КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1359
УДК 004.056.5:007.52

Пахомов Михайло Васильович
аспірант кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0009-0007-7343-6912
m.pakhomov.asp@kubg.edu.ua

Соколов Володимир Юрійович
кандидат технічних наук, доцент
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

АДАПТАЦІЯ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ ДЛЯ КІБЕРФІЗИЧНИХ РОБОТОТЕХНІЧНИХ СИСТЕМ: БАЗОВІ ВИМОГИ ТА МЕЖІ СТІЙКОСТІ БЕЗПРОВОДОВОГО КАНАЛУ

Анотація. Проаналізовано проблему застосування підходу нульової довіри ‘Zero Trust’ (ZT) для безпеки кіберфізичних робототехнічних систем ‘Cyber-Physical Robotic Systems’ (CPRS). Обґрунтовано, що тісна взаємодія мережевих обчислень, сенсорів, актуаторів і систем фізичного керування формує єдину площину ризику, де компрометація ідентифікаційних даних, телеметрії чи каналів зв’язку загрожує як витоком інформації, так і небезпечними фізичними інцидентами. Досліджувана сфера охоплює промислові й мобільні роботи, безпілотні літальні апарати, сервісні та колаборативні роботи, функціонування яких залежить від кіберкомпонентів, здатних впливати на фізичну поведінку. У межах розробки архітектури сформульовано п’ять базових вимог ZT: перевірювана ідентифікація, контекстна авторизація, сегментація мережі, оцінювання актуальності й надійності телеметрії, а також адаптивне реагування з обмеженою експлуатацією та локальною відмовостійкістю. Для визначення меж стійкості безпроводового каналу керування проведено симуляційне моделювання в середовищі ns-3 (стандарт IEEE 802.11ax WiFi 6, одна точка доступу, 20 клієнтських станцій). На основі аналізу 140 трас (відстані 30–125 м, сумарне навантаження 100 Мбіт/с) оцінено сукупну корисну пропускну здатність (aggregate goodput), затримку p95 та відсоток втрат пакетів. Виявлено двоетапний характер деградації каналу зв'язку: межа раннього часового погіршення зафіксована на відстані 40 м (стрибок затримки p95 до 351,8 мс майже без втрат), а межа стійкої деградації втрат — на 50 м (втрати 9,61%). За критичної відстані 125 м goodput знижується до 0,387 Мбіт/с із втратами 99,81%. Встановлено, що отримані межі стійкості безпроводового зв’язку є визначальними для доставки телеметрії та вибору режимів реагування, проте ізольовано не гарантують реалізації ZT. Для комплексної валідації архітектури нульової довіри запропоновано конвеєр синхронізованого аналізу мережевих метрик, подій безпеки та фізичного стану робота.

Ключові слова: Zero Trust, кібербезпека, кіберфізична система, робототехнічна система, ns-3, стійкість, безпроводовий зв’язок, безперервна верифікація, авторизація, політика безпеки.

ВСТУП

CPRS функціонують у взаємопов’язаному середовищі. Промислові маніпулятори, мобільні роботи, безпілотні транспортні засоби, колаборативні та сервісні роботи на базі штучного інтелекту дедалі більше залежать від безпроводових з’єднань, платформ керування парком техніки, периферійних шлюзів, хмарної аналітики, інтеграції даних датчиків і каналів оновлення програмного забезпечення. Така взаємопов’язаність розширює площину атаки, охоплюючи кіберпростір, фізичні процеси та рівень взаємодії «людина-робот». Дослідження з безпеки робототехніки підкреслюють, що атаки на роботів можуть спричиняти фізичні пошкодження, небезпечні рухи, втрату продуктивності, порушення

© М.В. Пахомов, В.Ю. Соколов, 2026

конфіденційності та зниження довіри до автоматизації [1–3]. У систематичному огляді безпеки кіберфізичних систем Yu та ін. [4] такі системи розглядаються як середовища, у яких обчислювальні й комунікаційні збої можуть мати фізичні наслідки.

Архітектура ZT виходить із протилежного припущення: жоден пристрій, сервіс чи сегмент мережі не є надійним апріорі. Натомість кожен запит на доступ оцінюється безперервно – за ідентичністю, станом пристрою, політикою, телеметрією та контекстом [5–8]. Перенесення цього принципу в робототехнічні CPRS ускладнюється тим, чого корпоративні IT-системи не знають: рішеннями керування в мілісекундному масштабі, переривчастим безпроводовим зв'язком, потребою в локальній автономії за відключення від хмари та вимогами функціональної безпеки. За таких умов відмова в доступі не може бути бінарною подією – вона сама стає чинником ризику.

Отже, окреслені загрози для CPRS оцінюються за п'ятьма вимогами ZT: перевірюваною ідентифікацією, контекстною авторизацією, сегментацією, оцінюванням актуальності та надійності телеметрії й керованим реагуванням із відновленням.

Постановка проблеми. Метою статті є аналіз проблеми забезпечення кібербезпеки CPRS на основі підходу ZT та формалізація п'яти базових вимог. Експериментальна частина оцінює вплив відстані AP-STA на aggregate goodput, p95 затримки й втрати пакетів у безпроводовій мережі 20 STA і однією AP. Вимірювання спрямовані на визначення меж, релевантних актуальності телеметрії та контрольованій деградації функцій.

Досліджувана сфера охоплює промислові й мобільні роботи, безпілотні літальні апарати, сервісні та колаборативні роботи, функціонування яких залежить від кіберкомпонентів, здатних впливати на фізичну поведінку. CPRS розглядаються як багаторівневі системи, що включають фізичну інфраструктуру, робототехнічну платформу, проміжне програмне забезпечення, мережу, периферійні або хмарні сервіси, оркестрування групи роботів і взаємодію з людиною.

Розглянуто принципи й архітектурні компоненти ZT для CPRS, загрози для ідентичності, проміжного програмного забезпечення, безпроводового зв'язку, датчиків і актуаторів, а також наявні засоби захисту та результати моделювання мережевої надійності. На цій основі сформовано вимоги до побудови архітектури ZT, придатної для CPRS.

