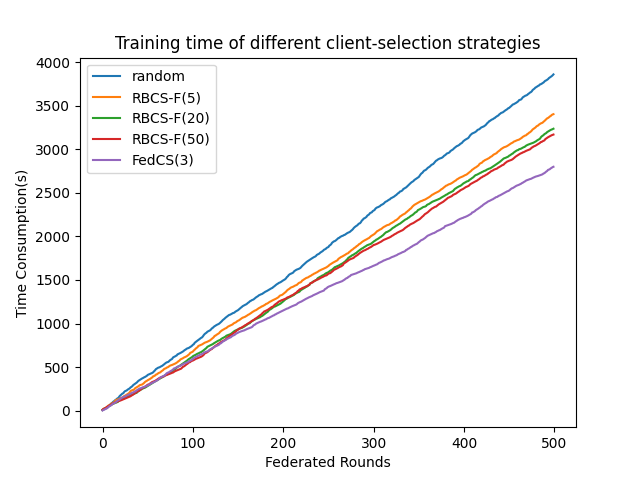
בחלק זה נדון בתשעה גרפים שקיבלנו כאשר שיחזרנו את הניסויים שבוצעו במאמר, אך ראשית נגדיר את תנאי ההתחלה והפרמטרים לפיהם מימשנו את הסימולציה שלנו:  
  
נחלק את ארבעים הלקוחות המשתתפים בלימוד המאוחד לארבעה סוגים, כאשר זמן ההתחלה והסיום נתונים לעיל ובנוסף עם נתון יחס האות לרעש עבור כל סוג לקוח, פקטור זה נועד למדל את ההשפעה של הפרעות בקו התקשורת בין בעל המודל לבין כל סוג מבין ארבעת סוגי הלקוחות.  
  
תמונה שמכילה שולחן

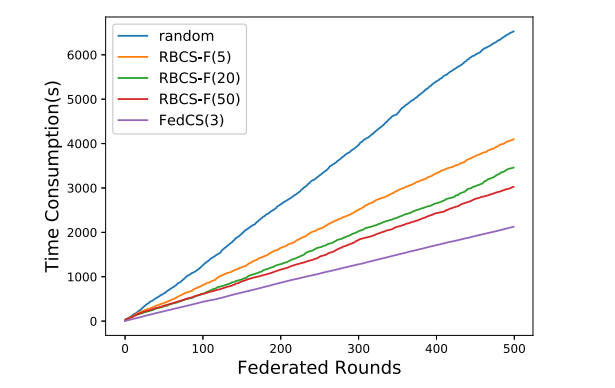
התיאור נוצר באופן אוטומטי נגדיר את הפרמטרים הנ"ל כקבועים שילוו את תהליך הלימוד לאורך כל סבבי הלימוד.  
  
בנוסף, ישנם משתנים נוספים הנקבעים לאורך המאמר, נציין אותם ברשימה הבאה:  
  
 *– זמינות חישובית (של מעבד\ים) נלקחת ממשתנה אחיד בתחום [200% – 50%].  
 – רוחב פס קבוע* MB*20 .  
 – קבוע שרירותי לחסימת הרעש שנקבע להיות (בהתאם לפיתוחים קודמים).  
 – זמינות הלקוחות נקבעת לפי פילוג (הסתברות של 0.8 להשתתפות).*

בנוסף נציין כי בדיקת האלגוריתם נעשית אל מול שני אלגוריתמים נוספים לבחירת משתתפים, האחד הוא האלגוריתם הרנדומלי שבוחר משתתפים בצורה אקראית מבין אלו המעוניינים להשתתף והשני אלגוריתם FedCS(3) [1] שעליו הרחבנו לעיל.

**השפעת פקטור ההוגנות על התכנסות התורים הווירטואליים:**  
  
נציג את תוצאות הסימולציה עבור ההשפעה של V על אורך התורים עבור 500 סבבי אימון:  
   
כפי שציפינו בהתאמה לניתוח התיאורטי, ערכי גדולים מביאים להארכת זמן התכנסות הלימוד, זמן התכנסות זה מתבטא באורך התורים שכפי שניתן לראות בבירור בגרפים, גדל עבור ערכי גדולים.  
בנוסף, ניתן לראות כי בכל אחד מבין הגרפים קיימת נקודה בה הגרף מתחיל להתייצב, תופעה זו יכולה להסביר את הבטחת ההוגנות שהאלגוריתם מתחייב אליה, אנו יודעים כי אורך התורים מחויב להיות יציב, לכן התמתנות הגרפים עד כדי קו אופקי מעידה על קיום יציבות זו.  
נראה גם כי כאשר ערכי גדלים אורך התור שאליו מתכנס האלגוריתם גדל בהתאם, מכך אפשר להסיק כי הבטחת ההגינות תופסת פחות נפח עבור הסיבובים הראשונים של הלימוד, לכן הגדלת פקטור ההוגנות (ענישה) מביאה לתוצאות פחות הוגנות לזמן אימון קצר, שוב בהתאמה לתוצאות התיאורטיות.  
  
