УДК 004.716:004.054

ДЕТЕКЦІЯ КРОСРІВНЕВИХ ПОМИЛОК В ІНТЕЛЕКТУАЛЬНИХ ШЛЮЗАХ ВИСОКОЩІЛЬНОГО ІНТЕРНЕТУ РЕЧЕЙ

Панченко В.І., к.т.н.[1]; Орлова Т.О.[2]
[1,2]Національний технічний університет «Харківський політехнічний інститут»
[1,2]Україна, Харків
[1]ORCID 0000-0003-3364-3398; [2]ORCID 0000-0001-8835-7570

Анотація. *Розглянуто задачу виявлення кросрівневих помилок шлюзів високощільного Інтернету речей, що виникають лише у взаємодії рівнів стека й не фіксуються локальними оракулами. Розширено алгебраїчну модель еволюційного синтезу тестів, запропоновано метрику кросрівневого покриття та узгоджене з нею керування синтезом.*

Ключові слова: *кросрівневі помилки; інтелектуальний шлюз; високощільний Інтернет речей; синтез тестів; генетичні алгоритми.*

Вступ. Високощільний Інтернет речей (High-Density IoT, HDIoT) передбачає підключення тисяч пристроїв на квадратний кілометр [1], а інтелектуальний шлюз периферійного шару (Intelligent Edge Layer Gateway, IELG) виконує в ньому агрегацію даних, трансляцію протоколів і локальну аналітику Edge AI. Огляд [2] показує, що сучасні багатопротокольні шлюзи поєднують різнорідні інтерфейси й архітектурні рівні, кожен з яких має власні засоби контролю. Через це частина відмов не локалізується в межах одного рівня: втрата кадрів на радіорівні спричиняє перебудову маршруту, затримку черги повідомлень і недостовірний вихід моделі Edge AI, хоча кожен рівень окремо проходить власні перевірки. Такі відмови далі називаємо кросрівневими помилками (cross-layer errors).

За узагальненням у [1], огляд [3] виділяє гетерогенність протоколів як головний бар'єр тестування IoT і констатує, що наявні фреймворки не забезпечують кросрівневого покриття, а огляд [4] вказує на брак засобів, здатних адаптуватися до зміни топології мережі. Кросрівневі підходи зосереджені переважно на безпеці та моніторингу мережі: у [5] показано, що однорівневі захисні механізми недостатні для пристроїв з обмеженими ресурсами, а система виявлення аномалій [6] працює на канальному й мережевому рівнях, розподіляючи задачі між вузлами та маршрутизатором. Дослідження [7] присвячене виявленню та класифікації відмов у промисловому IoT за неповних даних сенсорів, але не передбачає цілеспрямованого синтезу тестових впливів. У роботах автора [1, 8, 9] запропоновано адаптивний метод синтезу тестів для IELG на основі генетичних алгоритмів, дворівневого керування «Планувальник–Диспетчер» та апарату універсальних алгебр і теорії категорій; проте виникає необхідність подальшого удосконалення методу для множини несправностей компонентів з урахуванням помилок, що виникають лише під час взаємодії рівнів.

Метою роботи є розроблення розширення методу синтезу тестів [1, 8] для детекції кросрівневих помилок IELG: формалізація такої помилки, метрики кросрівневого покриття та узгоджених із нею моделі генерації тестів і керування синтезом.

Основна частина. Для формалізації помилки розглянемо шлюз як множину шарів $L = \{l_1, \ldots, l_5\}$: підключення пристроїв, керування даними, Edge-AI, Edge-контейнеризації та сервісів, безпеки [9]. Тестовий вплив t породжує трасу подій $\tau(t) = (e_1, \ldots, e_n)$, кожна подія якої має мітку шару; $\tau_l(t)$ – проєкція траси на шар l. Кожен шар має локальний оракул O_l, що перевіряє цю проєкцію. Кросрівневі інваріанти $R = \{r_k\}$ – це предикати над подіями щонайменше двох рівнів у часовому вікні Δ; наприклад, якщо на шарі підключення

зафіксовано N втрат кадрів поспіль, то шар керування даними має позначити пакет неповним не пізніше ніж за T_r, а вихід Edge AI – позначено як недостовірний. Кросрівневою помилкою x_k вважаємо порушення інваріанта r_k за умови, що всі локальні оракули виконуються:

$$x_k(t) \Leftrightarrow \left[r_k\left(\tau(t)\right) = 0\right] \wedge \bigwedge_{l \in L}\left[O_l\left(\tau_l(t)\right) = 1\right]. \quad (1)$$

Така помилка недосяжна для тестів, що оцінюються лише локальними оракулами. Для її кількісної оцінки вводимо кросрівневе покриття (у відсотках):

$$C_X = 100 \cdot \frac{|X_d|}{|X_p|}, \quad (2)$$

де X_d – множина помилок, виявлених тестовим набором; X_p – множина потенційних кросрівневих помилок (за інваріантами R).

