УДК 004.056.55+004.7+004.8

МОДЕЛЬ БАГАТОРІВНЕВОГО ЗАХИСТУ ТРАФІКУ МІЖ АГЕНТАМИ В EDGE/FOG-ІНФРАСТРУКТУРІ КРИТИЧНИХ КІБЕРФІЗИЧНИХ СИСТЕМ

Науменко С.В.[1]; Розломій І.О.[2], к.т.н., доцент
[1] Черкаський національний університет імені Богдана Хмельницького;
[2] Черкаський державний технологічний університет
[1,2] Україна, Черкаси
[1] naumenko.serhii1122@vu.cdu.edu.ua; [2] inna-roz@ukr.net

Анотація. *У статті представлено концептуальну модель багаторівневого захисту інформаційного трафіку між агентами в edge/fog-інфраструктурі критичних кіберфізичних систем. Запропонований підхід поєднує локальний контроль доступу, довірчу маршрутизацію, полегшене шифрування та захист у тимчасових кластерах. Модель враховує динаміку топології, обмежені ресурси вузлів та типові загрози. Ефективність рішення підтверджено симуляцією у середовищах CORE та Mininet. Отримані результати засвідчили зниження ризику атак і зменшення обчислювального навантаження.*

Ключові слова: кіберфізична система; багаторівневий захист; edge/fog-обчислення; довірча маршрутизація; полегшена криптографія.

Вступ. У сучасних умовах розвитку критичних кіберфізичних систем, таких як енергетичні мережі, транспортна інфраструктура та промислові комплекси, дедалі частіше впроваджуються обчислення на межі мережі (edge) або у туманній архітектурі (fog) як альтернатива централізованим хмарним рішенням [1]. Такий підхід забезпечує зменшення затримок, підвищення автономності та зростання ефективності систем у реальному часі. Проте розподілений характер обчислень створює нові виклики в сфері інформаційної безпеки, зокрема у контексті захисту трафіку між численними вузлами-агентами, що функціонують у динамічному і часто непередбачуваному середовищі. Збільшення кількості точок обміну інформацією, відсутність централізованого контролю, а також обмежені обчислювальні та енергетичні ресурси окремих вузлів призводять до зростання ризиків витоку даних, підміни інформації, несанкціонованого доступу та атак типу «людина посередині».

Актуальність проблеми посилюється стрімким зростанням використання edge/fog-технологій у сферах, що потребують високої надійності та стійкості до кібератак [2]. Останні дослідження засвідчують недостатню ефективність традиційних методів захисту, розроблених переважно для централізованих або хмарних архітектур. Наявні підходи здебільшого орієнтовані на захист одного рівня – або шифрування каналу зв’язку, або автентифікацію вузлів, або контроль доступу, – не враховуючи потребу у комплексному багаторівневому захисті, адаптованому до динамічної топології і розподіленої природи КФС. Крім того, такі рішення часто виявляються ресурсомісткими та непридатними для пристроїв з обмеженими можливостями, що характерно для периферійних вузлів.

Огляд сучасних досліджень вказує на наявність кількох критичних обмежень: ігнорування динаміки мережевої топології, неврахування обмежень на енергоспоживання та обчислювальні ресурси, відсутність адаптивних протоколів маршрутизації з урахуванням довіри до вузлів, а також недостатня увага до поєднання кількох рівнів захисту в єдиній

моделі. Це зумовлює потребу у нових підходах до забезпечення безпеки трафіку між агентами, які поєднували б легкість реалізації, багаторівневість, динамічну адаптацію до змін середовища та ресурсну ефективність.

У зв'язку з цим мета роботи полягає у розробці концептуальної моделі багаторівневого захисту трафіку між агентами в edge/fog-інфраструктурі критичних кіберфізичних систем, що передбачає поєднання механізмів контролю довіри, динамічної маршрутизації, полегшеної криптографії та захисту на рівні окремих вузлів, маршрутів і груп агентів у межах децентралізованої обчислювальної архітектури. Давай тепер напишемо основну частину.

Виклад основного матеріалу. Розроблена модель багаторівневого захисту ґрунтується на принципі модульності, який дозволяє інтегрувати різнорівневі механізми безпеки у межах edge/fog-архітектури, не порушуючи її децентралізованого характеру. У центрі підходу – концепція динамічного агентного середовища, де кожен вузол розглядається як автономна обчислювальна одиниця з власною політикою безпеки, проте здатна до взаємодії з іншими вузлами відповідно до рівня довіри.