Аналіз останніх досліджень і публікацій. Найактуальніші дослідження демонструють перехід від загальних принципів ZT до спеціалізованих механізмів для промислових і CPRS. Фенг і Ху [9] запропонували архітектуру Cyber-Physical-ZTA з багаторівневим контролем доступу, фізичними моделями та засобами аналізу даних. У моделюванні цей підхід підвищив імовірність виявлення атак ін'єкції хибних даних більш ніж на 31% порівняно зі стандартною ZTA. Гасан, Амундсон і Гардін [10] формалізували повторно використовувані шаблони ZT мовою опису архітектури AADL та застосували їх до безпілотної авіаційної системи. Для неоднорідних і застарілих середовищ запропоновано динамічну мікросегментацію разом із рольовим та атрибутним керуванням доступом RBAC/ABAC [11]. Занасі, Руссо і Колаянні [12] реалізували архітектуру IoT на основі мікросегментації, програмно-конфігурованої мережі та асинхронного поширення політик. Такий підхід підтримує децентралізовану роботу навіть за відмов окремих компонентів. Для розумного виробництва також обґрунтовано інвентаризацію пристроїв, контроль кожного доступу, мікросегментацію та безперервний моніторинг [13]. Подальші роботи поширюють ZT на життєвий цикл фундаментальних моделей в IoT та поєднують федеративне навчання, блокчейн-ідентифікацію, довірені середовища виконання й поведінкову аналітику [14]. Інший напрям охоплює оркестрування довірених мікросервісів на периферійному рівні промислових CPRS [15]. Огляд інтеграції IoT з периферійними обчисленнями підтверджує необхідність узгодженого використання ZT, програмно-конфігурованих мереж, блокчейну, цифрових двійників і виявлення аномалій [16]. Графовий підхід додатково об'єднує репозиторій політик, базу активів і потокові метадані для аналізу атак без доступу до зашифрованого вмісту [17].

МЕТОДИКА ДОСЛІДЖЕННЯ

Широке охоплення є необхідним, оскільки модель ZT може бути неефективною за її застосування лише на периферії мережі. Робот може бути доступним через захищену віртуальну приватну мережу VPN і водночас приймати небезпечні команди через проміжне програмне забезпечення. Сервіс керування може автентифікувати користувачів, але допускати латеральне переміщення між темами роботів, каналами оновлення, журналами та інтерфейсами цифрових двійників. Механізм застосування політик може коректно ідентифікувати пристрій, проте не виявити фізично невірну команду приводу. Отже, дослідницьке завдання полягає в інтеграції ідентичності, контексту, телеметрії, сегментації та безпечного реагування в межах усього кіберфізичного стеку (див. рис. 1 і табл. 1).

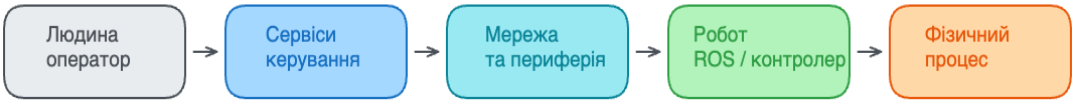

Рис. 1. Багатошарова доменна модель, що використовується для формування концепції кібербезпеки за принципом Zero Trust для робототехнічних систем «людина-машина»

Загрози для CPRS слід описувати з огляду на їхні точки вторгнення в кіберпростір та фізичні наслідки. До відповідних точок вторгнення належать незахищені мережеві служби, слабка ідентифікація пристроїв, незахищене проміжне програмне забезпечення роботів, скомпрометована вбудована програмна частина, вразливі механізми оновлення, інтерфейси прикладного програмування API хмарних сервісів та груп роботів, зловмисні або необережні оператори, а також порушення роботи безпроводових мереж. До відповідних наслідків належать маніпулювання командами, відмова в обслуговуванні, небезпечні рухи, введення датчиків в оману, втрата оператором контролю, витік конфіденційної інформації та каскадні збої в системах із декількома роботами [1–3, 18–22].

З точки зору підходу ZT ці загрози передбачають п’ять взаємопов’язаних базових вимог, які визначають напрями застосування політик у CPRS:

1. **Ідентичність та стан пристрою.** Кожен робот, оператор, сервіс, датчик, виконавчий механізм і компонент програмного забезпечення повинен мати ідентифікацію, яку можна перевірити; перевірка виконується постійно, а не лише під час підключення, і враховує поточний стан пристрою.
2. **Безперервна авторизація.** Авторизація пов’язується з контекстом виконання завдання та фізичним станом, а не лише з місцем розташування в мережі; рішення щодо політик враховують критичність місії, працездатність пристрою, стан мережі та фізичну близькість.

Таблиця 1

Базова лінія загроз та вимог архітектури Zero Trust для Cyber-Physical Robotic Systems

Сфера загроз	**Приклад CPRS**	**Вимоги до архітектури ZT**
Компрометація ідентифікаційних даних [3]	Викрадені облікові дані оператора або підроблена служба робота	Надійна ідентифікація, контроль стану безпеки пристрою, короткострокові облікові дані, контекстна авторизація.
Зловживання проміжним ПЗ [18]	Несанкціонована публікація в топіку операційної системи робота або виклик служби	Сегментація топіків/служб, автентифіковані вузли, зв’язок за принципом найменших привілеїв.
Погіршення безпроводового зв'язку [23]	Втрата телеметрії або затримка обміну даними під час автентифікації	Локальне застосування політик на периферійному рівні, кешування політик, прийняття рішень про довіру з урахуванням рівня надійності.
Маніпуляції з датчиками і актуаторами [24]	Сфальсифіковані дані датчиків або небезпечна команда виконавчому механізму	Перевірка аномалій з урахуванням фізичних законів та обмеження на основі правдоподібності команд.
Латеральне (горизонтальне) переміщення у зоні [25]	Використання одного скомпрометованого робота для отримання доступу до інших	Мікросегментація за завданням (місією), групою роботів, робочим простором та рівнем конфіденційності даних.

3. **Мікросегментація.** Сегментація обмежує горизонтальне переміщення між функціями роботів та зонами, а групи роботів розділяються за завданням (місією), робочим простором, зоною безпеки та рівнем конфіденційності даних, а не за простим членством у локальній мережі.

4. **Довіра з урахуванням телеметрії.** Телеметричні дані оцінюються на актуальність, повноту та надійність, а не лише за їхнім змістом, оскільки затримка телеметрії може призвести до помилкових рішень щодо політики безпеки.