Розширення алгебраїчної моделі. У [1, 8] процес синтезу описано парою універсальних алгебр: A_1 (генерація тестових наборів) та A_2 (еволюція популяцій), між якими та класичними генетичними алгоритмами встановлено гомоморфізм; коректність перетворень тестових наборів описано мовою теорії категорій [8]. Пропонується ввести третю алгебру $A_3 = (M_3, D_3)$, носієм якої є розподілені сценарії $s = (t_1, \ldots, t_m, \delta)$: проєкції t_l стимулів на кожен шар і вектор δ часових зсувів між ними. Сигнатура D_3 містить операції проєкції π_l (виділення стимулів шару l), зсуву θ (мутація вектора δ) та обміну проєкціями ω (кросовер за шарами). Розширення категорійного опису [8] передбачає функтори між категоріями станів окремих шарів; доведення збереження ними структури операцій A_3 є предметом подальшої роботи.

Для реалізації заохочення сценаріїв, що активують нові інваріанти, а не лише збільшують локальне покриття використовується метрика k_X, значення якої прямо пропорційне кількості виявлених міжрівневих помилок. Планувальник [1] додатково відстежує швидкість $\Delta C_X/\Delta T$: коли локальне покриття насичується, а C_X відстає, він перемикається на стратегії з підвищеною ймовірністю мутації θ і кросоверу ω.

Для реалізації детекції кросрівневих помилок пропонується така архітектура: Диспетчер генерує сценарії s і подає їх на рівні шлюзу; монітор збирає траси $\tau(t)$, кросрівневий оракул перевіряє інваріанти R, а метрики C_X і k_X повертаються Планувальнику (рис. 1).

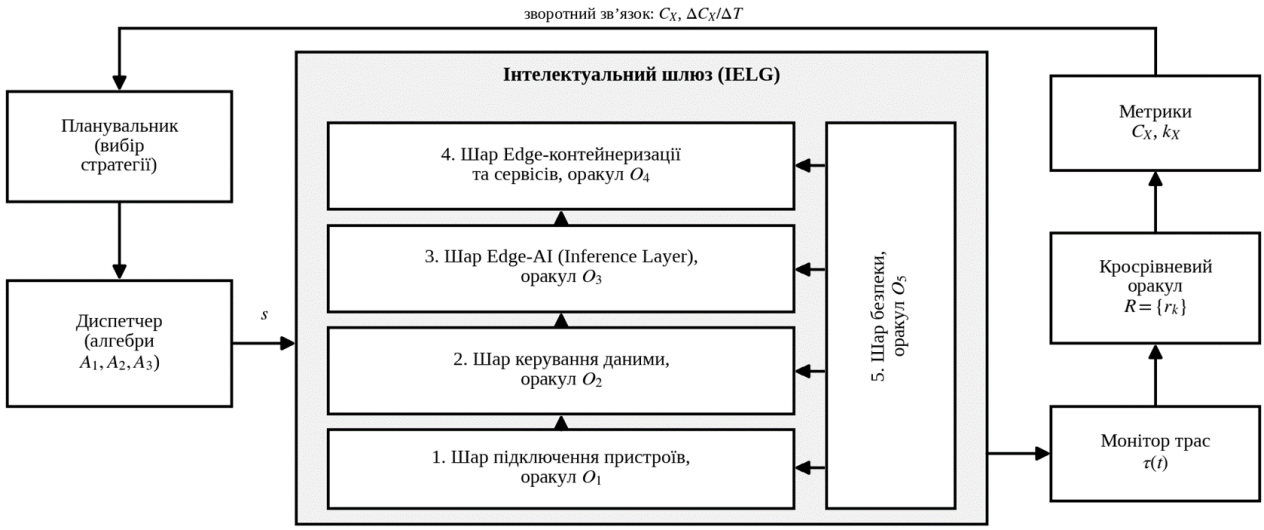


Рис. 1. Архітектура детекції кросрівневих помилок

Перевірку розширення методу передбачено виконати на імітаційній моделі [1], доповнивши її класами «траса подій» і «кросрівневий інваріант», за планом повного

факторного експерименту з додатковими факторами: кількість шарів, ширина вікна Δ та інтенсивність операції θ. Функцією відгуку є час синтезу до досягнення C_X = 95 %.