  
להלן הגרף המקביל שהוצג במאמר:  
ניתן לראות את הדמיון בין תוצאות הסימולציה שביצענו לעומת הסימולציה במאמר:   
מגמת הגרפים, היחס בין הגרפים השונים וזמן ההתכנסות כמעט זהה בין הסימולציות השונות.   
אך נראה כי גדלי התורים בסימולציה שלנו קטנים יותר, כנראה כתוצאה מהשפעתה של מידת האקראיות הנכללת באלגוריתמים.

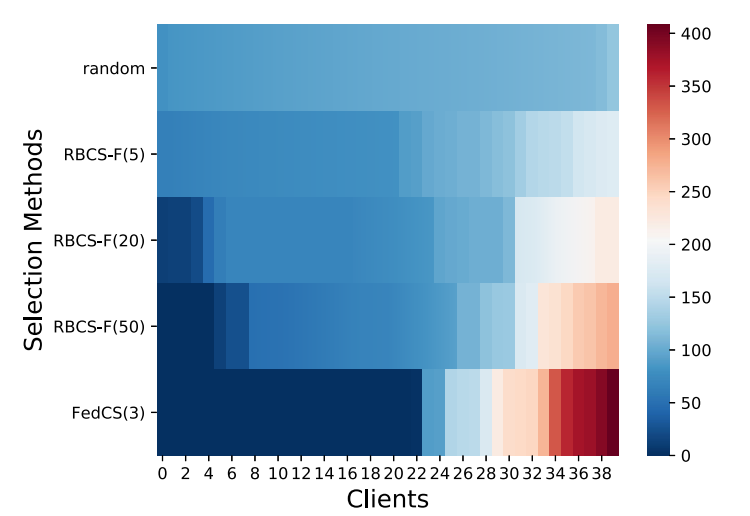
**זמן אימון תחת אסטרטגיות בחירת משתתפים שונות:**נציג את תוצאות הסימולציה עבור זמן האימון הכולל עבור אסטרטגיות בחירת משתתפים שונות:



כפי שניתן לראות האלגוריתם המוצע במאמר מראה תוצאות טובות משמעותית מאלגוריתם הבחירה הרנדומלי, כאמור, האלגוריתם דואג לשמירה על הוגנות אך עדיין מבצע בחירות על סמך מזעור זמן הלימוד המשוערך, לכן השיפור אל מול האלגוריתם הרנדומלי הינו בהתאמה לתוצאות שהיינו מצפים לקבל. לעומת זאת, נראה כי האלגוריתם FedCS(3) מניב תוצאות טובות בפער משמעותי מתוצאות האלגוריתם עבור ערכי ה – השונים. FedCS(3) איננו אלגוריתם הוגן, אלא מסתמך אך ורק על שערוך זמני לימוד ובחירת הלקוחות שיביאו למזעור זמני לימוד משוערכים אלו, לכן גם כאן הפער בזמן הלימוד הינו כפי שהיינו מצפים שיהיה, זו גם אינדיקציה נוספת עברונו שאכן קיימת הוגנות בין לקוחות, אחרת לקוחות "איטיים" יותר היו נבחרים פחות.

להלן הגרף המקביל שהוצג במאמר:  
גם כאן ניתן לראות את הדמיון הרב בין תוצאות הסימולציה שביצענו לעומת הסימולציה במאמר  
בצורה דומה לגרף הקודם.  
גם כאן כמו בגרף הקודם נראה שישנו פער מסוים בין גודל הערכים המתקבלים במאמר לבין הערכים בסימולציה שלנו.

**כמות הפעמים בהם נבחרים הלקוחות תחת אסטרטגיות בחירת משתתפים שונות:**נציג את תוצאות הסימולציה עבור כמות הפעמים בהם נבחרים הלקוחות לאורך 500 סבבי אימון:  
(הערה: גם כאן וגם במאמר הערכים ממוינים בסדר עולה, מספר הלקוחות בציר ה-X להמחשה בלבד).

מתוצאות הגרף ניתן לראות כי ככל שמגדילים את פקטור ההוגנות (ענישה) כך גדל המספר המקסימלי של הבחירות עבור לקוח מסוים, כלומר, במילים אחרות, כאשר פקטור ההוגנות גדל האלגוריתם נוטה לבחור יותר בלקוחות מסוימים מאשר אחרים ובכך מבטא פחות את עקרון ההוגנות (עבור זמן סופי).  
שני האלגוריתמים האחרים הן דוגמאות טובות לאלגוריתמים קיצוניים באופן הבחירה שלהם.  
האלגוריתם הרנדומלי מציג מספר בחירות מינימלי לכל לקוח (כמעט שווה), זאת מכיוון שכל לקוח נבחר באופן אחיד, ללא תלות באף פרמטר אחר, לכן ניתן לראות שההוגנת במצב זה היא אידיאלית.  
מצד שני, FedCS(3) הוא אלגוריתם מוטה בייסודו, הוא מתעדף בחירה של לקוחות "מהירים" וניתן לראות זאת בבירור מהתוצאות.  
כפי שציינו, האלגוריתם שמציע המאמר מקיים הוגנות לצד שמירה על זמני החלפה מינימליים ככל הניתן, לכן הוא נמצא בין האלגוריתמים האחרים כפי שניתן לראות בצורה טובה בגרף.

