Трансформація підходів до побудови тестів цифрових пристроїв на шлюзи IoT

Панченко В.І., Національний технічний університет «Харківський політехнічний інститут», Україна

Сучасний етап розвитку кіберфізичних систем характеризується переходом від ізольованих обчислювальних пристроїв до глобально інтегрованих мереж Інтернету речей (IoT). Ключовим елементом цієї інфраструктури є інтелектуальний шлюз граничного шару (IELG) високощільного IoT (HDIoT), який виконує функції агрегації даних, трансляції протоколів та локальної аналітики. Традиційні методи тестування, орієнтовані на верифікацію цифрової логіки, виявляються недостатніми для забезпечення якості таких систем через їхню ієрархічну складність та стохастичну природу функціонування.

На відміну від «плоскої» структури класичних цифрових пристроїв, IELG HDIoT являє собою багаторівневу систему, що вимагає специфічних підходів до валідації на кожному етапі. Ключовою проблемою є неможливість прямого застосування класичної моделі константних несправностей («stuck-at faults»), яка історично використовується для тестування цифрових схем та базується на припущенні про фізичні дефекти, що фіксують сигнал у стані 0 або 1. Більшість проблем у роботі шлюзу не викликаються фізичними пошкодженнями, вони пов’язані з логічними помилками, нестачею ресурсів, конфліктами в протоколах або некоректною інтерпретацією даних. Модель константних несправностей є абсолютно недостатньою для валідації шлюзів IoT – високий відсоток покриття тестами константних несправностей для IELG гарантує лише те, що процесор шлюзу справний фізично, але нічого не говорить, наприклад, про те, чи зможе шлюз коректно обробити чергу повідомлень при нестабільному зв’язку.

При використанні сучасних методів автоматичної генерації тестів (наприклад, еволюційних алгоритмів) критично важливим є правильне визначення функції пристосованості, яка керує пошуком помилок. Для IoT-орієнтованого підходу виконується перехід від врахування лише покриття коду або кількості переключень станів до аналізу стресу системи або ймовірності виникнення рідкісних подій, пов’язаних з перевищенням довжин черг повідомлень, часу відгуку, споживання енергії, зменшенням вільної оперативної пам’яті.

Таким чином запропоновано розглядати не тільки статичні (фізичні) несправності, але й специфічні для IELG: динамічні (часові) несправністі – помилки синхронізації, порушення часових обмежень у системах реального часу; ресурсні – витоки пам’яті, фрагментація купи, нестача дескрипторів; стохастичні – відмови мереж та спотворення пакетів даних; семантичні – вразливості ML-моделей до вхідних даних з невеликими модифікаціями, які змушують нейромережу приймати некоректні рішення.

Оскільки повністю відтворити складність реального середовища в лабораторії неможливо, тестування зміщується на етап експлуатації обладнання. Методологія хаос-інжинірингу передбачає навмисне введення несправностей у працюючу систему (наприклад, примусове розривання з’єднань, примусове завершення процесів, емуляція затримок) для перевірки здатності системи до самовідновлення). Забезпечення якості тестування IELG вимагає відмови від детермінованих перевірок до та впровадження метрик покриття, що враховують не лише складність структури, але й семантику даних та стійкість системи до зовнішніх впливів. Таким чином, тестування шлюзу не може бути розділене на ізольовані тести апаратної і програмної частини – система може бути протестована лише при аналізі всіх рівнів її архітектури.

Проведене дослідження лежить в основі розробки еволюційних методів тестування, що дозволяють створювати самоадаптивні системи верифікації для інтелектуальних шлюзів високощільного IoT. Такий комплексний підхід дозволить забезпечити надійність критичної інфраструктури, яка стає основою цифрового суспільства.