УДК 004.056.53:004.89:621.39 DOI: 10.31673/2412-4338.2026.019005

Хворостяний Родіон Віталійович
аспірант Навчально-наукового інституту кібербезпеки та захисту інформації
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0009-0004-4591-7100
rodionhvorostyanoy@gmail.com

Туровський Олександр Леонідович
доктор технічних наук, професор, завідувач кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0002-4961-0876
s19641011@ukr.net

МЕТОД ВЗАЄМОДІЇ АГЕНТІВ В МУЛЬТИАГЕНТНІЙ СИСТЕМІ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТРАНСПОРТНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ПІД ЧАС ДІАГНОСТУВАННЯ КІБЕРАТАК

Анотація: *У статті досліджується проблема організації мультиагентної системи управління кібербезпекою телекомунікаційних мереж (ТТМ) в умовах зростання складності та прихованості кібератак. Запропоновано ієрархічну модель системи, що поєднує локальні та глобальні контури управління й узгоджується зі структурною організацією ТТМ. Визначено базові типи агентів, зокрема моніторингу, виявлення загроз, оцінки ризику, прийняття рішень, реагування та координації, а також агенти сервісного та організаційного рівнів. Розкрито їх функціональне призначення та інформаційні зв'язки в межах єдиного циклу управління. Запропоновано класифікацію кібератак за ознакою діагностичної визначеності. Виокремлено діагностично визначені атаки, що супроводжуються виходом параметрів мережі за допустимі межі та можуть бути виявлені засобами базової діагностики, і діагностично невизначені (стелс-атаки), які не порушують контрольованих показників і потребують додаткових інтелектуальних процедур аналізу. Обґрунтовано, що для ТТМ характерна поява стелс-атак, за яких можливе формування суперечливої інформації між агентами самодіагностики, що ускладнює однозначне встановлення факту атаки. Для підвищення ефективності діагностування запропоновано систему виявлення стелс-атак з використанням швидкого алгоритму аналізу на основі даних моніторингу та детектування загроз. У разі недостатньої достовірності результатів роботи алгоритму застосовується другий рівень із використанням розширених процедур оцінки ризику та прийняття рішень. Проведене моделювання підтвердило зростання достовірності діагностування зі збільшенням масштабу мережі та прийнятний характер її зниження при збільшенні кількості атакованих вузлів. Встановлено також, що час діагностування зростає майже лінійно та зберігає прогнозований характер, що свідчить про масштабованість і практичну придатність запропонованого підходу.*

Ключові слова*: кібербезпека, транспортна телекомунікаційна мережа, інтелектуальний агент, мультиагентна система, діагностування кібератак, стелс-атака, ієрархічна модель управління.*

Khvorostianyi Rodion
Postgraduate student at the Educational and Scientific Institute of Cybersecurity and Information Protection
State University of Information and Communication Technologies, Kyiv
ORCID 0009-0004-4591-7100
rodionhvorostyanoy@gmail.com

Oleksandr Turovsky
Doctor of Technical Sciences, Professor, Head of the Department of Technical Cybersecurity Systems
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0002-4961-0876
s19641011@ukr.net

METHOD OF AGENT INTERACTION IN A MULTI-AGENT CYBERSECURITY MANAGEMENT SYSTEM OF A TRANSPORT TELECOMMUNICATION NETWORK DURING CYBERATTACK DIAGNOSIS

Abstract: *The paper addresses the problem of organizing a multi-agent cybersecurity management system for transport telecommunication networks (TTN) under conditions of increasing complexity and stealthiness of cyberattacks.*

A hierarchical system model is proposed that integrates local and global control loops and is aligned with the structural organization of the TTN. The basic types of agents are defined, including monitoring, threat detection, risk assessment, decision-making, response, and coordination agents, as well as service- and policy-level agents. Their functional roles and information interactions within a unified control cycle are described. A classification of cyberattacks based on diagnostic determinability is proposed. Diagnostically detectable attacks, which cause network parameters to exceed permissible limits and can be identified by basic diagnostic mechanisms, are distinguished from diagnostically undetermined (stealth) attacks that do not violate controlled parameters and therefore require additional intelligent or correlation-based analysis. It is substantiated that TTNs are particularly susceptible to stealth attacks, where contradictory diagnostic information may be generated by self-diagnostic agents, complicating reliable attack identification. To improve diagnostic efficiency, a two-level stealth attack detection system is proposed. The first level implements a fast primary analysis algorithm based on monitoring and threat detection data. If the obtained results are insufficiently reliable, a second level employing enhanced risk assessment and decision-making procedures is activated. Simulation results confirm that diagnostic reliability increases with network scale and decreases acceptably as the number of compromised nodes grows. The diagnostic time increases almost linearly and remains predictable, demonstrating the scalability and practical applicability of the proposed approach.

Keywords: *cybersecurity, transport telecommunication network, intelligent agent, multi-agent system, cyberattack diagnosis, stealth attack, hierarchical control model.*

1. Вступ

В умовах постійної інтеграції телекомунікаційних технологій у критичну інфраструктуру суттєво зростають вимоги до забезпечення кібербезпеки транспортних телекомунікаційних мереж (ТТМ) [1,2]. Такі мережі характеризуються розподіленою структурою, великою кількістю взаємопов'язаних вузлів, та частковою спостережуваністю їх станів, що ускладнює своєчасне виявлення кібератак, зокрема стелс-атак, спрямованих на приховане порушення функціонування мережі [3]. Традиційні централізовані підходи до діагностування виявляються недостатньо ефективними через обмежену масштабованість, значні затримки обробки інформації та наявність єдиної точки відмови. Перспективним напрямом підвищення ефективності управління кібербезпекою ТТМ є використання мультиагентних систем, здатних забезпечувати розподілену обробку даних, локальну автономію прийняття рішень та узгодження результатів на різних рівнях управління [4,5].