להלן הגרף המקביל שהוצג במאמר:  
נראה כי גם כאן, תוצאות המאמר כמעט זהות אך מעט מובהקות יותר מאשר תוצאות הסימולציה שלנו, (ניתן לשים לב לפער בצבעים בין הגרפים).  
אך המגמה זהה והמסקנות נשארות כשהן כאשר מתבוננים בגרף שהוצג מהמאמר.

**אימון על מסדי נתונים ציבוריים:**

כחלק מבדיקת האלגוריתם RBCS-F, מעבר לניתוח תוצאות האלגוריתם מבחינת זמן לימוד והוגנות בחירת המשתתפים (המטריקות העיקריות לבדיקה), כותבי המאמר מצרפים בנוסף גם ניתוח מעמיק שבו הם מדגימים את התנהגותו של האלגוריתם תוך שימוש במסדי נתונים אמיתיים והשפעת בחירת המשתתפים על דיוק המודל לאורך הסימולציה.  
כותבי המאמר משתמשים ב – Pytorch על מנת לבנות רשת נוירונים עם שכבות קונבולוציה בתוכו (CNN Network) – קונסטלציית הרשת נמצאת במאמר וביחד עם מסדי הנתונים fashion – MNIST ו- CIFAR-10 מקיימים סימולציה שבודקת את דיוק הלימוד של מערכת המבצעת לימוד מאוחד.  
  
כותבי המאמר בודקים את דיוק הלימוד אל מול שני מקרי בוחן, האחד הוא השפעת חילוק מידע תלוי או בלתי תלוי על דיוק התוצאות והשני הוא הרצת האלגוריתמים השונים ובדיקת דיוק התוצאות תחת כל אלגוריתם.  
בעבור הסימולציות הבאות, נגדיר שני משתנים נוספים שנעזר בהם לניתוח דיוק התוצאות:

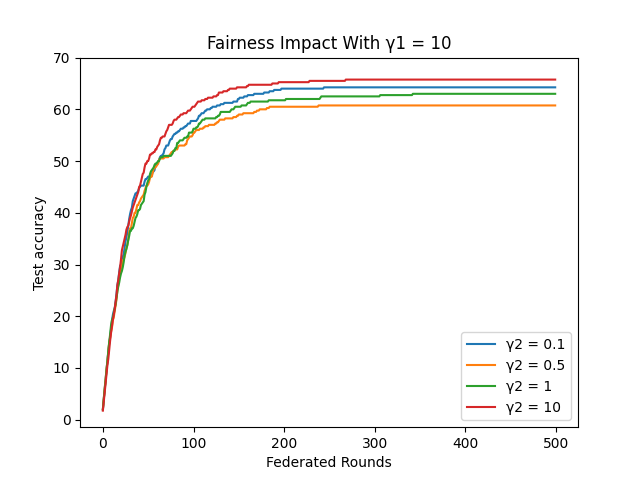
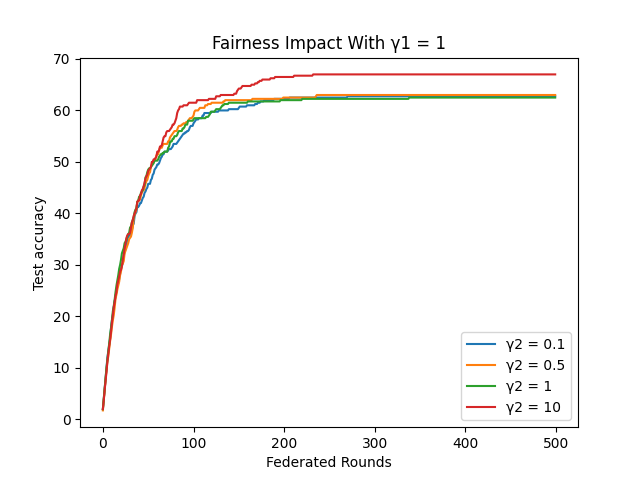
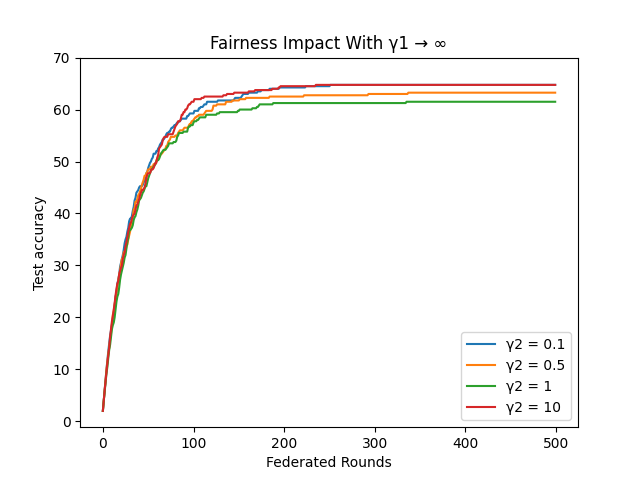
*:*

