не очікує остаточного формування взаємоблокування процесів. Він реагує на появу небезпечної ресурсної залежності ще на етапі очікування зайнятого ресурсу. Саме це створює можливість для попереджувального втручання.

Отже, запропонований метод прогнозування стану взаємоблокування процесів у комп'ютерній системі забезпечує своєчасне визначення процесів, ресурсна взаємодія яких може призвести до взаємоблокування. Він поєднує формалізований опис процесів у вигляді сигнатур, базу нечітких правил, пороговий механізм відбору небезпечних станів і процедуру вибору процесу для керуючої дії. Це дозволяє перейти від пасивного спостереження за ресурсними подіями до активного попередження взаємоблокування процесів.

Удосконалення механізмів синхронізації на основі довіри у багаторівневій архітектурі мереж 6G

УДК 004.056.53

Максим Толкачов[1], Наталія Дженюк[2], Гліб Хівренко[3]

Національний технічний університет «Харківський політехнічний інститут», [1]maksymtolkachov@gmail.com, [2]natalidzh16@gmail.com, Харківський національний університет радіоелектроніки, [3]hlib.khivrenko@nure.ua

У сучасних мережах покоління 6G відбувається інтеграція розподіленого штучного інтелекту, програмно-керованих мереж та віртуалізації мережевих функцій, семантичних комунікацій і механізмів оркестраційної взаємодії в єдине когнітивне середовище взаємодії [1], [2]. У таких архітектурах критичну роль відіграють механізми синхронізації контексту, через які здійснюється передавання параметрів довіри, оркестраційних команд, рішень штучного інтелекту та оновлень семантичного стану між рівнями мережі. Компрометація цих механізмів може призвести до каскадної дестабілізації всієї архітектури 6G через поширення фальшивих оркестраційних команд, семантичного спотворення та шкідливих оновлень моделей штучного інтелекту [4].

У роботі запропоновано самоорганізовану модель синхронізації довіри як удосконалення механізмів довірчої синхронізації для багаторівневої архітектури мереж 6G. Основна ідея моделі полягає у використанні самоорганізованих карт Кохонена для формування самоорганізованого простору довіри між рівнем штучного інтелекту, програмно-керованими контролерами мережі, ядром довіри та рівнем оркестрації [3]. На відміну від класичних механізмів довірчої синхронізації, де коефіцієнт довіри формується переважно на основі статистичних або репутаційних параметрів, запропонований підхід враховує поведінкові, часові, семантичні та когнітивні характеристики контекстних повідомлень.

Кожне контекстне повідомлення описується багатовимірним вектором ознак:

$$X_j = (T_{node}, F_{sync}, H_{sem}, D_{net}, A_{conf}, \Delta\tau, B_{stab}, P_{valid}, R_{dev}), \quad (1)$$

де T_{node} – коефіцієнт довіри до вузла, F_{sync} – частота оновлень синхронізації, H_{sem} – семантична ентропія повідомлення, D_{net} – відхилення поточного стану

мережі, A_{conf} – рівень впевненості моделі штучного інтелекту, B_{stab} – коефіцієнт поведінкової стабільності.

Після нормалізації ознак повідомлення подається на самоорганізовані карти, де визначається нейрон-переможець:

$$MU = \arg\min_{t} \mathrm{P}\hat{X}_j - W_i \mathrm{P}. \quad (2)$$

На основі топологічної відстані до довіреного кластера формується SOM-коефіцієнт довіри:

$$T_{som}(m_j) = \frac{1}{1+d_j}. \quad (3)$$

Інтегральний коефіцієнт довіри визначається як:

$$T_{\text{int}} = \alpha T_{node} + \beta T_{som} + \gamma H_{sem} + \delta A_{conf} + \lambda P_{valid} \quad (4)$$

де $\alpha, \beta, \gamma, \delta, \lambda$ – вагові коефіцієнти моделі.

Для перевірки ефективності запропонованого підходу проведено експериментальне моделювання на наборі з 1000 контекстних повідомлень між рівнями архітектури 6G. У процесі моделювання розглядалися атаки семантичного спотворення, фальшиві оркестраційні команди та шкідливі оновлення моделей штучного інтелекту типу Byzantine як типові міжрівневі загрози для середовищ, орієнтованих на використання розподіленого штучного інтелекту.

Результати експериментального моделювання показали, що використання самоорганізованої моделі синхронізації довіри дозволяє підвищити ефективність виявлення міжрівневих атак у мережах 6G, орієнтованих на використання розподіленого штучного інтелекту. Зокрема, показник повноти виявлення атак зріс із 94,67% для класичних механізмів довірчої синхронізації до 99,2% для моделі на основі самоорганізованих карт. При цьому загальна точність системи досягла 98,8%, а F1-міра перевищила 98%. Отримані результати підтверджують, що застосування самоорганізованих карт дозволяє не лише оцінювати статичний рівень довіри до вузла, а й аналізувати поведінкову топологію контекстних повідомлень у багатовимірному просторі міжрівневої взаємодії.

Запропонований підхід забезпечує можливість раннього виявлення семантичного спотворення, аномальних оркестраційних шаблонів та шкідливих оновлень моделей штучного інтелекту ще до моменту поширення каскадних керуючих помилок між рівнем штучного інтелекту, програмно-керованими контролерами мережі та системами оркестрації. Це дозволяє розглядати самоорганізовану модель синхронізації довіри як перспективний механізм побудови адаптивних систем довірчої синхронізації для багаторівневої архітектури мереж 6G.

1. M. Z. Chowdhury, M. Shahjalal, S. Ahmed and Y. M. Jang, “6G Wireless

Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions," IEEE Open Journal of the Communications Society, vol. 1, pp. 957–975, 2020. DOI: 10.1109/OJCOMS.2020.3010270.

2. N. H. Mahmood, H. Alves, O. A. López, M. Shehab, D. P. M. Osorio and M. Latva-aho, "Six Key Features of Machine Type Communication in 6G," IEEE Communications Standards Magazine, vol. 5, no. 1, pp. 34–40, 2021. DOI: 10.1109/MCOMSTD.001.2000034.
3. T. Kohonen, "The Self-Organizing Map," Proceedings of the IEEE, vol. 78, no. 9, pp. 1464–1480, 1990. DOI: 10.1109/5.58325.
4. H. Sedjelmaci and S. M. Senouci, "An Accurate and Efficient Collaborative Intrusion Detection Framework to Secure Vehicular Networks," Computers & Electrical Engineering, vol. 43, pp. 33–47, 2015. DOI: 10.1016/j.compeleceng.2015.02.018.