

1 מבוא: סוכני AI ופרוטוקול MCP

1.1 מהו סוכן AI?

סוכן AI הוא תוכנה אוטונומית. הסוכן מקבל מידע מהסביבה. הוא מעבד את המידע. לאחר מכן הוא מבצע פעולות.

סוכן AI שונה מתוכנית רגילה. תוכנית רגילה מבצעת הוראות קבועות מראש. סוכן AI מחליט בעצמו מה לעשות. ההחלטה מבוססת על המצב הנוכחי.

1.1.1 מאפיינים של סוכן AI

לכל סוכן AI יש מספר מאפיינים:

- **אוטונומיות** – הסוכן פועל באופן עצמאי.
- **תפיסה** – הסוכן קולט מידע מהסביבה.
- **פעולה** – הסוכן משפיע על הסביבה.
- **תכליתיות** – לסוכן יש מטרה מוגדרת.

בספרו של ד"ר יורם סגל "סוכני AI עם MCP" [1], מוסבר כיצד סוכנים מתקשרים. הספר מציג את פרוטוקול MCP בהרחבה. אנו נשתמש בעקרונות אלה בתרגיל.

1.2 פרוטוקול MCP – Model Context Protocol

MCP הוא פרוטוקול תקשורת. הפרוטוקול פותח על ידי חברת Anthropic. הוא מאפשר לסוכני AI לתקשר זה עם זה.

1.2.1 עקרונות הפרוטוקול

הפרוטוקול מבוסס על מספר עקרונות:

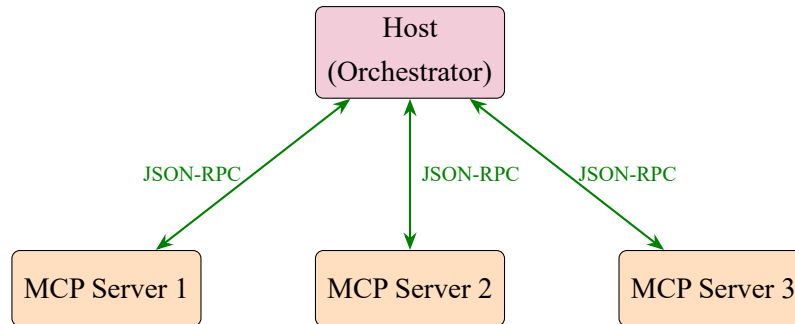
1. **הודעות מובנות** – כל הודעה היא אובייקט JSON.
2. **תקן JSON-RPC 2.0** – הפרוטוקול משתמש בתקן זה.
3. **כלים (sloot)** – סוכנים חושפים פונקציות כ"כלים".
4. **תחבורה גמישה** – אפשר להשתמש ב-HTTP או stdio.

1.2.2 ארכיטקטורת Host/Server

במערכת MCP יש שני סוגי רכיבים:

שרת MCP – רכיב שמספק שירותים. השרת חושף "כלים" שאפשר לקרוא להם. כל כלי הוא פונקציה עם פרמטרים מוגדרים.

מארח (Host) – רכיב שמתאם בין שרתים. המארח שולח בקשות לשרתים. הוא מקבל תשובות ומעבד אותן.



1.3 תחבורת HTTP על localhost

בתרגיל זה נשתמש בתחבורת HTTP. כל סוכן יפעל על פורט שונה ב-localhost.

1.3.1 הגדרת פורטים

נגדיר פורטים קבועים לכל סוכן:

- League Manager – פורט 8000

- Referee – פורט 8001

- שחקנים – פורטים 8101 עד 8104

כל סוכן מממש שרת HTTP פשוט. השרת מקבל בקשות POST בנתיב /mcp. תוכן הבקשה הוא JSON-RPC 2.0.

1.3.2 דוגמה לכתובת סוכן

כתובת שרת League Manager:

`http://localhost:8000/mcp`

כתובת שרת שחקן ראשון:

`http://localhost:8101/mcp`

1.4 מבנה הודעת JSON-RPC

כל הודעה בפרוטוקול היא אובייקט JSON. להודעה יש מבנה קבוע.

מבנה בסיסי של הודעה

```
{
  "jsonrpc": "2.0",
  "method": "tool_name",
  "params": {
    "param1": "value1",
    "param2": "value2"
  },
  "id": 1
}
```

השדות בהודעה:

- jsonrpc – גרסת הפרוטוקול, תמיד "2.0".

- method – שם הכלי שרוצים להפעיל.

- params – פרמטרים לכלי.

- id – מזהה ייחודי לבקשה.

1.5 מטרת התרגיל

בתרגיל זה נבנה מערכת ליגה לסוכני AI. המערכת תכלול שלושה סוגי סוכנים:

1. **מנהל ליגה (League Manager)** – מנהל את הליגה, כולל רישום שחקנים ושופטים.

2. **שופט (Referee)** – נרשם למנהל הליגה ומנהל משחקים בודדים.

3. **סוכני שחקן (Player Agents)** – משתתפים במשחקים.

תהליך הרישום: לפני תחילת הליגה, גם שופטים וגם שחקנים חייבים להירשם אצל מנהל הליגה. מנהל הליגה שומר רשימה של שופטים זמינים ומקצה אותם למשחקים. המשחק הספציפי בתרגיל הוא "זוגי/אי-זוגי". הפרוטוקול הכללי מאפשר להחליף משחק בעתיד. אפשר יהיה להשתמש באיקס-עיגול, 12 שאלות, או משחקים אחרים.

1.5.1 יעד הלמידה

בסיום התרגיל תוכלו:

- להבין את פרוטוקול MCP.
- לבנות שרת MCP פשוט.
- לתקשר בין סוכנים שונים.
- להריץ ליגה מלאה בסביבה שלכם.

- לוודא תאימות פרוטוקול עם סטודנטים אחרים.

חשוב: כל הסטודנטים ישתמשו באותו פרוטוקול. זה יאפשר לסוכנים שלכם לשחק זה נגד זה בעתיד.