*פרמטר ריכוזיות (*concentration*) שמטרתו לשלוט על התלות בין הלקוחות השונים.   
כל לקוח מקבל מידע ממסד הנתונים לפי פילוג דריכלה כך שעבור תת-קבוצה של דגימות  
 נבחרת כך ש: עבור שרירותי.  
עבור כל הלקוחות מחזיקים במידע זהה ועבור כל הלקוחות מחזיקים במידע ב"ת.* *:*

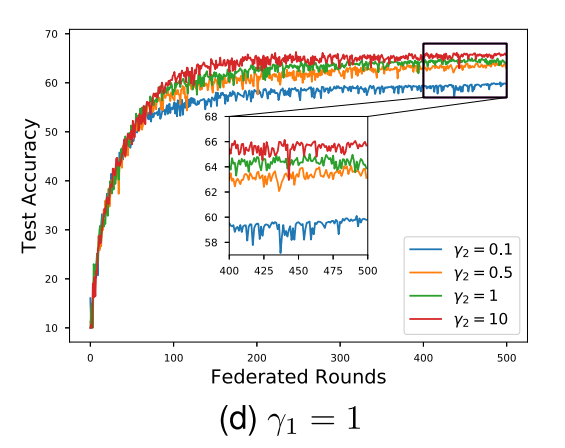
*פרמטר הוגנות שמטרתו להתחשב בהוגנות של בחירת הלקוחות.  
כל לקוח מקבל מידע ממסד הנתונים לפי פילוג דריכלה כך שעבור תת-קבוצה של דגימות  
 נבחרת כך ש: עבור שרירותי.  
  
עבור הסימולציה שלנו, אנו משתמשים במכפלה של פרמטר הריכוזיות בפרמטר ההוגנות על מנת לייצר פילוג דריכלה משולב מהצורה הבאה:*

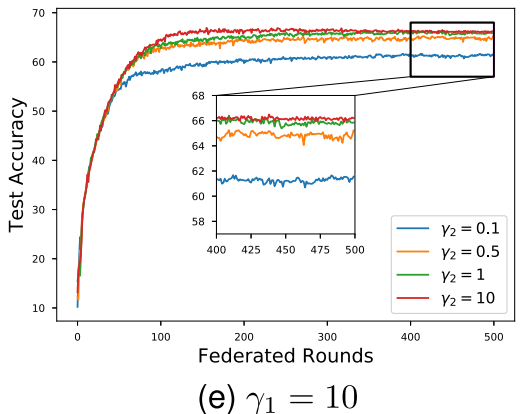
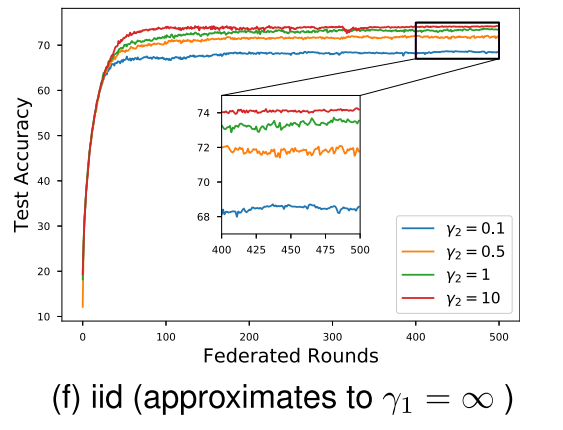
*מתוך פילוג זה אנו מחלקים לכל אחד מבין 40 המשתתפים סט של 10 מספרים (יתכנו כפילויות), כל המספרים שנבחרים הם בתחום השלמים [400 – 1] כך שבמקרה הבלתי תלוי כל אחד מבין המשתתפים יקבל עשרה מספרים ב"ת כך שכל הלקוחות ביחד יפרשו את תחום המספרים הנתון.  
  
מספרים אלו מייצגים "מידע ייחודי" שלקוח יכול ללמוד ממנו, כאמור, על מנת שמודל יגיע לתוצאות מיטביות עליו לקבל כמות מידע גדולה אך מעבר לכמות המידע, עליו גם להיתקל בסוגים שונים של דגימות כך שלא יהפוך למוטה עבור מידע מסוים ויבצע עליו* Overfit*.   
  