5. **Відмовостійке застосування політик.** Точки застосування політик підтримують режими роботи з обмеженими можливостями, локальну відмовостійку поведінку та процеси відновлення, а не бінарну поведінку «дозволити/заборонити».

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Опрацювання існуючих рішень

Опрацьовано існуючі рішення та дослідження, що застосовуються для захисту CPRS. Розглянуто архітектури ZT, механізми автентифікації та авторизації, сегментацію мережі, захист проміжного програмного забезпечення роботичних операцыних систем ‘Robot Operating System’ (ROS), моніторинг телеметрії, виявлення аномалій і локальне застосування політик на периферійному рівні. Аналіз проведено за критеріями придатності до робототехнічних систем: вплив на затримку, робота за нестійкого зв'язку, підтримка автономності, обмеження обчислювальних ресурсів і здатність зменшувати наслідки компрометації окремого компонента. Результати опрацювання використано для виявлення прогалин наявних підходів і формування вимог до запропонованої архітектури [26–29]. До методологічного контексту також належать дослідження моделювання IEEE 802.11 DCF і спеціалізованих моделей IEEE 802.11 у ns-3 [30–32].

Джерела охоплюють засади ZT, безпеку кіберфізичних і робототехнічних систем, захист ROS, виявлення атак, периферійні обчислення та моделювання безпроводових мереж у ns-3 [5, 7, 9, 18, 23, 30, 33–38]. Посилання розподілено за тематичними твердженнями в тексті, а не зведено до суцільного діапазону; усі джерела оцінюються за їхнім внеском у п’ять базових вимог ZT.

Матеріали відбиралися за такими критеріями: висвітлення механізмів ідентифікації обладнання, алгоритмів оцінювання довіри, надійної передачі телеметрії, мікросегментації та відмовостійкості. Обов’язковою умовою була наявність технічних деталей, достатніх для класифікації описаних механізмів захисту.

З аналізу виключено роботи, що описують винятково корпоративні IT-рішення без можливості адаптації до кіберфізичних систем, публікації без контексту CPRS, а також дослідження моделювання без конкретних вимірюваних показників роботи мережі чи систем безпеки.

Концептуальна модель кодування

Розглянуті роботи класифіковані за вісьмома категоріями засобів контролю в моделі ZT: ідентифікація, стан пристрою, мікросегментація, безперервна автентифікація та авторизація, телеметрія, прийняття рішень щодо довіри, забезпечення дотримання політик та реагування на інциденти. Для CPRS кожна категорія розглядається крізь призму фізичної безпеки: при прийнятті рішення щодо довіри слід враховувати не лише те, хто запитує доступ, а й те, які фізичні дії можуть послідувати, наскільки актуальними є дані телеметрії, чи може робот безпечно продовжувати роботу у разі відключення, а також чи створює відмова у доступі більшу небезпеку, ніж обмежена робота.

На рис. 2 подано узагальнену архітектуру, яка пов’язує ідентичності, контекстну авторизацію, сегментацію, оцінювання телеметрії та реагування в єдиному циклі прийняття рішень.

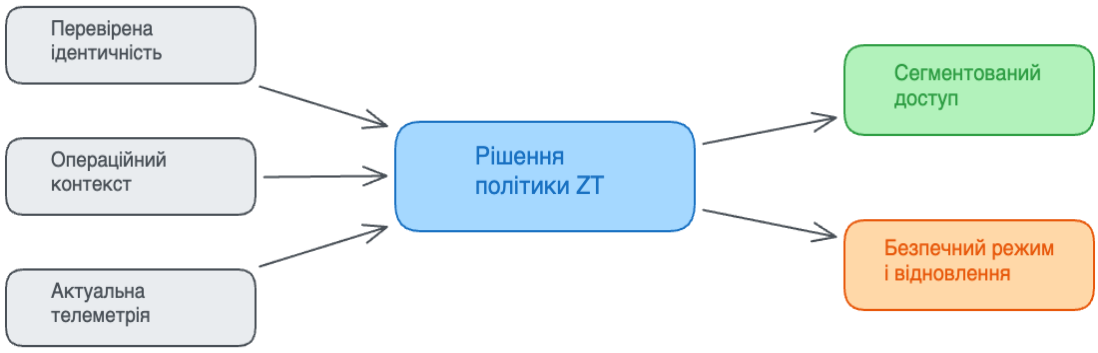

Рис. 2. Узагальнена архітектура застосування політик Zero Trust для кіберфізичних робототехнічних систем

Архітектура показує, що п’ять базових вимог мають виконуватися на кожному рівні: від ідентифікації суб’єкта до локального застосування політики та безпечного відновлення після порушення зв’язку.

Аналітичні аспекти

У статті використовуються чотири аналітичні виміри, які розкривають п’ять базових вимог ZT у дослідницькій моделі CPRS. Їх взаємозв’язок узагальнено в табл. 2. Ці виміри не утворюють ізольованого переліку контрольних пунктів: кожне рішення політики оцінюється за п’ятьма базовими вимогами ZT з урахуванням часу, фізичного руху, актуальності телеметрії та наслідків для безпеки. Тому однакова кібербезпекова дія може потребувати різних режимів реагування залежно від типу робота та умов місії.

Таблиця 2

Взаємозв’язок аналітичних вимірів дослідницької моделі Cyber-Physical Robotic Systems із базовими вимогами Zero Trust

Аналітичний вимір	Зміст у дослідницькій моделі CPRS	Базові вимоги ZT та операційна інтерпретація
Ідентичність активів	Суб’єкти й компоненти, представлені в моделі політики: робот, користувач, сервіс, датчик, виконавчий механізм, програмний вузол і канал оновлення.	Достовірна аутентифікація всіх активів. Права доступу, телеметрія та команди управління прив’язуються до конкретного елемента чи суб'єкта, ігноруючи топологію мережі як єдиний критерій довіри.
Операційний контекст	Змінні місії, робочого простору, мережі та фізичного стану, які впливають на рішення щодо доступу.	Динамічна авторизація на основі контексту. Правила доступу враховують специфіку поточного завдання, фізичний стан, часові рамки, динаміку переміщення та мінливість зовнішнього середовища.
Місце виконання	Рішення приймається у самому роботі, на периферійному шлюзі, у службі управління або в хмарі.	Мікросегментація та локалізований контроль. Розміщення точок застосування політик максимально близько до виконавчих механізмів запобігає латеральному (горизонтальному) поширенню загроз та гарантує автономність при втраті зв'язку.
Безпека реагування	Поведінка системи за невизначеної довіри, неповної телеметрії або погіршення якості зв’язку.	Валідація даних та платформозалежна відмовостійкість. Безперервна оцінка надійності телеметрії, здатність до роботи в обмеженому режимі та локальне відновлення. Сценарії безпеки адаптуються під тип пристрою (наприклад, протокол аварійної зупинки наземного апарата не підходить для дрона).

