

כותרת המאמר היא "תוכנית שימור הפרטיות בשיתוף פעולה". כותרת זו באה לבטא בעיה נפוצה במערכות הדורשות שיתוף ידע בין מספר סוכנים. מערכת כזו, שנשענת על שיתוף פעולה והפצת מידע אישי כדי להשיג מטרה מסוימת, מצידה דורשת כביכול דרישה מקסימלית לחשיפת מידע, דבר שפוגע בפרטיות המשתתפים עצמם. ככלל, ככל שנדרש שיתוף הפעולה ושיתוף המידע יהיה גדול יותר על מנת להשיג את המטרה, כך גם נפגעת פרטיות כל משתתף. הצורך בשמירה על פרטיות המידע של כל משתתף עם הצורך להשיג מכל אחד כמות מידע גדולה ילך ויגדל ככל שאפליקציות ותוכנות יורחבו אל כל תחומי החיים. הצורך במידול של הבעיה והצגת האלגוריתמים הקיימים מקל על היכולת לפתח פתרונות חדשים ומותאמים ולהצביע על בעיות שיכולות להיווצר עפ"י המודל.

המאמר בא לרכז 4 נושאים מרכזיים בבעיה הזו (של שמירת פרטיות והסתרת מידע בשיתוף פעולה):

1. המאמר מתאר את המודל שאליו נכניס בעיות מסוג זה (מבנה בעיות התכנון). את המודל (הנקרא STRIPS והרחבתו MA-STRIPS), פיתחו שני חוקרים ישראלים רונן ברפמן (בן גוריון) וכרמל דומשלק (טכניון). במאמרם הם הראו שפתרון של מיפוי אזורים "ציבוריים" ו"פרטיים" הוא בסיבוכיות פולינומיאלית בגודל מספר המשתתפים שנדרשים לפתרון הבעיה (לכל סוכן כזה משוואת פולינום בלבד). פתרון אסוציאטיבי לבעיה הוא אקספוננציאלי. המודל מסווג את פרטי הבעיה לקבוצות – פרטים ציבוריים, פרטים אישיים (פרטיים), המשתתפים עצמם. כל הקבוצות נכנסות למודל המציין: **מצב התחלתי, מצב המטרה, מצב נוכחי ו"פעולה" המורכבת משני ערכים – תנאי מקדים ואפקט על המצב**. למודל מספר כללים על מנת שהאלגוריתמים והתיאוריות יהיו מותאמים. פעולות ופרטים אישיים (עובדות אישיות) אינם חשופי לשאר המשתתפים, פרטים ציבוריים חשופים לכולם, מטרת שיתוף הפעולה ידוע לכולם, פעולות אישיות ופרטיות אינן יכולות להשפיע על ההתנהגות הכללית. תיאור המודל במאמר כדוגמה נעשה באמצעות משאיות שצריכות להעביר חבילות ומרכזים לוגיסטיים.

2. המאמר מציין מספר הגדרות פרטיות עפ"י המודל STRIPS: (הגדרות הפרטיות גם הן נבחנו בידי ברפמן ודומשלק) פרטיות חלשה – המציינת את רמת הסקת המסקנות של משתתפים אחרים מהתוכנית הציבורית. למשל, אם בתוכנית הציבורית נדרש שסוכן מס' 3 יאסוף את החבילה ממרכז לוגיסטי (ציבורי) כלשהו – יוכלו שאר המשתתפים להסיק שלסוכן מס' 3 יש גישה אל אותו מרכז לוגיסטי ויש לו בעלות על המשאית (או על אחת מהמשאיות) עם גישה אל אותו מרכז לוגיסטי (ציבורי). הסקת המסקנות משפיעה על רמת הפרטיות והופכת אותה לחלשה. פרטיות חזקה – פרט או עובדה מסוימת נחשבת לפרטית בצורה חזקה אם שאר הסוכנים לא יכולים להסיק את העובדה ע"י הסקת מסקנות מעובדות ציבוריות. אלגוריתם יחשב כעומד בקריטריון של שמירה על פרטיות חזקה אם אפשר להסיק מתוך התכנון רק את רצף פעולות ציבוריות המתקבלות כתוכנית הציבורית, ההודעות בין הסוכנים במהלך תכנון התוכנית הציבורית והחלק הפרטי שהוא חלקם שלהם בלבד. סיפוק רמה כזו של פרטיות כל כך קשה עבור אלגוריתם – שידוע רק על שני אלגוריתמים שמספקים פרטיות חזקה וגם זאת רק לאחר תנאים מסוימים בלבד. אלגוריתמים אחרים שמנסים לספק פרטיות חזקה אינם שלמים בהגדרתם או אינם רשמיים. (רשמיים במובן זה שלכל בעיה נתונה מחושב הפתרון הציבורי עפ"י מצבים פרטיים)

שתי ההגדרות הראשונות הן קיצוניות ולכן באו שתי הגדרות ביניים:

פרטיות סוכן – היא פרטיות בה אין אפשרות להסיק על קיומו של סוכן אחר שלא נמצא בתת קבוצה של שיתוף מידע. (תת קבוצה היא כזו שמאגדת מספר משתתפים תחת עובדות

פרטיות רק לקבוצה) כלומר – כל משתתף מכיר את קיימותם ופעולותם של שכניו בלבד ואינו מודע לקיומם של משתתפים אחרים ובטח שלא למשימות הפרטיות שלהם.
פרטיות קרדינאלית – שום סוכן אינו יכול לדעת מהו השטח הפרטי שעליו שולט סוכן אחר (כמה ערים) ואילו משאבים יש לו על מנת לפתור את הבעיה (מספר משאיות או מספר חבילות) אבל אפשרי שמשתתף ידע על קיומם של כל הסוכנים המשתתפים.

גישות הפרטיות השונות מגבילות את פיתוח האלגוריתם ומהוות בעיה. כאשר אלגוריתם נתקל בבעיה שיש עליה יותר מדי פתרונות אפשריים ומצבים תלויים וחסר מידע, הוא מתפשר על רמת הפרטיות שלו כדי למקד את חיפוש המסלול.

3. המאמר מעלה שתי גישות של אלגוריתמים שמפותחים על מנת לפתור את בעיית התכנון:
א. אלגוריתם שמבוסס על "סכמת קאורדינאטות" – כלומר לפי אזורים של כל סוכן - ומחלק את פתרון הבעיה לתכנון ציבורי שאינו מפורט ולאחר מכן תכנון פרטי מפורט עבור כל אחד מהסוכנים. נמנים עם קבוצה זו אלגוריתם GPPP - אלגוריתם "גרידי" שמביא פתרון חלקי אך נתקל בבעיות רבות, ואלגוריתם DPP
ב. אלגוריתם שמבוסס על חיפוש מבוצר – נמנה עם קבוצה זו אלגוריתם MAFS ואלגוריתם MADLA.

4. היוריסטיקה – שתי הגישות של האלגוריתמים שמתיימרים להעלות פתרונות לבעיות מהסוג הזה משתמשות בתכנון ובחיפוש "היוריסטי" כדי לתכנן את המסלול עצמו של כל סוכן פרטי. הפונקציות ההוריסטיות חייבות להיות אינפורמטיביות וקלות לחישוב בכל אלגוריתם אך ב-CPPP החישוב שלהן חייב גם לשמור על אותה רמת פרטיות של תהליך התכנון. ההתאמה של חישובים היוריסטים למודל בעיית CPPP נבדקה פעמים רבות במחקרים שונים.
תכנון היוריסטי FF (Fast Forward) מבצע הפחתה על גרף – התכנון הזה יכול להתאים למודל של בעיות CPPP לאחר שהסוכנים בנו גרף תכנון ציבורי ביחד.
תכנון היוריסטי Landmarks – כל סוכן מחליט על איזור מסומן שאותו יפתח ומחזיר לתוכנית הציבורית איזור מסומן אחר שצריך להתפתח (ומשתתף אחר ייקח).

המאמר בא לסכם את כל ההתקדמות הקיימת בנושא הזה של שמירת פרטיות, להגדיר אלו פתרונות קיימים ולאילו קטגוריה הפתרונות משתייכים על מנת לסקר פערים בהתקדמות ותשומת דגש על בעיות שעדיין לא נפתרו בתחום הזה.

המאמר מציג מספר אפשרויות למחקר עתידי ולפיתוח בתחום הזה. שאלות מחקר כמו מה קורה כאשר מידע אישי הופך לציבורי אחרי זמן מסוים? או האם ניתן להגביל את ההגדרה לעובדות ציבוריות בלבד (כל הפעולות הן פרטיות)?
כמו כן, ניתוח של גרף דינאמי או גרף גדל עם שינויים בהתאם למציאות.
דברים אלה הם שאלות ומצבים שראויים להתייחסות ומחקר מעמיק – שנדרש עבורם ידע נרחב יותר והתעניינות גבוהה יותר מצד המחקרים.

לדעתי, המאמר לא מציין איך אפשר להשתמש בכלים שהוזכרו כדי לפתור בעיות נרחבות. המאמר לא נוגע בסיבוכיות והשלכות הנובעות משינויים (אלא רק מזכיר את המאמרים שכן דנים בכך..). המאמר לא מזכיר את הדרישות הבסיסיות למודל על מנת שיתקיים בסיבוכיות נדרשת. המאמר לא מטפל בשגיאות ובשיקולים אנושיים מציאותיים אלא רק בנתונים יבשים – כאשר הפתרון נועד לאפליקציות/חברות הפועלות בעולם האמיתי – נדרש עולם מושגים ספציפי יותר ומותאם יותר עבור כל קבלת החלטה בפועל.

המאמר אינו מחדש נוסחאות או רעיונות חדשים – הוא מביא מספר מאמרים ומסכם את הנושא וההתקדמות שבו עד לכאן.