את דיוק הלימוד אנו בודקים בעזרת כמות המספרים הייחודיים שהצליח המודל להשיג בכל סבב לימוד, כאמור, אם ישנם 400 מספרים אפשריים, במידה ועד סבב המודל הצליח לאסוף 250 מספרים ייחודיים כך שבכל סבב הוא אוסף מספר יחיד מכל משתתף, ניתן לחשב את הדיוק שלו בקלות על ידי חילוק :  
  
   
הסתכלות מפושטת זו על החזקת מידע חוסכת מאיתנו לבנות סימולציה של לימוד מכונה מבוזר בעל לקוחות משתנים בזמן שאינה נכללת בחומר הקורס.*

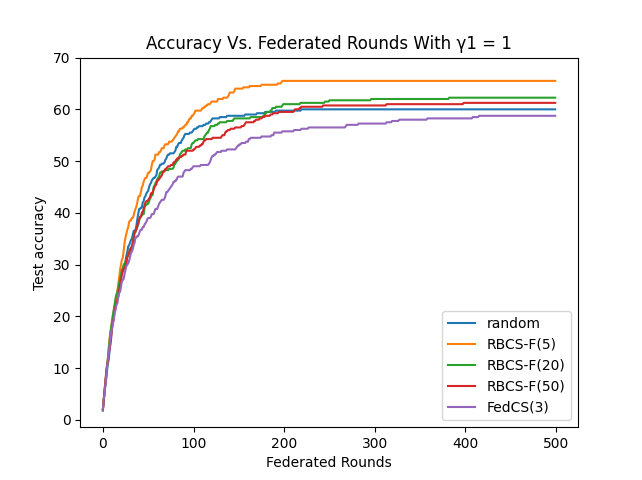
***השפעת פקטור ההוגנות עם ערכי פקטור ריכוזיות שונים:***

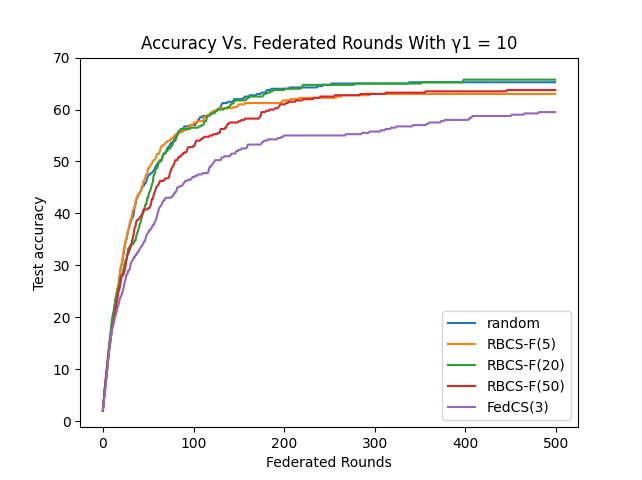
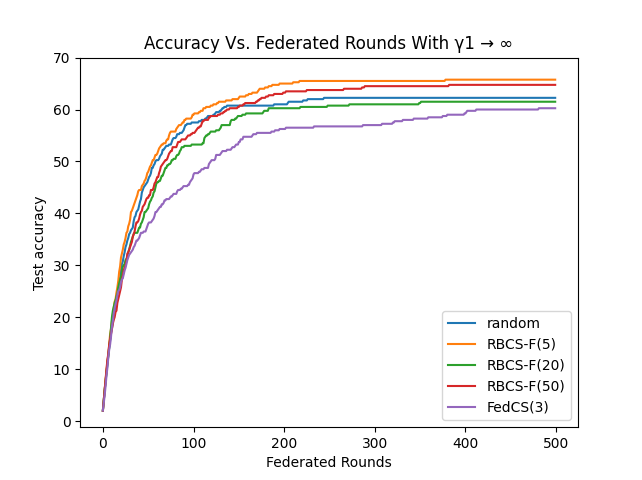
******נציג את תוצאות הסימולציה עבור ערכי פקטור הוגנות משתנים בהינתן פקטור ריכוזיות קבוע:  


*כפי שניתן לראות בכל הגרפים, כאשר פקטור ההגינות הוא הגדול ביותר (האדום), ניתן לראות שיפור משמעותי בדיוק תוצאות הלימוד, במיוחד עבור הערכים הקטנים של פקטור הריכוזיות.  
נראה כי גם כאן יש מגמת שיפור דומה שמראה התאמה בין הגינות לבין דיוק התוצאות, אך מכיוון שזהו מודל מפושט, עבור הבדל בין הערכי הגינות קטנים (בין 0 ל – 1) לא בהכרח ניתן לראות זאת.  
נראה כי תוצאות הדיוק אינן משתנות משמעותית בשינוי פקטור הריכוזיות.*