2. Аналіз літературних даних і постановка проблеми

Питанням застосування мультиагентних систем до управління комп'ютерними мережами та кібербезпекою ТТМ присвячено достатньо велику кількість досліджень.

Так, у огляді мультиагентних систем для спільного виявлення вторгнень [6] підкреслюється зростаюча роль MAS у побудові колаборативних IDS та пропонується таксономія існуючих підходів, хоча і відзначається наявність відкритих проблем, серед яких недостатня узгодженість стратегій взаємодії агентів та обробка складних корельованих подій у великих мережах. У статті [7] досліджується інтеграція мультиагентної штучної інтелектуальної моделі в розподілені системи виявлення атак, підкреслюючи, що MAS можуть покращити адаптивність та ресурсоефективність DIDS, хоча і не пропонуються загальні механізми координації агентів у умовах часткової інформації та перехресних загроз.

Класична робота про розподілені IDS [8] з автономними агентами демонструє архітектуру ієрархічної взаємодії агентів без централізованого компонента, але ця модель розглядає лише базові механізми комунікації та не охоплює сучасні вимоги до гнучких стратегій узгодження рішень у контексті складних атак. Публікація [9] описує мультиагентну систему захисту IoT, де агенти координують виявлення і реагування, але водночас декларує лише загальні концептуальні рішення, які не вирішують низку практичних питань щодо ефективної взаємодії агентів у великих мережах. В огляді [10] підкреслюють потенціал мультиагентного навчання з підкріпленням у сфері захисту мереж, але також вказують на наявність проблем зі стійкістю, масштабованістю та узгодженістю агентичних стратегій у складних сценаріях атаки.

Аналіз практичних прикладів застосування моделей MAS у кіберфізичних системах [11] показує, що хоч окремі агенти можуть виконувати локальні функції захисту та адаптуватися у відповідь на зміни, питання ефективних протоколів координації, обміну контекстною інформацією та вирішення конфліктів під час колективного діагностування залишається малодослідженим. Дослідження у галузі архітектур мережних IDS [12] демонструють ефективність кооперативних агентних моделей, проте більшість з них або зводяться до централізованого аналізу зібраних даних, або не пропонують формальних механізмів взаємодії агентів у розподіленому контексті.

Таким чином, хоча мультиагентні системи доводять свою ефективність для виявлення атак у розподілених мережах, проблеми організації взаємодії агентів під час діагностування кібератак

залишаються недостатньо дослідженими, що обґрунтовує потребу в подальших роботах, спрямованих саме на розроблення узгоджених моделей співпраці та комунікації між агентами в складних мережевих середовищах.

3. Мета і задачі дослідження

Метою статті є розроблення методу взаємодії агентів у мультиагентній системі управління кібербезпекою транспортної телекомунікаційної мережі під час діагностування кібератак, який забезпечує підвищення достовірності діагностування, скорочення часу реагування та збереження властивостей масштабованості системи в умовах зростання кількості вузлів і інтенсивності дестабілізуючих впливів.

Для досягнення поставленої мети потребують вирішення такі завдання:

- обгрунтування структури мультиагентної системи управління кібербезпекою ТТМ;
- розробка діагностичної моделі мультиагентного управління кібербезпекою ТТМ;
- розробка алгоритмів взаємодії агентів при діагностуванні атаки на ТТМ;
- оцінка достовірності методу взаємодії агентів мультиагентній системі управління кібербезпекою ТТМ під час діагностування кібератак.

4. Структура мультиагентної системи управління кібербезпекою ТТМ

Ієрархічна мультиагентна система управління (рис. 1), яка пропонується, відображає багаторівневу структуру ТТМ, розміщення функціональних агентів на кожному рівні та їх логічні зв'язки, реалізуючи принципи розподілу функцій і поєднання локальної автономії з глобальною координацією в процесах виявлення загроз та реагування.

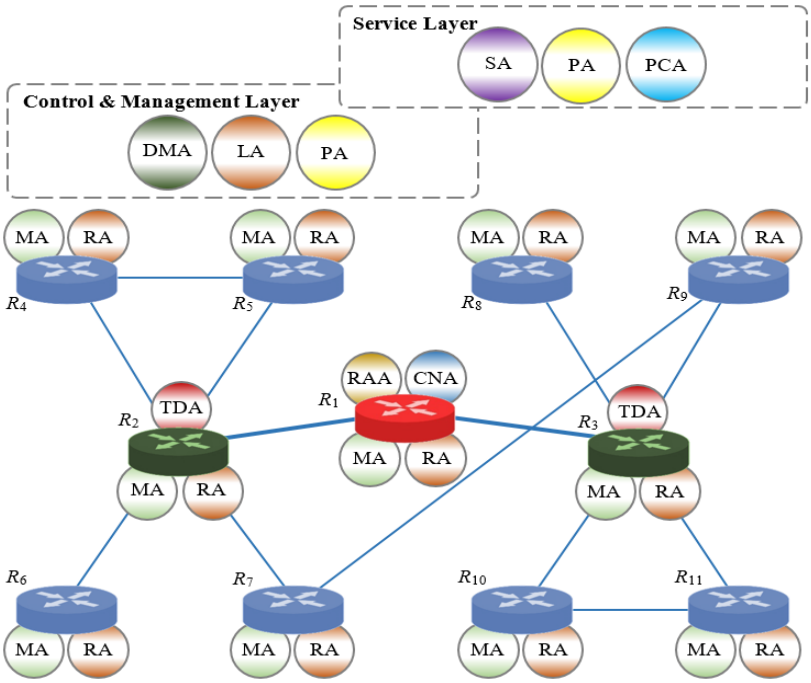

Рис. 1. Структура мультиагентної системи управління кібербезпекою ТТМ

У мультиагентній системі управління кібербезпекою ТТМ виокремлюються такі базові типи агентів:

Monitoring Agent (MA) здійснює збір і первинну обробку даних про стан елементів телекомунікаційної мережі, передає результати агентам виявлення загроз, реагування та оцінки ризику, а також отримує параметри моніторингу від координаційних і виконавчих компонентів;

Threat Detection Agent (TDA) виконує виявлення кібератак на основі аналізу аномалій, сигнатур і поведінкових характеристик мережі; передає сформовані події агентам оцінки ризику та прийняття рішень;

Risk Assessment Agent (RAA) забезпечує кількісну оцінку ймовірності та наслідків атак і формує інтегральні показники ризику для подальшого вибору стратегії реагування;

Decision-Making Agent (DMA) обирає оптимальну стратегію протидії загрозам на основі аналітичних результатів, координує взаємодію з іншими агентами та ініціює виконання керуючих дій;

Response Agent (RA) реалізує технічні заходи реагування (фільтрацію трафіку, зміну маршрутів, ізоляцію сегментів, застосування політик безпеки), забезпечуючи трансляцію управлінських рішень у конкретні мережеві дії;

Coordination–Negotiation Agent (CNA) узгоджує локальні рішення агентів відповідно до глобальної стратегії захисту, підтримуючи баланс між автономністю компонентів і цілісністю управління системою.

Окрім базових компонентів, до мультиагентної системи управління кібербезпекою ТТМ входять агенти сервісного та управлінського рівня: SLA / Service Agent (SA), Learning Agent (LA), Policy Agent (PA) і Policy Compliance Agent (PCA). Їх формальні моделі визначаються архітектурою конкретної ТТМ і класом завдань кіберзахисту, що в ній реалізуються. Таким чином, ієрархічна мультиагентна система функціонує як сукупність взаємопов'язаних локальних і глобальних контурів управління, узгоджених зі структурною ієрархією телекомунікаційної мережі.

5. Розробка методу взаємодії агентів при діагностуванні кібератак на ТТМ

Типи кібератак на ТТМ. З позиції можливостей автономного виявлення в мультиагентній системі управління кібербезпекою ТТМ доцільно виокремити два типи кібератак:

1. *Діагностично визначені атаки* (Diagnostically Detectable Cyberattacks) – спричиняють вихід параметрів функціонування мережі за допустимі межі, що забезпечує їх однозначне виявлення агентами моніторингу та виявлення загроз (MA, TDA) [13].
2. *Діагностично невизначені атаки* (Diagnostically Undetermined Cyberattacks, Stealth Cyberattacks) – не порушують нормативних значень контрольованих параметрів, тому не завжди фіксуються засобами базової діагностики й потребують додаткового інтелектуального аналізу на рівні агентів оцінки ризику та прийняття рішень (RAA, DMA) [14].

Отже, для ТТМ характерні стелс-атаки, за яких компоненти самодіагностики можуть формувати суперечливу інформацію про стан вузлів. Це зумовлює необхідність впровадження окремого ієрархічного рівня механізмів виявлення довільної або узгодженої прихованої поведінки. Відтак, пропонується дворівнева система діагностування стелс-атак. На першому рівні використовується швидший алгоритм (MA, TDA), що забезпечує мінімальні часові витрати. За недостатньої ефективності застосовується розширений алгоритм другого рівня (RAA, DMA), який забезпечує вищу якість діагностики. Такий підхід узгоджується з ієрархічною організацією мультиагентної системи управління кібербезпекою ТТМ.

Діагностична модель мультиагентного управління кібербезпекою ТТМ. При розробці такої моделі скористаємось підходом, наведеним у [15, 16]. Розглянемо ТТМ, яка складається з множини вузлів з відповідним набором агентів (рис. 1). Агент у даному випадку – це процес на апратних ресурсах певного вузла, відтак, будемо вважати, що нормальний (неатакований) стан вузла відповідає нормальній роботі самого агента.

Також, приймемо наступні припущення:

1. В системі існує механізм, що дозволяє всім агентам ТТМ одночасно, чи у певний проміжок часу, перейти до діагностування.
2. Агенти здатні обмінюватись повідомленнями з множини $Mes = \{0,1,\varnothing\}$, де 0 – відсутність атаки; 1 – вузол атакований; $\varnothing$ – відсутність повідомлення.
3. Кожен агент визначає стан його вузла $S(i)$ за допомогою засобів самодіагностування. Стан може бути: *NF* (нормально-функціонуючий) і *UA* (атакований).

Ідея методу. Під час діагностування ТТМ на наявність кібератак серед агентів, які приймають у ній участь, призначається один Master-агент, який розпочинає процедуру перевірки і якому на певний проміжок часу підпорядковуються інші Slave-агенти. Кожному Slave-агенту мережі Master-агент вузла *k* надсилає повідомлення (припущення 3). Slave-агенти $n, n = 1...N-1$ пересилають повідомлення від Master-агента один одному. Після цього кожнен Slave-агент формує матрицю, за якою визначаються Slave-агенти атакованих вузлів. В кінці процедури діагностування агенти досягають згоди з приводу "атакованих" чи "неатакованих" вузлів – виключити їх з трафіку, чи продовжити роботу.

Нелояльність (стелс-поведінка) агента полягає в тому, що в різних повідомленнях нелояльний Slave-агент передає суперечливі повідомлення іншим. Якщо в результаті діагностування кожен

лояльний агент нормально-функціонуючого вузла однозначно визначає нелояльних агентів атакованих вузлів, то можна констатувати, що угода між лояльними Slave-агентами і лояльним Master-агентом досягнута. При цьому кожним Slave-агентом враховуються думки лише лояльних агентів.