Рис. 3 конкретизує безперервну верифікацію як циклічний процес: збір телеметрії, оцінювання її актуальності й надійності, контекстне рішення, застосування політики та зворотний зв’язок.

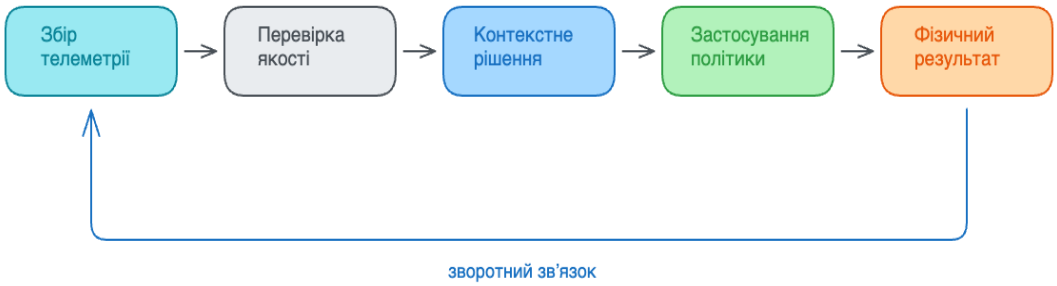

Рис. 3. Цикл безперервної верифікації, адаптований для кіберфізичних робототехнічних систем

Цикл забезпечує перегляд авторизації не лише за мережевою ідентичністю, а й за фазою місії, фізичним станом робота та достовірністю отриманої телеметрії; за невизначеності він переводить систему до обмеженого, але керованого режиму.

Описані сценарії формують структуру майбутньої комплексної перевірки п'яти вимог ZT. У поточній кампанії безпосередньо вимірюються лише характеристики безпроводового каналу, що впливають на актуальність телеметрії та вибір режиму реагування; ідентифікація, авторизація й сегментація залишаються атрибутами моделі та потребують окремих журналів політик.

Модель порушника та межі довіри

Модель порушника охоплює мережевого або автентифікованого зловмисника, здатного прослуховувати, затримувати, повторювати, підміняти чи блокувати повідомлення. Також передбачається можливість компрометації однієї STA, програмного сервісу або облікових даних оператора. Такі можливості відповідають загрозам підміни команд, маніпуляції телеметрією, відмови в обслуговуванні та латерального переміщення [1–3, 18, 23–25].

Захищеними активами є ідентичності роботів і користувачів, команди керування, телеметрія, стан політик, програмне забезпечення та канали виконавчих механізмів. Межі довіри проходять між роботом, AP і периферійним шлюзом, службою керування або хмарою та робочим місцем оператора. Перехід через кожну межу потребує перевірюваної ідентичності, контекстної авторизації та реєстрації рішення політики.

Поза межами поточного експерименту залишаються фізичне руйнування обладнання або атаки на ланцюг постачання. Симуляція не відтворює активну атаку й не доводить ефективність конкретного механізму ZT. Модель порушника визначає сценарії, для яких мережеві метрики надалі мають поєднуватися з журналами безпеки та фізичним станом робота.

Дизайн експерименту і простежування походження даних

Основну експериментальну кампанію виконано в симуляторі ns-3 версії 3.46.1 для топології з 20 STA та однією точкою доступу AP. Досліджено 14 фіксованих відстаней AP-STA: 30, 40, 50, 60, 70, 80, 85, 90, 100, 105, 110, 115, 120 і 125 м. На кожній відстані всі STA нерухомо та рівномірно розміщено на кільці навколо AP в одній площині ($z = 0$). Виконано по десять повторень із базовим параметром RngSeed = 1 та параметром незалежного підпотоку RngRun = 1–10; загалом отримано 140 трас.

Фізичний рівень відповідає IEEE 802.11ax WiFi 6 у діапазоні 5 ГГц: центральний канал 42 з частотою 5210 МГц, ширина 80 МГц, менеджер швидкості IdealWifiManager, потужність передавання AP і STA 24 дБмВт. AP має чотири антени та по чотири просторові потоки передавання й приймання; кожна STA – дві антени та по два просторові потоки. Черга канального рівня містить до 500 пакетів. Базова модель затухання LogDistance використовує показник втрат n = 3 та опорну відстань d_0 = 1 м, на якій опорні втрати становлять L_0 = 46,7 дБ як відношення переданої потужності до прийнятої; це значення відповідає втратам у вільному просторі за формулою Фріїса на відстані 1 м для частоти 5,15 ГГц. До неї послідовно додано модель завмирання Nakagami з порогами 80 і 200 м: m_0 = 1,5 для d < 80 м, m_1 = 0,75 для 80 ≤ d < 200 м та m_2 = 0,75 для $d \geq 200$ м.

Після початкової секунди кожна STA передає прикладному серверу на AP трафік через пакетний сокет: пакети корисного навантаження по 1500 байт з інтервалом 2,4 мс, тобто 5 Мбіт/с на STA і 100 Мбіт/с сумарного запропонованого навантаження. Метрики реєструються в односекундних інтервалах. Вибір ns-3 як дискретно-подієвого симулятора узгоджується з практикою мережевих досліджень [35, 38].

Сценарії типізовано за аналітичною роллю. Основна вимірювальна кампанія охоплює всі 140 трас і є єдиною основою для табл. 4 та рис. 4–9. Допоміжні калібрувальні й контрольні запуски використовуються лише для перевірки конфігурації та впливу окремих параметрів каналу; їх не включено до медіан, порогів або висновків основної кампанії. Такий поділ запобігає змішуванню різних топологій, навантажень і моделей поширення.