*נצרף את הגרפים המקבילים מהמאמר עבור מודל* CIFAR-10 *:*

**

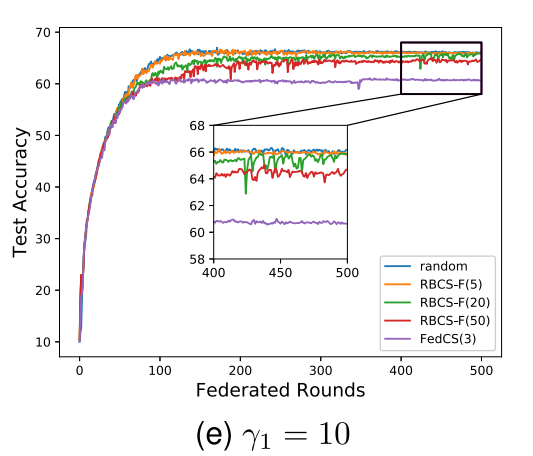
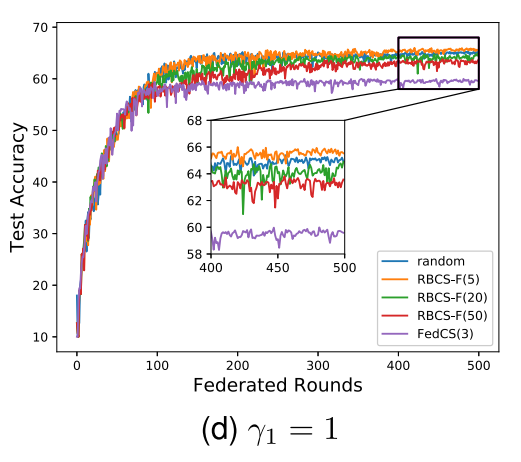
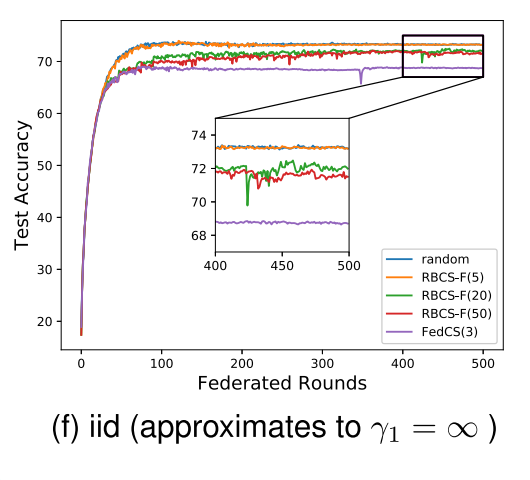
*כפי שניתן לראות, המודל האמיתי מראה תוצאות מדויקות יותר מהסימולציה המפושטת שלנו, ניתן לראות בגרפים אלו בבירור את השיפור הנעשה בשינוי פקטור ההוגנות (בשלנו הוא פחות מובהק).  
בנוסף, ניתן לראות תנודות (*jitters*) כתוצאה מירידה באחוזי הדיוק במהלך הלמידה, דבר שאינו קיים במודל המופשט שלנו ובפרט נראה כי הגדלת פקטור הריכוזיות מקטינה את כמות התנודות הללו.  
לעומת זאת, מגמת הגרפים שלנו דומה לגרפים מהמאמר וניתן להגיע לחלק מהמסקנות מהמאמר תוך הסתכלות על הגרפים שלנו.****השפעת האלגוריתמים השונים על אחוזי הדיוק:***נציג את תוצאות הסימולציה עבור ערכי האלגוריתמים השונים בהינתן פקטור ריכוזיות קבוע:



*כפי שניתן לראות מתוצאות הגרפים השונים, תוצאות הדיוק הגבוהות של האלגוריתם המוצע במאמר אל מול האלגוריתם* FedCS(3) *מובהקות גם כאן, בנוסף, ניתן לראות כי דיוק האלגוריתם עם פקטור ההוגנות () הנמוך ביותר הוא הגבוה ביותר בהתאמה למגמה מהניסויים קודמים.*

*האלגוריתם הרנדומלי גם מניב תוצאות יפות, זאת לאור העובדה שהוא אלגוריתם שוויוני לכן מצליח לאסוף מספר רב של מספרים.  
מסקנה נוספת מהגרפים היא שאלגוריתמי* F-RBCS *בעלי ערכי הגינות גבוהים יותר מתכנסים לאחר פרק זמן ארוך יותר, זאת בהתאמה לאורכי התכנסות התורים הווירטואליים שדנו בהם עבור הגרפים הקודמים. ניתן להבין מכך שערכי הגינות גבוהים מתייחסים להוגנות רק כאשר גדלי התורים הווירטואליים הם גדולים, כלומר לאחר הרבה סבבי לימוד.*

*נצרף את הגרפים המקבילים מהמאמר עבור מודל* CIFAR-10 *:*

**

עבור ניסוי זה ניתן לראות דמיון מובהק בין הגרפים מהסימולציה שלנו לבין הגרפים מהמאמר, אמנם לא קיימות התנודות כפי שציינו בניסוי הקודם, אך המסקנות משני הגרפים הן זהות מלבד זה.

**מסקנות וביקורת על המאמר**

**מסקנות מהמאמר:**

ניתן לראות כי תוצאות המאמר ותוצאות הסימולציות שביצענו מראות בצורה חד משמעית כי שימוש באלגוריתם RBCS-F מניב דיוק גבוה יותר מאשר שימוש באלגוריתם FedCS שלא ממש הוגנות כלל.  
לעומת זאת, אל מול האלגוריתם הרנדומלי ההוגן ביותר, RBCS-F בעלי פקטורי הוגנות (ענישה) גבוהים הראו פער מסוים בתוצאות הדיוק הסופיות עבור מספר סבבים סופי.  
התוצאות שהתקבלו אכן מוכיחות את ההשערות התיאורטיות המניחות כי התכנסותו של האלגוריתם לכדי אורך תור וירטואלי סופי קורת לכל פקטור הוגנות, ניתן לראות זאת לפי הגרפים השונים ופרט לפי הגרף הראשון שצירפנו.  
  