Вихідний набір, що формується *n*-м Slave-агентом, має вигляд наступної матриці

$$A_n = \begin{bmatrix} a_{11}^n & \cdots & a_{1L}^n \\ \cdots & \cdots & \cdots \\ a_{L1}^n & \cdots & a_{LL}^n \end{bmatrix}, \quad (1)$$

де $L = N - 1$ – кількість вузлів, які діагностуються.

Рядки *i* матриці (1) утворюються з векторів повідомлень всіх Slave-агентів, передані ними до Slave-агента *n*. Стовпці *j* матриці (1) утворюються з повідомлень Slave-агента *j*, які були передані ним всім *i*-м Slave-агентам. Головна діагональ матриці (1) утворюється з повідомлення *j*-х Slave-агентів a_{ij}^n, які були надіслані ними самим собі.

Рішення щодо лояльних чи нелояльних агентів, а, відповідно – атакованих чи неатакованих вузлів, приймається шляхом "голосування" із застосуванням функції *Vote*, яка обирає значення за більшістю значень елементів стовпця матриці (1). Логічно припустити, що система на основі "голосування" здатна виявити не більше половини $\left(\frac{N-1}{2}\right)$ від загальної кількості вузлів, що входять до ТТМ.

Алгоритм взаємодії агентів при діагностуванні атаки на ТТМ. Розглянемо ТТМ, яка складається з *N* вузлів з номерами $1...N$. Діагностування такої мережі здійснюється розгорнутими на вузлах агентами шляхом взаємообміну повідомленнями з іншими агентами.

Алгоритм включає наступні кроки:

1. **send_Message :** $mes_k \Rightarrow n,\ mes_k \in Mes,\ n = 1...N-1,\ n \neq k;$
2. **send_message :** $mes_k^n \Rightarrow n,\ n = 1...N-1$
3. **form_vector :** $Row(n) = \left[mes_1 \quad ... \quad mes_{N-1}\right]$
4. **send_vector :** $Row(n) \Rightarrow n$
5. **form_matrix :** $A_n = \begin{bmatrix} a_{11}^n & \cdots & a_{1L}^n \\ \cdots & \cdots & \cdots \\ a_{L1}^n & \cdots & a_{LL}^n \end{bmatrix}, L = 1...N-1$
6. **form_vector :** $Prs_n(j) = Vote\left[a_{ij}^n \middle| i = 1...L\right]$
7. **fix_elements :** $Prs_n(j_l) \middle| Prs_n(j_l) \neq a_{ij}^{n*},\ l = 1...L_{max}$
8. **if** $L_{max} \neq 0$ **then**
9. $\quad$ **logic_function :** $Susp = \bigwedge_{l=1}^{L_{max}} (i_l \vee j_l)$
10. **end if**
11. **DNF :** $Susp' = \mathrm{DNF}\left[Susp\right]$
12. **delete_terms :** $Susp'' = Susp' \middle| \textbf{not}\ Susp'_j \geq (N-1)/2$
13. **if** $\left|Susp''\right| > 1$ **then**
14. $\quad Result \leftarrow 1$
15. **else**
16. $\quad Result \leftarrow 0$
17. **end if**

18. **cross_rows_columns :** $B_n \leftarrow A_n$
19. **if** $\left(\forall i = 1...N-L,\ b_{ij} = 0\ \textbf{xor}\ 1\right)$ **then**
20. $\quad State(k) \leftarrow 0$
21. $\quad Result \leftarrow 0$
22. **else if** $\left(\forall i = 1...N-L,\ b_{ij} = 0\ \textbf{or}\ 1\right)$ **then**
23. $\quad State(k) \leftarrow 1$
24. $\quad Result \leftarrow 0$
25. $\quad$ **else if** $\left(\forall i = 1...N-L,\ b_{ij} = \left(0\ \textbf{xor}\ 1\right)\ \textbf{and}\ \left(0\ \textbf{or}\ 1\right)\right)$ **then**
26. $\quad\quad State(k) \leftarrow \varnothing$
27. $\quad\quad Result \leftarrow 1$
28. $\quad\quad$ **end if**
29. $\quad$ **end if**
30. **end if**
31. **print**$\left[Susp'', Result\right]$

Дамо пояснення основним крокам алгоритму. На кроці 1 Master-агент *k* надсилає іншим Slave-агентам *n* повідомлення mes_k. На кроці 2 Slave-агенти *n* пересилають його один одному. На кроці 3 з отриманих повідомлень кожний *n*-й агент формує вектор $Row(n) = \left[mes_1 \quad ... \quad mes_{N-1}\right]$. На кроці 4 агенти обмінюються векторами $Row(n), n = 1...N-1$, а на кроці 5 кожен агент формує базову матрицю A_n. Після цього на кроці 6 застосовується процедура голосування *Vote* до стовпців матриці A_n, та формується вектор Prs_n результатів голосування. На кроці 7 у векторі Prs_n фіксуються елементи $a_{ij}^{n^*}, i, j = 1...N-1$ матриці A_n, які відрізняються від більшості елементів стовпця: $Prs_n(j) \neq a_{ij}^{n^*}$. На кроках 8–10 визначається підозріла область $Susp = \bigwedge_{l=1}^{L_{max}} \left(i_l \vee j_l\right)$. На кроці 11 вираз $Susp$ приводиться до диз'юнктивної нормальної форми (DNF). На кроках 15–17 визначається результат діагностування: $Result = 1$ або $Result = 0$. На кроках 19–27 перевіряється стан вузла k – вузол функціонує нормально $State(k) = 0$, чи вузол атаковано $State(k) = 1$. Також визначається результат діагностування (ступінь впевненості алгоритму) $Result = 0$ – атаковані вузли визначено, або $Result = 1$ – алгоритм не виявив атаковані вузли. На кроці 31 алгоритм виводить список атакованих вузлів $Susp''$ та результати діагностування $Result$. При $Result = 1$ агент МА повідомляє агентів RAA та DMA про необхідність використання інших, більш складних, алгоритмів.