Походження кожної траси визначається назвою файла normal_distance{d}m_run{r}.csv, яка містить відстань і номер повторення. На початку файла події FIXED_STA_DISTANCE, FIXED_TX_POWER_DBM і NAKAGAMI_FADING підтверджують ключові параметри сценарію. Подальші записи мають часову мітку, ідентифікатор вузла NodeID, тип вузла, тип події та значення. У компактному режимі щосекундно фіксуються AGGREGATE_THROUGHPUT_MBPS, SENT_COUNT, RECV_COUNT і LATENCY_P95_MS; події ASSOC, JOINED та WIFI_DROP зберігають стан асоціації й відкидання пакетів. Код сценарію ns-3, скрипти запуску кампанії та всі 140 трас розміщено у відкритому репозиторії [39].

Поточний набір даних дає змогу відтворити aggregate goodput, p95 затримки та частку втрат на рівні прикладної доставки. Він не містить повних пакетних послідовностей, відношення сигнал/шум, джиттера,

кількості повторних передавань, схеми модуляції та кодування і причин втрат на всіх рівнях мережевого стека. Ці показники потребують окремого пакетного трасування та даних монітора потоків.

Отже, основна кампанія безпосередньо перевіряє умови зв'язку, що впливають на актуальність телеметрії та вибір безпечного режиму реагування. Ідентичність, контекстна авторизація та сегментація задаються як атрибути сценарію, але самі мережеві журнали не доводять правильність їх реалізації. Для повної перевірки п'яти вимог ZT мережеві дані потрібно поєднати з журналами політик і станом робота в конвеєрі.

Типізація та правила обробки даних

Основною метрикою є сукупна aggregate goodput на прикладному рівні, яку для кожного односекундного інтервалу обчислено один раз на AP

$$G = 8\,B_{\text{app}}/(106 \cdot T), \tag{1}$$

де B_{app} – кількість байтів корисного навантаження, фактично прийнятих одним сервером від усіх 20 STA, а T = 1 с. Показником прогону є медіана односекундних значень G; показником відстані – медіана десяти прогонів. Такий розрахунок усуває подвійний облік і не зараховує службовий обмін як корисні дані.

Дані поділено на конфігураційні параметри, сирі події, похідні безперервні метрики та індикатори рішення. У кожному односекундному інтервалі 'LATENCY_P95_MS' обчислюється лише за доставленими пакетами; показником прогону є 95-й процентиль цієї часової серії, а підсумком для відстані – медіана десяти прогонів. Частку втрат для прогону обчислено за сумами 'SENT_COUNT' і 'RECV_COUNT' за

$$L = 100 \cdot \left(1 - \frac{N_{\text{recv}}}{N_{\text{sent}}}\right), \tag{2}$$

після чого для відстані також використано медіану.

Ранню межу погіршення затримки визначено відносно бази 30 м; кандидатами є лише наступні виміряні відстані d_j > 30 м. Нехай

$$R_T(d_j) = \tilde{T}_{95}(d_j)/\tilde{T}_{95}(30), \tag{3}$$

де $\tilde{T}_{95}(d)$ – медіанний показник затримки. Індикатор $D_T(d_j)$ = 1, якщо $R_T(d_j) \geq 1{,}5$, $\tilde{T}_{95}(d_j) \geq 100$ мс і обидві умови виконуються на наступній відстані d_{j+1}. Межа d_T^* є найменшою відстанню-кандидатом, для якої D_T = 1. Значення 100 мс використовується як допоміжна нижня умова матеріальності, а не як самостійний поріг переходу.

Межу стійкої деградації втрат визначено окремо. Нехай

$$\Delta L(d_j) = \tilde{L}(d_j) - \tilde{L}(30), \tag{4}$$

де $\tilde{L}(d)$ – медіанна частка втрат. Індикатор $D_L(d_j)$ = 1, якщо $\Delta L(d_j) \geq 5$ відсоткових пунктів і $\Delta L(d_{j+1}) \geq 5$ відсоткових пунктів; інакше $D_L(d_j)$ = 0. Межа $d_L^* = \min\{d_j : D_L(d_j) = 1\}$.

Відносне зростання на 50%, допоміжна нижня умова 100 мс і приріст втрат на 5 відсоткових пунктів є наперед визначеними операційними критеріями алгоритму. Вони не є універсальними нормативами безпеки. Вимога повторного виконання критерію на наступній відстані відсіює одиничну флуктуацію. Міжпрогонову мінливість подано квартильним відхиленням Q та значеннями окремих прогонів.

У наступній кампанії записи мають доповнити наявні дані відношенням сигнал/шум, джиттером, повторними передаваннями та коефіцієнтом доставки пакетів. Журнали застосунків безпеки повинні фіксувати автентифікацію, авторизацію, версію політики, місце її застосування, надсилання телеметрії та перехід робота до обмеженого режиму. Усі рівні даних мають використовувати спільні 'TRACE_ID', 'NODE_ID' і часову шкалу, що підводить методику до конвеєра даних.

Результати систематизації досліджень Zero Trust для робототехнічних систем

Джерела систематизовано за механізмами ZT та їх придатністю до CPRS. Результат показує, що загальні праці з ZT групують контроль навколо ідентичності, шифрування, мікросегментації, розрахунку довіри й автоматизації безпеки [5, 6, 13, 14]. У працях про CPRS до цього набору додається аналіз міжрівневого переходу кіберкомпрометації у фізичну поведінку [33]. Окрему групу утворюють архітектурні та гарантійні шаблони, придатні до повторного застосування в CPRS [40–47].

Робототехнічні системи поєднують вбудовані контролери, проміжне програмне забезпечення, датчики, виконавчі механізми, мережеві інтерфейси та поведінку, орієнтовану на взаємодію з людиною,

що розширює їхню «поверхню атаки» порівняно зі звичайними кінцевими пристроями [1–3]. Найважливішою зміною для CPRS є те, що рішення щодо контролю доступу мають бути пов'язані з робочим станом. Наприклад, робот, який використовує застарілі телеметричні дані, не обов'язково має бути негайно відключений; йому може знадобитися обмежений локальний режим, зміна маршруту, обмеження швидкості, ручне передання керування або процедура повторної автентифікації на периферії [48–50].