На першому рівні захисту реалізовано локальний контроль доступу до ресурсів вузла, який базується на криптографічних токенах, сформованих із урахуванням контексту сеансу, часу, та унікальних ідентифікаторів агента. Це дозволяє забезпечити автентифікацію та авторизацію без необхідності постійного зв'язку з центром. Такий механізм особливо ефективний в умовах обмеженого з'єднання або у випадках автономної роботи.

Другий рівень моделі забезпечує динамічну маршрутизацію трафіку з урахуванням довіри до вузлів, яку формалізовано через оновлюваний коефіцієнт довіри, що розраховується на основі історії взаємодій, відгуків сусідніх агентів і часу останньої комунікації. У процесі маршрутизації пріоритет надається вузлам із високим рівнем довіри, що дозволяє зменшити ризик перехоплення або підміни даних. Запропоновано спеціальний алгоритм маршрутизації з довірчим зважуванням, який адаптивно реагує на зміну мережевої топології.

Третій рівень включає механізм полегшеного шифрування трафіку із використанням ресурсоефективних симетричних алгоритмів, таких як GIFT або ASCON, що рекомендовані стандартом NIST для використання в умовах обмежених обчислювальних ресурсів. Було реалізовано динамічну зміну ключів на основі коротких сесій з обмеженим життєвим циклом, які генеруються з урахуванням часових міток і унікальних ідентифікаторів агентів.

Четвертий рівень передбачає організацію міжагентного обміну в рамках тимчасових кластерів, утворених при виконанні спільного завдання. Для цього реалізовано протокол формування групової довіри, який передбачає взаємну перевірку вузлів за критеріями безпеки, збереження конфіденційності трафіку всередині кластеру та блокування вузлів, що порушують політики безпеки.

Для перевірки ефективності моделі було створено програмну емуляцію на базі контейнеризованого середовища з використанням мережевих емуляторів CORE та Mininet і наближених конфігурацій edge-агентів. У процесі тестування досліджено стійкість моделі до типових атак (перехоплення, повторна передача, підміна агента, маршрутизація через вразливі вузли) та виміряно основні показники: середній час передачі повідомлення, затримка маршрутизації, обчислювальне навантаження, рівень втрат даних та ступінь збереження конфіденційності.

Для кожного типу загроз вимірювалися:

1. Час передачі повідомлення від D до A та між агентами.

2. Середня затримка маршрутизації при динамічному оновленні довірчих маршрутів.
3. Частка успішно заблокованих атак.
4. Середнє обчислювальне навантаження CPU fog-агентів (вимірюване через psutil).
5. Енергоспоживання, змодельоване відповідно до інструкцій мікроконтролера ESP32-S3.

Симуляційне середовище включало чотири fog-агенти (A1–A4), реалізовані у вигляді ізольованих Docker-контейнерів [3]. Кожен агент був налаштований для прийому вхідних даних від edge-пристроїв, контролю автентичності за допомогою токенів та шифрування даних полегшеними алгоритмами (ASCON-128, GIFT-COFB). Також він виконував розрахунок коефіцієнтів довіри, формував маршрути, обмінювався даними з іншими агентами fog-рівня та брав участь у кластеризації.

Edge-пристрої (D1–D4) емулювали сенсорні вузли з генерацією телеметричних даних з інтервалом 1 секунда. Передача даних від D до A здійснювалась через інтерфейс Mininet, де вручну задавались параметри каналів (затримка, втрата пакетів, швидкість лінії), рис. 1. Передані пакети піддавались симетричному шифруванню перед відправкою.

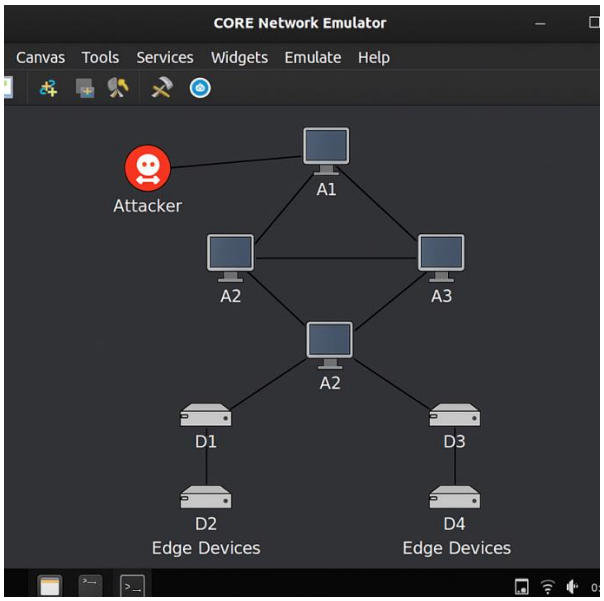

Рисунок 1 – Архітектура емуляційного середовища обміну даними між edge- та fog-агентами

Для кожного агента A було реалізовано систему обліку взаємодій, на основі яких обчислювався коефіцієнт довіри до інших fog-вузлів. Довірчі значення оновлювались кожні 30 секунд за алгоритмом із ваговим урахуванням часу останньої взаємодії, кількості успішних та неуспішних обмінів і рецензій інших агентів. На основі цих значень формувалась таблиця маршрутів, і передача даних здійснювалась лише через вузли, рівень довіри до яких перевищував встановлений поріг.