Приклад. На базі наведеної топології системи (рис. 1) для іллюстрації алгоритму розглянемо приклад, у якому ТТМ складається з $N = 11$ вузлів, кількість атакованих серед яких дорівнює $t = 4$. Атакованими вузлами визначимо Master #11 та вузли Slave #2, #4, #10. Мультиагентну систему управління кібербезпекою ТТМ можна подати у вигляді графа (рис. 2), на якому "нелояльні" агенти позначені кольором. Агенти обмінюються повідомленнями за принципом "всі–всім". Для спрощення на графі показані лише зв'язки передачі повідомлень "нелояльними" агентами.

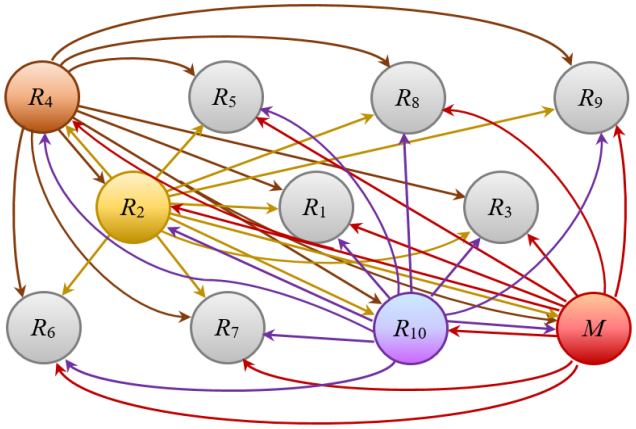

Рис. 2. Граф взаємодії в мультиагентній системі управління

Після обміну повідомленнями mes_k та векторами $Row(n)=[mes_1 \quad ... \quad mes_{N-1}]$ агенти сформували матриці A_n. Розглянемо одну із таких матриць, наприклад матрицю агента A_1, за якою, використовуючи функцію *Vote*, визначено вектор Prs_1. У такій матриці A_1 червоним кольором позначені елементи, які відрізняються від відповідних елементів вектора Prs_1.

$$A_1 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{array} \begin{array}{c} \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0^* \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0^* \\ 1 & 1^* & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0^* \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1^* & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0^* \\ 1 & 1^* & 0 & 0^* & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0^* & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

$$Prs_1 = \begin{bmatrix} 1 & \mathbf{0} & 0 & \mathbf{1} & 0 & 0 & 1 & 1 & 0 & \mathbf{1} \end{bmatrix}. \qquad (2)$$

Підозріла область для матриці (2) буде [17]:

$$\begin{aligned} Susp &= (2 \vee 10) \wedge (3 \vee 10) \wedge (4 \vee 2) \wedge (4 \vee 10) \wedge \\ &\wedge (6 \vee 2) \wedge (7 \vee 10) \wedge (8 \vee 2) \wedge (8 \vee 4) \wedge (9 \vee 4) = \\ &= (2 \wedge 4 \wedge 10) \vee (2 \wedge 8 \wedge 9 \wedge 10) \vee (4 \wedge 6 \wedge 8 \wedge 10). \end{aligned} \qquad (3)$$

Вираз (3) дає 3 рішення. Аналізуючи A_1 у поєднанні з Prs_1 бачимо, що терми $(2 \wedge 8 \wedge 9 \wedge 10)$ та $(4 \wedge 6 \wedge 8 \wedge 10)$ не відповідають процедурі $Prs_n(j)$, що дозволяє виключити їх з $Susp$ (крок 18). Рішенням (3) буде матриця B_1, яка отримана з A_1 шляхом викреслення рядків та стовпців 2, 4, 10 (вузли #2, #4, #10 вважаються атакованими)

$$B_1 = \begin{array}{c} \\ 1 \\ 3 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & 3 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}. \quad (4)$$

Для визначення стану Master-агента (вузол #11) проаналізуємо матрицю B_1. Тут видно, що агенти вузлів #1, #3, #5, #6, #7, #8, #9 отримали різні повідомлення від Master-агента. Відтак, агент #1 відзначає нелояльність Master-агента. Алгоритм діагностування виконано успішно і $Result = 0$, тобто, та визначено атаковані вузли #2, #4, #10.

Якщо результат алгоритму є неоднозначним $Result = 1$, то це свідчить або про велику кількість атакованих вузлів, або про наявність складних стелс-атак, які алгоритм не здатен виявити. У такому випадку агент *n* (рівня MA, TDA) надсилає повідомлення агентам вищого рівня (RAA, DMA), які виконують більш складну процедуру діагностування.

6. Оцінка достовірності методу взаємодії агентів мультиагентній системі управління кібербезпекою ТТМ під час діагностування кібератак

Достовірність наведених результатів теоретичних досліджень можна перевірити математичним моделюванням процедури мультиагентного діагностування ТТМ, що складаються з $N = 6…20$ вузлів. При цьому, метою експериментальних досліджень є:

− аналіз коректності алгоритму діагностування ТТМ під дією стелс-атак;

− оцінка достовірності та тривалості процедури діагностування.