Ці механізми контролю відображаються на п'ять базових вимог ZT, сформульованих у вступі, і в CPRS мають виконуватися спільно, а не вибірково. Окремі безпроводові дослідження оцінюють затримку, надійність і доступ до спектра в щільних Wi-Fi-середовищах, але не є доказом ефективності ZT у CPRS [51–53].

Зіставлення засобів контролю Zero Trust та обмежень робототехнічних систем

За процедурою концептуального кодування отримано зіставлення засобів контролю ZT з обмеженнями CPRS. Порівняно з корпоративними системами, робототехнічні платформи додатково потребують детермінованої синхронізації, роботи з обмеженими бортовими ресурсами та врахування вимог функціональної безпеки. Важливими також є змінна топологія мережі й доступність критичних локальних функцій за втрати зв'язку. Результат зіставлення наведено в табл. 3.

Дослідження безпеки ROS додатково підкреслюють цю проблему. Ефективність та зручність механізмів захисту відрізняються, а конфігурації за замовчуванням можуть не забезпечувати належного захисту від мережевих зловмисників [18]. Дослідження ROS також виявляють ризики в багатокористувацьких середовищах. До них належать підвищення привілеїв і витік інформації через вузли та теми [19]. Тому в CPRS із підходом ZT компоненти проміжного програмного забезпечення розглядаються як самостійні об'єкти політики [54–59]. Такими об'єктами є теми, сервіси, вузли, файли запуску, контейнери та мости, а не лише зовнішня мережева інфраструктура.

Таблиця 3

Засоби контролю Zero Trust та обмеження робототехнічних Cyber-Physical Systems

Контроль ZT	Обмеження CPRS	Дослідницька інтерпретація
Ідентичність	Роботи містять багато ідентичностей: оператор, робот, датчик, виконавчий механізм (актуатор), вузол, сервіс та канал оновлень.	Моделюйте машинну ідентичність на різних рівнях, а не лише ідентичність користувача.
Стан пристрою	Робот може бути в мережі, але при цьому фізично небезпечним, пошкодженим, з низьким зарядом акумулятора або працювати за межами параметрів місії.	Оцінка стану повинна включати індикатори як кібернетичного, так і фізичного «здоров'я».
Мікросегментація	Робототехнічні системи взаємодіють через топіки (теми), сервіси, API та цикли управління, які не завжди збігаються з межами сервісів на основі 'Internet Protocol' (IP).	Сегментуйте за функціями та завданнями, включаючи об'єкти на рівні проміжного програмного забезпечення.
Безперервна авторизація	Управління в реальному часі не може чекати на віддалені хмарні перевірки в кожному циклі.	Використовуйте локальні периферійні точки прийняття рішень та кешовані політики з правилами терміну дії.
Телеметрія	Телеметрія може надходити із затримкою, бути зашумленою, неповною або зловмисно сфальсифікованою.	Рішення щодо довіри повинні містити метадані про рівень впевненості та актуальність (свіжість) даних.
Реагування	Відмова в доступі може створити фізичну небезпеку, якщо робот рухається або несе вантаж.	Визначте режими обмежених дій та безпечного режиму відмови 'fail-safe' для ситуацій з невизначеним рівнем довіри.

Отримане зіставлення задає структуру подальшої експериментальної перевірки. Для кожного рішення потрібно визначати змінні стану, місце застосування політики, допустиму затримку та поведінку

за недоступності механізму політик. Окремі метрики мають показувати, чи підвищується кібербезпека без погіршення експлуатаційної безпеки.

Експериментальні результати характеризують лише прикладну доставку даних, затримку та втрати в заданій безпроводовій конфігурації. Вони дають змогу оцінити умови актуальності телеметрії та вибору контрольованого режиму реагування, але не є доказом реалізації сегментації, перевірюваної ідентифікації чи контекстної авторизації.

Результати моделювання стійкості безпроводової мережі

Результати основної кампанії отримано за протоколом 20 STA і однією AP, 14 відстаней, десять повторень і 140 трас. Для кожної відстані наведено медіани aggregate goodput, p95 затримки та втрат; значення окремих прогонів використано для відображення мінливості. Подальша інтерпретація стосується лише цієї конфігурації мережі та не переноситься автоматично на інші топології, навантаження або фізичні середовища.

Відповідно до правил, основною метрикою є aggregate goodput на прикладному рівні. Його обчислено один раз на AP за сумарною кількістю корисних байтів, прийнятих одним сервером від усіх 20 STA. Для кожної відстані наведено медіану десяти прогонів, а в CSV збережено щосекундні агреговані лічильники та p95 затримки. Аналіз розрізняє дві межі: раннє погіршення затримки на 40 м і межу стійкої деградації втрат на 50 м.

Як показано на рис. 4, за сумарного навантаження 100 Мбіт/с на 30 м система працює майже без втрат: медіанний aggregate goodput становить 99,936 Мбіт/с, p95 затримки – 189,4 мс, а втрати – 0,27%. Базове значення p95 уже перевищує 100 мс, тому межу не визначають за самим фактом цього перевищення. На 40 м aggregate goodput зберігається на рівні 99,210 Мбіт/с, однак p95 зростає в 1,86 рази відносно бази. На 50 м aggregate goodput зменшується до 90,531 Мбіт/с, а втрати зростають до 9,61%. Отже, стійке відносне погіршення затримки передує стійкому збільшенню втрат.