נראה כי האלגוריתם החדש אכן מצליח לשפר את הוגנות בחירת המשתתפים תוך שמירה על זמני החלפה נמוכים יחסית, אך בדיקה נוספת עבור מספר סיבובים גדול יותר ופקטורי הוגנות גבוהים יותר צריכה להתקיים על מנת לאשר כי הבטחת ההוגנות אכן מתקיימת בצורה חד משמעית, ללא תלות במספר הסיבובים או קביעת פקטור ההוגנות.  
  
לסיכום, נראה כי המאמר מאיר באור חיובי על תחום ההגינות בלימוד המאוחד. השיפור בדיוק התוצאות והרווח החברתי הגבוה כתוצאה מהבחירה ההוגנת מעיד על שיטה שלדעתנו עתידה להצליח ולהשתלב במערכות מבוזרות שונות.

**חוזקות וחולשות במאמר:**

נציין כמה חוזקות וחולשות בהן נתקלנו במהלך קריאת המאמר:  
  
חוזקות:

1. המאמר מכיל את כל הפיתוחים המתמטיים המתאימים על מנת להדגים בצורה טובה את אופי פתרון הבעיה וכיצד על ידי שימוש בכלים מתמטיים ואלגוריתמיקה פשוטה ניתן לפתור אותה.  
   המאמר מדגים בצורה טובה את המעבר מהסתכלות על הבעיה כבעיית Offline לבעיית תכנות לינארי בזמן-אמת על ידי שימוש ב- Lyapunov ופיתוחים מתמטיים נלווים.
2. הניסויים המצורפים למאמר מדגימים בצורה טובה את יעילותו של האלגוריתם ומוכיחים כמעט בצורה חד משמעית את החומר התיאורטי העומד מאחורי האלגוריתם, בנוסף, בזכות ההסברים המורחבים הצלחנו לשחזר בצורה אפקטיבית את הניסויים בעצמנו.
3. המאמר פורץ דרך בתחומו, כפי שצוין במאמר וכפי שניתן לראות מהחומר המצורף אליו, לא קיים עד לרגע כתיבת מאמר זה שום אלגוריתם המממש הוגנות בלימוד המאוחד, עצם המחשבה על אלגוריתם הוגן בתהליכי אימון עבור בינה מלאכותית ראויה להערכה.

חולשות:

1. המאמר מדגים את אופן התנהגותו של האלגוריתם עבור פקטורי הגינות נמוכים יחסית וגם עבור מספר סבבי לימוד קטן יחסית, לכן ישנו מקום לניסויים נוספים שיתמכו בתוצאות המאמר למקרי קיצון.
2. למרות שתוצאות הניסויים שלנו היו קרובות מאוד לאלו במאמר, קיים פער מסוים בין רמת המובהקות של תוצאות המאמר לבין התוצאות שלנו, יתכן כי ישנה תלות באקראיות או בהנחות חסרות שלא צוינו במפורש.
3. בתור מאמר ראשון בתחומו, נראה כי היה חסר ניתוח תיאורטי עמוק על פקטור ההגינות, אך כאמור לא קיים חומר מקדים בנושא.

**כיווני מחקר עתידיים:**

לאור התוצאות החיוביות מהמאמר לא מן הנמנע שהיינו מצפים לראות את השתלבות האלגוריתם או אלגוריתמים אחרים המקיימים הוגנות בתהליכי לימוד מכונה מבוזר בעתיד.  
אנו סבורים כי אף ניתן לפתח אלגוריתמים מתוחכמים יותר, אולי כאלו שייקמו הוגנות במהלך כל סבבי הלימוד ללא תלות בפקטור הוגנות מסוים, או אולי טכניקות שיערוך חדשות שניתן לממש.  
בנוסף, אנו חושבים שישנו צורך לבדיקות נוספות עבור ערכים קיצוניים יותר באלגוריתם הקיים, היינו מציעים לכותבי המאמר לבצע ניתוח מעמיק יותר, כזה שגם לוקח בחשבון תהליכי לימוד ארוכים, ניתוח עמוק של פקטור ההוגנות והשפעתו על תהליכי לימוד ארוכים לדעתנו חסרה בנושא כרגע.  
  
מאידך, אנו יודעים כי מהירות לעיתים עדיפה על דיוק, לכן היינו מציעים לכותבי המאמר להתמקד גם בניתוח מעמיק הנותן אינדיקציה מספרית למידת התועלת מהמעבר לתהליכים הוגנים.  
שאלת ההגינות אל מול מהירות הלימוד מקבלת ייחס עד רמה מסוימת במאמר, אך לא קיימת תשובה חד משמעית בנושא, כאמור, למרות תוצאות הדיוק הגבוהות, ישנו מקום לבדיקת הרווח (או המחיר לעומת תועלת) במעבר לאלגוריתמים הוגנים בלימוד המאוחד.