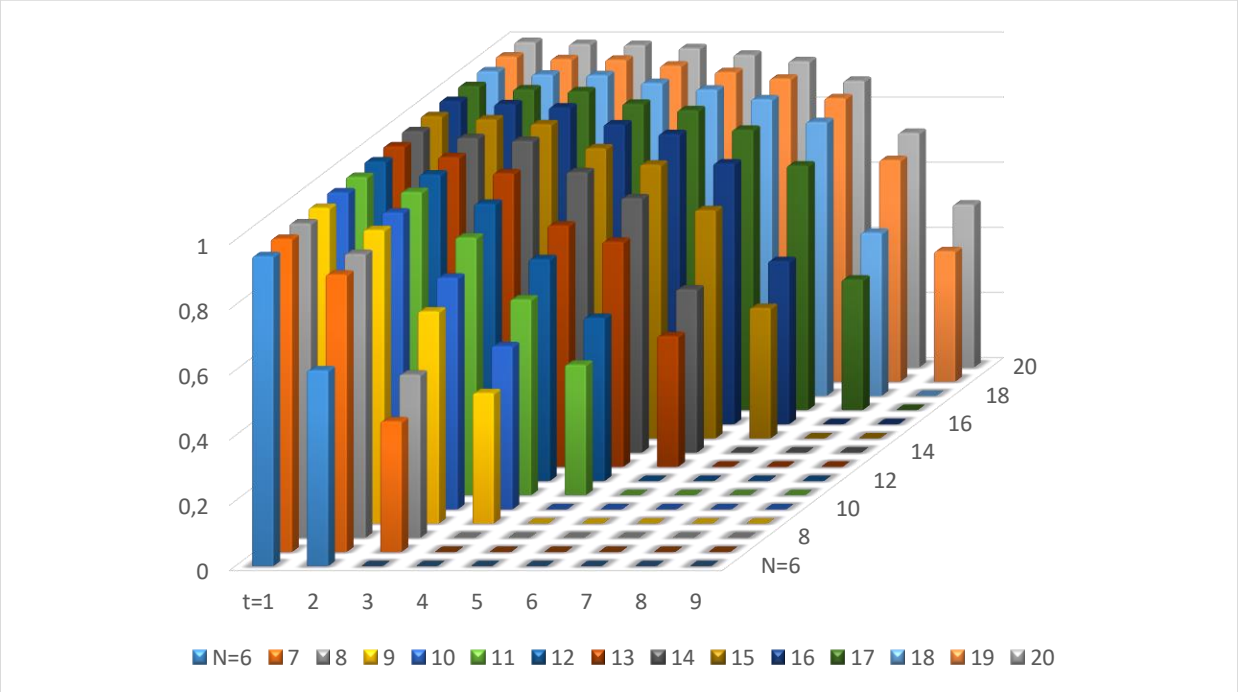

Рис. 4. Достовірність діагностування *D* в залежності від кількості атакованих вузлів *t* та кількості вузлів *N* мережі

Під час моделювання випадковим чином задавався стан вузлів ТТМ для наступних параметрів мережі: $t = 1...(N-2)/2$, де *t* – кількість атакованих вузлів, *N* – загальна кількість вузлів ТТМ. В

результаті застосування алгоритму визначався стан мережі $Sn(N)$ та несуперечливість діагностування $Result = 0$ або $Result = 1$. Достовірність діагностування визначалася шляхом порівняння заданого та отриманого розподілу атакованих вузлів у системі *D* та середній час діагностування $t_д$.

Результати, отримані під час моделювання, наведені на рис. 4 та в табл. 1.

Аналіз результатів оцінювання достовірності (рис. 4) показує, що в умовах малої кількості атакованих вузлів ($t = 1...2$) вона залишається високою в усьому діапазоні $N = 6...20$ і зростає зі збільшенням розміру мережі, що зумовлено наявністю більшої кількості неатакованих вузлів і, відповідно, розширенням інформаційної бази для узгодження локальних рішень агентів. Зі збільшенням *t* достовірність знижується, особливо в малих мережах, проте ефект масштабованості компенсує цей вплив у більших конфігураціях, забезпечуючи прийнятний рівень якості діагностування навіть при зростанні інтенсивності атак.

Таблиця 1

Час діагностування $t_д$ в залежності від кількості атакованих вузлів *t* та кількості вузлів *N* мережі (мс)

К-ть вузлів *N*	Кількість атакованих вузлів *t*								
	1	2	3	4	5	6	7	8	9
6	35,8	55,3	–	–	–	–	–	–	–
7	35,9	55,4	74,9	–	–	–	–	–	–
8	36,0	55,5	75,0	–	–	–	–	–	–
9	36,1	55,6	75,1	94,6	–	–	–	–	–
10	36,2	55,7	75,2	94,7	–	–	–	–	–
11	36,2	55,7	75,2	94,7	114,2	–	–	–	–
12	36,3	55,8	75,3	94,8	114,3	–	–	–	–
13	36,4	55,9	75,4	94,9	114,4	133,9	–	–	–
14	36,4	55,9	75,4	94,9	114,4	133,9	–	–	–
15	36,5	56,0	75,5	95,0	114,5	134,0	153,5	–	–
16	36,5	56,0	75,5	95,0	114,5	134,0	153,5	–	–
17	36,5	56,0	75,5	95,0	114,5	134,0	153,5	173,0	–
18	36,6	56,1	75,6	95,1	114,6	134,1	153,6	173,1	–
19	36,6	56,1	75,6	95,1	114,6	134,1	153,6	173,1	192,6
20	36,7	56,2	75,7	95,2	114,7	134,2	153,7	173,2	192,7

Дослідження часових характеристик (табл. 1) свідчить, що за фіксованих значень *t* тривалість діагностування зростає зі збільшенням кількості вузлів майже лінійно, що підтверджує масштабованість і ефективність паралельної обробки в ієрархічній мультиагентній архітектурі.