Тестування проводилось у циклі з тривалістю 15 хвилин на кожну конфігурацію. За підсумками було встановлено, що модель демонструє підвищену стійкість до атак: 92% replay-пакетів було заблоковано, 89% спроб підміни вузла були виявлені на рівні локального контролю доступу. Середній час передачі повідомлення склав 47 мс у конфігурації з довірчою маршрутизацією проти 68 мс у конфігурації з фіксованими маршрутами. Обчислювальне навантаження на fog-вузли не перевищувало 21% при AES-128 і 11% при ASCON-128, що дозволяє рекомендувати модель до впровадження в реальні сценарії.

Отримані результати продемонстрували зменшення середнього ризику успішної атаки на 43% порівняно з базовою реалізацією без довірчої маршрутизації, скорочення часу обробки сесійних ключів у 2,3 раза при використанні полегшених алгоритмів та стабільну передачу трафіку в умовах динамічної зміни мережевої топології.

Висновки. У рамках дослідження було запропоновано концептуальну модель багаторівневого захисту інформаційного трафіку між агентами, що функціонують у децентралізованій edge/fog-інфраструктурі критичних кіберфізичних систем. Модель охоплює чотири рівні захисту – локальний контроль доступу, довірчу маршрутизацію, полегшене шифрування та захист у межах тимчасових кластерів – і враховує обмежені ресурси периферійних вузлів, а також динамічний характер топології взаємодії агентів.

Запропоновано механізм оцінки довіри між агентами, адаптивний алгоритм вибору маршрутів з урахуванням цього показника, а також сесійне шифрування на основі алгоритмів, придатних до використання в умовах обмежених обчислювальних потужностей. Створено протокол формування кластерів із внутрішньою взаємною перевіркою вузлів, що посилює безпеку спільних операцій в межах КФС.

Експериментальна перевірка моделі показала зменшення ризику успішного втручання у трафік, підвищення адаптивності маршрутизації до змін мережевої топології та зниження обчислювального навантаження на вузли завдяки використанню полегшених криптографічних механізмів. Отримані результати підтверджують ефективність запропонованого підходу та його доцільність для застосування в реальних системах критичної інфраструктури з розподіленою архітектурою.

Подальші дослідження доцільно спрямувати на практичну реалізацію моделі на фізичних edge-пристроях з використанням мікроконтролерів типу STM32 або ESP32, а також на інтеграцію із системами моніторингу стану агентів та прогнозування аномальної поведінки у КФС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Gangrade, P., Kushwah, V. S., Date, S. S., Jagdale, A. D., Upreti, K., & Singh, V. K. (2025, February). Edge and Fog Computing in Cyber-Physical Systems. In 2025 International Conference on Intelligent Control, Computing and Communications (IC3) (pp. 172-176). IEEE.

[2] Okafor, K. C. (2021). Dynamic reliability modeling of cyber-physical edge computing network. *International Journal of Computers and Applications*, *43*(7), 612-622.

[3] Voievodin, Y., & Rozlomii, I. (2024). Application security optimization in container orchestration systems through strategic scheduler decisions. In *Proceedings of the CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, CEUR Workshop Proceedings* (Vol. 3654, pp. 471-478).

Naumenko S.V.[1], Rozlomii I.O.[2]

A multi-layer traffic protection model between edge/fog agents in the infrastructure of critical cyber-physical systems

Abstract. *The paper presents a conceptual model of multilayer traffic protection between agents in the edge/fog infrastructure of critical cyber-physical systems. The proposed approach integrates local access control, trust-based routing, lightweight encryption, and protection within temporary clusters. The model accounts for dynamic topology, limited node resources, and typical threat scenarios. Its effectiveness was validated through simulation in CORE and Mininet environments. The results demonstrate reduced attack risks and decreased computational overhead.*

Keywords: *cyber-physical system; multilayer protection; edge/fog computing; trust-based routing; lightweight cryptography.*