**נספחים**

1. Proof 1:

According to the queue theory (see in Theorem 2.5, [22]), if all the virtual queues remain mean rate stable across the FL process (or formally, ), the time  
average arrival rates of the queue will be smaller than the service rates, namely, we have:

Through basic mathematics operations, we can reconstruct the above inequality into the form of (2) with ease. This completes the proof.

1. Proof 2:  
     
   The complete proof is given in Appendix A, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/10.1109/ TPDS.2020.3040887.
2. Proof 3:  
     
   The complete proof is given in Appendix C, available in the online supplemental material.
3. Proof 4:  
     
   The complete proof is given in Appendix D, available in the online supplemental material.

**סימוכין**

[1] T. Nishio and R. Yonetani, “Client selection for federated learning with heterogeneous resources in mobile edge,” in Proc. IEEE Int. Conf. Commun., 2019, pp. 1–7.

[2] Q. Zeng et al., “Energy-efficient radio resource allocation for federeated Edge learning,” in Proc. IEEE Int. Conf. Commun. Workshops, 2020, pp. 1–6.

[3] F. Li, J. Liu, and B. Ji, “Combinatorial sleeping bandits with fairnness constraints,” IEEE Trans. Netw. Sci. Eng., vol. 7, no. 3, pp. 1799–1813, Third Quarter 2020.  
  
[4] S. Deng, H. Zhao, J. Yin, S. Dustdar, and A. Y. Zomaya, “Edge intelligence: The confluence of Edge computing and artificial intelligence,” 2019, arXiv: 1909.00560   
  
[5] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, “InEdge AI: Intelligentizing mobile edge computing, caching and communication by federated learning,” IEEE Netw., vol. 33, no. 5, pp. 156–165, Sep./Oct. 2019.   
  
[6] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, “Edge intelligence: Paving the last mile of artificial intelligence with Edge computing,” arXiv: 1905.10083, May 2019. [Online]. Available: http://arxiv.org/abs/1905.10083   
  
[7] Y. Kang et al., “Neurosurgeon: Collaborative intelligence between the cloud and mobile edge,” ACM SIGARCH Comput. Archit. News, vol. 45, no. 1, pp. 615–629, 2017.   
  
[8] B. McMahan et al., “Communication-efficient learning of deep networks from decentralized data,” Artif. Intell. Statist., pp. 1273–1282, 2017.   
  
[9] A. Hard et al., “Federated learning for mobile keyboard prediction,” 2018, arXiv: 1811.03604.   
  
[10] S. Ramaswamy, R. Mathews, K. Rao, and F. Beaufays, “Federated learning for emoji prediction in a mobile keyboard,” 2019, arXiv: 1906.04329.   
  
[11] Y. Liu et al., “Fedvision: An online visual object detection platform powered by federated learning,” 2020, arXiv: 2001.06202.   
  
[12] E. Jeong, S. Oh, H. Kim, J. Park, M. Bennis, and S.-L. Kim, “Communication-efficient on-device machine learning: Federated distillation and augmentation under non-iid private data,” 2018, arXiv: 1811.11479.   
  
[13] L. Liu et al., “Client-edge-cloud hierarchical federated learning,” in Proc. IEEE Int. Conf. Commun., 2020, pp. 1–6.   
  
[14] N. Yoshida et al., “Hybrid-FL for wireless networks: Cooperative learning mechanism using non-IID data,” in Proc. IEEE Int. Conf. Commun., 2020, pp. 1–7.   
  
[15] D. Ye, R. Yu, M. Pan, and Z. Han, “Federated learning in vehicular edge computing: A selective model aggregation approach,” IEEE Access, vol. 8, pp. 23 920–23 935, 2020.   
[16] H. H. Yang, Z. Liu, T. Q. Quek, and H. V. Poor, “Scheduling policies for federated learning in wireless networks,” IEEE Trans. Commun., vol. 68, no. 1, pp. 317–333, Jan. 2020.   
  
[17] C. Xie, S. Koyejo, and I. Gupta, “Asynchronous federated optimization,” 2019, arXiv: 1903.03934.   
  
[18] W. Wu, L. He, W. Lin, S. Jarvis, R. Mao, and C. Maple, “SAFA: A semi-asynchronous protocol for fast federated learning with low overhead,” 2019, arXiv: 1910.01355.   
  
[19] J. Kang, Z. Xiong, D. Niyato, H. Yu, Y.-C. Liang, and D. I. Kim, “Incentive design for efficient federated learning in mobile networks: A contract theory approach,” in Proc. IEEE VTS Asia Pacific Wireless Commun. Symp., 2019, pp. 1–5.   
  
[20] L. U. Khan et al., “Federated learning for edge networks: Resource optimization and incentive mechanism,” IEEE Commun. Mag., vol. 58, no. 10, pp. 88–93, 2020.   
  
[21] E. Bagdasaryan et al., “How to backdoor federated learning,” in Proc. Int. Conf. Artif. Intell. Statist., 2020, pp. 2938–2948.  
  
[22] M. J. Neely, “Stochastic network optimization with application to communication and queueing systems,” Synthesis Lectures Commun. Netw., vol. 3, no. 1, pp. 1–211, 2010