Висновки. Формалізовано кросрівневу помилку шлюза та введено метрику кросрівневого покриття (формули (1), (2)). Алгебраїчну модель еволюційного синтезу тестів [1, 8] розширено третьою алгеброю розподілених сценаріїв. Експериментальну перевірку та доведення властивостей функторів між рівнями віднесено до наступного етапу; серед перспектив – інтеграція з цифровими двійниками шлюзів [1].

Використання інструментів ШІ. Зміст роботи, формули та висновки виконані автором без використання засобів ШІ. Для пошуку джерел інформації використано інструменти ШІ Gemini (модель 3.1 Pro), перевірку результатів виконано автором особисто.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Панченко, В. І. (2026). Розробка та дослідження узагальненого методу синтезу тестів для діагностики інтелектуального шлюзу периферійного шару високощільного Інтернету речей. *Системи управління, навігації та зв'язку*, (1), 90–94. https://doi.org/10.26906/SUNZ.2026.1.090

[2] Abdelwahed, S. H., Hefny, I. M., Hegazy, M., Said, L. A., & Soltan, A. (2025). Survey of IoT multi-protocol gateways: Architectures, protocols and cybersecurity. *Internet of Things*, *33*, Article 101703. https://doi.org/10.1016/j.iot.2025.101703

[3] Lima, B., & Pinto, R. (2025). Current challenges and future perspectives in testing IoT systems: A comprehensive review. *IEEE Sensors Reviews*, *3*, 22–47. https://doi.org/10.1109/SR.2025.3628264

[4] Minani, J. B., Sabir, F., Moha, N., & Guéhéneuc, Y.-G. (2024). A systematic review of IoT systems testing: Objectives, approaches, tools, and challenges. *IEEE Transactions on Software Engineering*, *50*(4), 785–815. https://doi.org/10.1109/TSE.2024.3363611

[5] Altaibek, M., Issainova, A., Aidynov, T., Kuttymbek, D., Abisheva, G., & Nurusheva, A. (2025). A survey of cross-layer security for resource-constrained IoT devices. *Applied Sciences*, *15*(17), Article 9691. https://doi.org/10.3390/app15179691

[6] Thanigaivelan, N. K., Nigussie, E., Virtanen, S., & Isoaho, J. (2018). Hybrid internal anomaly detection system for IoT: Reactive nodes with cross-layer operation. *Security and Communication Networks*, *2018*, Article 3672698. https://doi.org/10.1155/2018/3672698

[7] Dzaferagic, M., Marchetti, N., & Macaluso, I. (2022). Fault detection and classification in industrial IoT in case of missing sensor data. *IEEE Internet of Things Journal*, *9*(11), 8892–8900. https://doi.org/10.1109/JIOT.2021.3116785

[8] Panchenko, V., & Kuchuk, H. (2026). Theoretical-algebraic basics of evolutionary test synthesis for gateways components of high-density IoT systems. *Автоматизовані системи управління та прилади автоматики*, (188), 44–53. https://doi.org/10.30837/0135-1710.2026.188.044

[9] Панченко, В. І. (2026). *Методи синтезу і агрегування тестів для діагностики інтелектуального шлюзу периферійного шару високощільного Інтернету речей* [Автореф. дис. канд. техн. наук, Національний технічний університет «Харківський політехнічний інститут»]. Електронний репозитарій НТУ «ХПІ». https://repository.kpi.kharkov.ua/handle/KhPI-Press/102163

Panchenko V.I., Orlova T.O.

Detection of cross-layer errors in intelligent gateways of high-density Internet of Things

Abstract. *The paper addresses the detection of cross-layer errors in intelligent gateways of high-density IoT, i.e., failures that appear only in the interaction of the radio, network and application/Edge AI layers and are not captured by local layer oracles. The algebraic model of evolutionary test synthesis is extended with a third algebra of distributed multi-layer test scenarios; a cross-layer coverage metric and a cross-layer novelty coefficient of the fitness function are introduced, and the Scheduler–Dispatcher control is adapted accordingly.*

Keywords: *cross-layer errors; intelligent gateway; high-density Internet of Things; test synthesis; genetic algorithms.*