Водночас кількість атакованих вузлів *t* є визначальним чинником впливу на час діагностування, який зростає майже лінійно через необхідність додаткової координації та обробки аномалій. Порівняння з існуючими підходами [15, 16] демонструє, що запропонований алгоритм забезпечує виявлення більшої кількості атакованих вузлів ($t \le (N-2)/2$ проти $t \le (N-1)/3$) за подібної достовірності та менших часових витрат завдяки скороченню раундів обміну повідомленнями й обсягів переданої інформації, що також зменшує апаратні вимоги до вузлів ТТМ.

7. Висновки

В умовах зростання масштабів транспортних телекомунікаційних мереж, підвищення складності їх топології та інтенсивності цілеспрямованих кібератак особливої актуальності набуває розроблення ефективних методів координації розподілених засобів діагностування. У ході дослідження обґрунтовано доцільність застосування ієрархічної організації мультиагентної системи та розроблено метод взаємодії агентів, який забезпечує узгодження локальних рішень і формування глобального

діагностичного висновку в умовах часткової спостережуваності та можливих відмов вузлів. Запропонований підхід дозволяє зменшити обсяг службового трафіку, скоротити кількість раундів обміну повідомленнями та забезпечити коректність діагностування за значної частки уражених елементів мережі.

Отримані результати підтвердили, що розроблений метод забезпечує високу достовірність і прийнятний час діагностування зі збереженням властивостей масштабованості та стійкості до дестабілізуючих впливів. Порівняння з існуючими алгоритмами засвідчило підвищення ефективності виявлення атакованих вузлів за менших часових і ресурсних витрат, що створює підґрунтя для впровадження запропонованого методу в системах управління кібербезпекою транспортних телекомунікаційних мереж та його подальшої алгоритмічної деталізації.

Внесок авторів. Родіон Хворостяний – концептуалізація методу; розробка моделі та алгоритму; розробка програмного забезпечення та моделювання; Олександр Туровський – збір і перевірка вхідних даних; емпіричне дослідження; аналіз джерел; формулювання висновків.

Декларація про штучний інтелект

Автор не використовував штучний інтелект при створенні матеріалів статті.

Конфлікт інтересів

Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

8. Список використаної літератури

1. Голь, В. Д., & Ірха, М. С. (2021). Телекомунікаційні та інформаційні мережі. Київ, ІСЗЗІ КПІ ім. Ігоря Сікорського, 250 с. https://ela.kpi.ua/server/api/core/bitstreams/35d4a2d2-53ed-453f-9bcd-fa883a982f53/content

2. Пановик, У. П. (2024). Кібербезпека в Телекомунікаційних Мережах та Системах. Наукові Записки, 1(68), 122–135. https://nz.uad.lviv.ua/media/1-68/13.pdf

3. Khoroshko, V., Khokhlachova, Y., & Vyshnevska, N. (2023). Decomposition of Computer Network Technology In Their Design. Ukrainian Scientific Journal of Information Security, 29(3), 130–137. https://doi.org/10.18372/2225-5036.29.18072

4. Khavina, I. P., Hnusov, Yu. V., & Mozhaiev, O. O. (2022). Development of multi-agent information security management system. Law and Safety, 87(4), 171–183. https://doi.org/10.32631/pb.2022.4.14

5. Кітура, О. В. (2023). Методика формування системи управління транспортною мережею зв'язку. Дис. докт. філософії за спец. 172 “Телекомунікації та радіотехніка”. Київ, ДУТ, 133 с. https://duikt.edu.ua/uploads/p_2625_85571738.pdf

6. Bougueroua, N., et al. (2021). A Survey on Multi-Agent Based Collaborative Intrusion Detection Systems. Journal of Artificial Intelligence and Soft Computing Research, 11(2), 111–142. https://doi.org/10.2478/jaiscr-2021-0008

7. Torres, M. (2025). Enhancing Distributed Intrusion Detection Systems Using Multi-Agent AI Models. International Annals of Intelligent Learning Systems Research (IAILSR), 9, 22–35. https://iailsr.org/index.php/iailsr/article/view/13

8. Sen, J. (2011). A Distributed Intrusion Detection System Using Cooperating Agents. arXiv:1111.0382. https://doi.org/10.48550/arXiv.1111.0382

9. Aydın, H., Aydın, G. Z. G., Sertbaş, A., & Aydın, M. A. (2023). Internet of things security: A multi-agent-based defense system design. Computers and Electrical Engineering, 111(B), 108961, https://doi.org/10.1016/j.compeleceng.2023.108961

10. Landolt, C. R., Würsch, C., Meier, R., Mermoud, A., & Jang-Jaccard, J. (2025). Multi-Agent Reinforcement Learning in Cybersecurity: From Fundamentals to Applications. arXiv:2505.19837. https://doi.org/10.48550/arXiv.2505.19837

11. Козловський, О. В., & Жарікова, М. В. (2025): Розробка моделі безпеки для багатоагентної мережі в кіберфізичній системі. Вісник Херсонського національного технічного університету, 2, 1(92), 76–83. https://doi.org/10.35546/kntu2078-4481.2025.1.2.11

12. Shamshirband, S., Anuar, N. B., Kiah, M. L. M., & Patel, A. (2013). An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. Engineering Applications of Artificial Intelligence, 26(9), 2105–2127. https://doi.org/10.1016/j.engappai.2013.04.010

13. Gallo, A. J., Barboni, A., & Parisini, T. (2020). On detectability of cyber-attacks for large-scale interconnected systems. Preprints of the 21st IFAC World Congress (Virtual), Berlin, Germany, July 12–17. https://ifatwww.et.uni-magdeburg.de/ifac2020/media/pdfs/1984.pdf