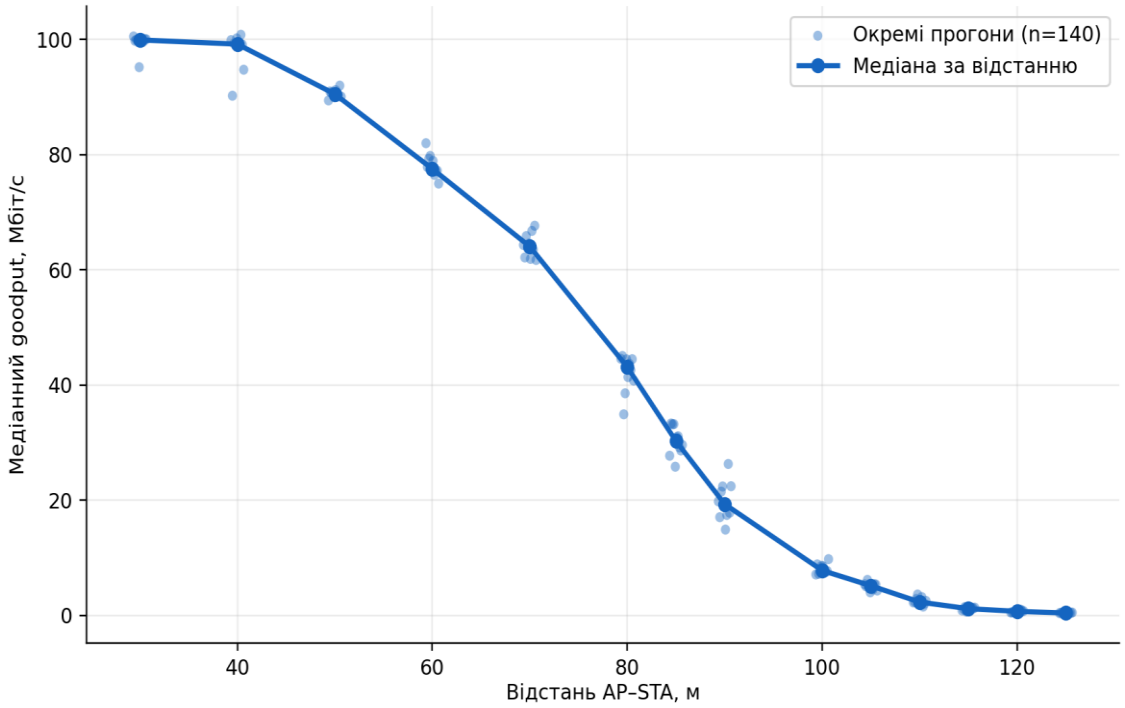

Рис. 4. Медіанний aggregate goodput і результати всіх 140 прогонів для топології 20 STA і однієї AP

Для кожної метрики міжпрогонову мінливість у табл. 4 подано у вигляді «медіана $\pm Q$», де $Q = (Q_3 - Q_1)/2$ – квартильне відхилення, тобто половина міжквартильного розмаху десяти повторень. Цей непараметричний показник характеризує розсіювання без припущення про нормальність розподілу і, на відміну від стандартного відхилення, не спотворюється одиничними викидами. Медіана залишається показником відстані, тому запис «медіана $\pm Q$» не є довірчим інтервалом і не передбачає симетричності розподілу.

Таблиця 4

Результати моделювання топології 20 STA і однією AP: медіана ± квартильне відхилення Q для десяти повторень на кожній відстані

Відстань AP-STA, м	Aggregate goodput, Мбіт/с; медіана ± Q	p95 затримки, мс; медіана ± Q
30	99,936±0,121	189,4±6,4
40	99,210±0,319	351,8±10,8
50	90,531±0,428	525,9±7,3
60	77,541±1,048	568,1±3,0
70	64,050±1,528	581,8±2,9
80	43,122±1,781	555,2±1,2
85	30,246±1,951	549,9±2,1
90	19,296±2,315	549,0±3,4
100	7,785±0,517	584,5±34,1
105	5,121±0,372	747,3±210,6
110	2,289±0,345	649,6±55,1
115	1,140±0,203	577,9±276,8
120	0,678±0,086	569,0±16,7
125	0,387±0,074	552,8±14,6

Табл. 4 узагальнює всі 140 трас кампанії. Aggregate goodput монотонно спадає від (99,936±0,121) Мбіт/с на 30 м до (0,387±0,074) Мбіт/с на 125 м, тобто більш ніж на два порядки. Втрати зростають так само монотонно – від (0,27±0,03)% до (99,81±0,05)%. Квартильне відхилення обох цих метрик залишається малим ($Q \leq 2{,}32$ Мбіт/с для goodput і $Q \leq 2{,}52$ відсоткового пункта для втрат), тому впорядкування відстаней є стійким і не зумовлене окремим повторенням.

Затримка поводиться інакше: у діапазоні 30–70 м p95 зростає монотонно – від (189,4±6,4) до (581,8±2,9) мс – за малого розсіювання ($Q \leq 10{,}8$ мс). Від 80 м показник виходить на плато 549–585 мс, а від 100 м втрачає монотонність: (584,5±34,1) мс на 100 м, (747,3±210,6) мс на 105 м і (649,6±55,1) мс на 110 м. Одночасно квартильне відхилення зростає на порядок, тобто саме там, де медіана перестає бути впорядкованою, оцінка стає найменш стійкою.

Немонотонність у зоні 100–125 м є артефактом вимірювання, а не покращенням каналу. Її причина – зміщення виживання: p95 обчислюється лише за доставленими пакетами. На 105 м медіанний прогін доставляє близько 8,0 тис. пакетів зі 150 тис. надісланих (94,66% втрат), а на 110 м – лише близько 3,6 тис. (97,59% втрат). У міру звуження цієї вибірки до неї потрапляють переважно пакети, які застали сприятливе вікно федінга й були доставлені швидко, тоді як пакети з тривалим перебуванням у черзі відкидаються і в p95 уже не враховуються. Тому падіння медіани з 747,3 до 649,6 мс відповідає не швидшій доставці, а зникненню повільних пакетів із вибірки.

Різниця між 105 і 110 м не є статистично значущою. Розподіли p95 за прогонами перекриваються майже повністю (548–1351 мс проти 552–1298 мс), а критерій Манна–Уїтні для двох груп по десять повторень дає $p \approx 0{,}65$. На 105 м розподіл до того ж двомодальний: чотири прогони дають 548–558 мс, а шість – 717–1351 мс, через що медіана потрапляє у верхню моду. Саме тому квартильне відхилення на цій відстані (210,6 мс) майже на два порядки перевищує значення на 50 м (7,3 мс).

Для CPRS на основі ZT це має конкретний наслідок: за втрат понад приблизно 90% p95 затримки втрачає діагностичну цінність і не може бути входом для політики. У цій зоні стійким індикатором залишається частка втрат або коефіцієнт доставки, які зберігають монотонність і малий розкид на всьому діапазоні. Тому обидві межі $d_T^* = 40$ м і $d_L^* = 50$ м визначено в межах 30–70 м, де затримка ще впорядкована, а не в зоні глибокої деградації.