14. Jakobsson, M., Wetzel, S., & Yener, B. (2003). Stealth attacks on ad-hoc wireless networks. IEEE Vehicular Technology Conference, 58(3), 2103–2111. https://doi.org/10.1109/vetecf.2003.1285396

15. Чмут, О. В., Калініченко, О. Г., & Бодашевський, Є. М. (2023). Технологія створення відмовостійкого багатомодульного програмного комплексу на основі процедури взаємних внутрішніх перевірок. Сучасний захист інформації, 4(56), 52–61. https://doi.org/10.31673/2409-7292.2023.030606

16. Мусієнко, А. П. Методологічні основи забезпечення функціональної стійкості бездротових сенсорних мереж на основі багатокритеріальної оптимізації : Дис. доктора техн. наук : спец. 05.13.06 - Інформаційні технології. Київ, ДУТ, 2019. – 328 с.

17. Гнатюк, Я. (2016). Логіка: сучасна перспектива традиційної теорії. Івано-Франківськ, “Симфонія форте”, 2016, 356 с.

9. References

1. Gol, V. D., & Irkha, M. S. (2021). Telecommunications and Information Networks. Kyiv, Igor Sikorsky Kyiv Polytechnic Institute, 250 p. https://ela.kpi.ua/server/api/core/bitstreams/35d4a2d2-53ed-453f-9bcd-fa883a982f53/content

2. Panovyk, U. P. (2024). Cybersecurity in Telecommunication Networks and Systems. Naukovi Zapisky, 1(68), 122–135. https://nz.uad.lviv.ua/media/1-68/13.pdf

3. Khoroshko, V., Khokhlachova, Y., & Vyshnevska, N. (2023). Decomposition of Computer Network Technology In Their Design. Ukrainian Scientific Journal of Information Security, 29(3), 130–137. https://doi.org/10.18372/2225-5036.29.18072

4. Khavina, I. P., Hnusov, Yu. V., & Mozhaiev, O. O. (2022). Development of multi-agent information security management system. Law and Safety, 87(4), 171–183. https://doi.org/10.32631/pb.2022.4.14

5. Kitura, O. V. (2023). Methodology for forming a transport network control system. Dissertation Doctor of Philosophy in speciality 172 “Telecommunications and Radio Engineering”. Kyiv, DUT, 133 p. https://duikt.edu.ua/uploads/p_2625_85571738.pdf

6. Bougueroua, N., et al. (2021). A Survey on Multi-Agent Based Collaborative Intrusion Detection Systems. Journal of Artificial Intelligence and Soft Computing Research, 11(2), 111–142. https://doi.org/10.2478/jaiscr-2021-0008

7. Torres, M. (2025). Enhancing Distributed Intrusion Detection Systems Using Multi-Agent AI Models. International Annals of Intelligent Learning Systems Research (IAILSR), 9, 22–35. https://iailsr.org/index.php/iailsr/article/view/13

8. Sen, J. (2011). A Distributed Intrusion Detection System Using Cooperating Agents. arXiv:1111.0382. https://doi.org/10.48550/arXiv.1111.0382

9. Aydın, H., Aydın, G. Z. G., Sertbaş, A., & Aydın, M. A. (2023). Internet of things security: A multi-agent-based defense system design. Computers and Electrical Engineering, 111(B), 108961, https://doi.org/10.1016/j.compeleceng.2023.108961

10. Landolt, C. R., Würsch, C., Meier, R., Mermoud, A., & Jang-Jaccard, J. (2025). Multi-Agent Reinforcement Learning in Cybersecurity: From Fundamentals to Applications. arXiv:2505.19837. https://doi.org/10.48550/arXiv.2505.19837

11. Kozlovsky, O. V., & Zharikova, M. V. (2025): Development of a security model for a multi-agent network in a cyber-physical system. Bulletin of the Kherson National Technical University, 2, 1(92), 76–83. https://doi.org/10.35546/kntu2078-4481.2025.1.2.11

12. Shamshirband, S., Anuar, N. B., Kiah, M. L. M., & Patel, A. (2013). An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique, Engineering Applications of Artificial Intelligence, 26(9), 2105–2127. https://doi.org/10.1016/j.engappai.2013.04.010

13. Gallo, A. J., Barboni, A., & Parisini, T. (2020). On detectability of cyber-attacks for large-scale interconnected systems. Preprints of the 21st IFAC World Congress (Virtual), Berlin, Germany, July 12–17. https://ifatwww.et.uni-magdeburg.de/ifac2020/media/pdfs/1984.pdf

14. Jakobsson, M., Wetzel, S., & Yener, B. (2003). Stealth attacks on ad-hoc wireless networks. IEEE Vehicular Technology Conference, 58(3), 2103–2111. https://doi.org/10.1109/vetecf.2003.1285396

15. Chmut, O. V., Kalinichenko, O. G., & Bodashevsky, E. M. (2023). Technology for creating a fault-tolerant multi-module software complex based on the procedure of mutual internal checks. Modern Information Security, 4(56), 52–61. https://doi.org/10.31673/2409-7292.2023.030606

16. Musienko, A. P. Methodological foundations of ensuring the functional stability of wireless sensor networks based on multi-criteria optimization: Dissertation of Doctor of Technical Sciences: special. 05.13.06 - Information Technologies. Kyiv, DUT, 2019. – 328 p.

17. Hnatyuk, Ya. (2016). Logic: a modern perspective on traditional theory. Ivano-Frankivsk, “Symphony forte”, 2016, 356 p.

Надійшла до редакції: 25.11.25
Прийнята до друку: 17.03.26
Опубліковано: 30.03.26