Межі стійкості безпроводового каналу та контрольована деградація функцій

Для детального аналізу використано виміряний піддіапазон 30–60 м, що охоплює чотири рівні відстані та 40 незалежних прогонів у тій самій топології з 20 STA та одна AP. На 30 м медіанний aggregate goodput дорівнює 99,936 Мбіт/с, p95 – 189,4 мс, а втрати – 0,27%. На 40 м aggregate goodput становить 99,210 Мбіт/с, p95 – 351,8 мс і втрати – 0,86%. На 50 м aggregate goodput зменшується до 90,531 Мбіт/с, p95 зростає до 525,9 мс, а втрати – до 9,61%. На 60 м aggregate goodput становить 77,541 Мбіт/с, p95 – 568,1 мс і втрати – 22,74%.

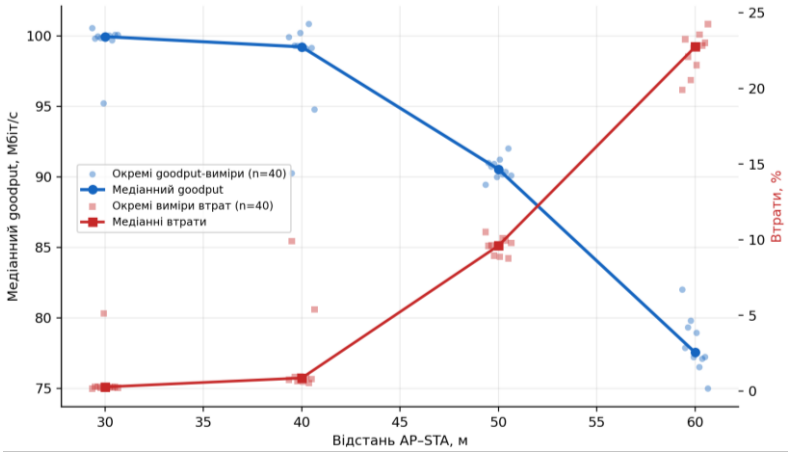

Рис. 5. Aggregate goodput і втрати у виміряному піддіапазоні 30–60 м

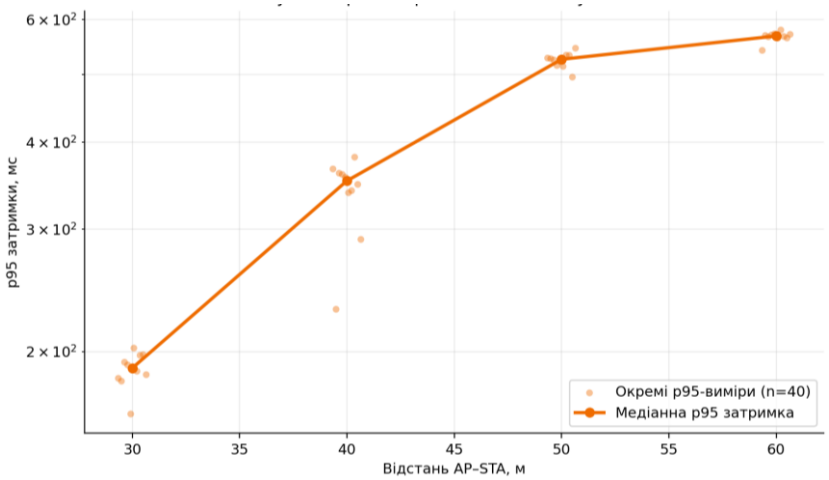

Рис. 6. p95 затримки у виміряному піддіапазоні 30–60 м: 40 прогонів і медіанна траєкторія

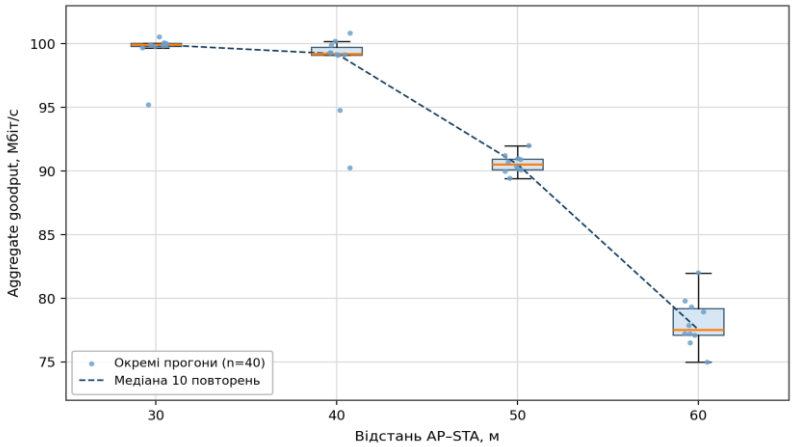

Рис. 7. Розподіл aggregate goodput у виміряному піддіапазоні 30–60 м

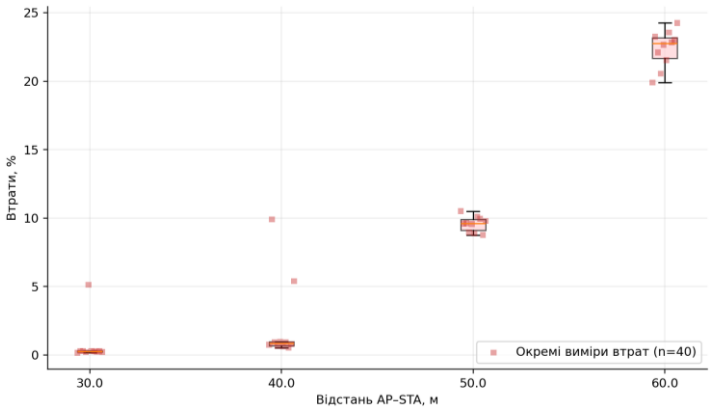

Рис. 8. Розподіл втрат у виміряному піддіапазоні 30–60 м

Рис. 5–8 показують двоетапну деградацію: p95 затримки істотно зростає вже на 40 м, тоді як стійке збільшення втрат формується від 50 м. Значення окремих прогонів та квартильне відхилення Q у табл. 4 підтверджують, що цей порядок не є наслідком лише одного випадкового повторення.

Для CPRS на основі ZT це означає, що рішення про режим роботи не слід пов'язувати з однією мережевою метрикою. Центральне застосування політик потрібно доповнювати локальними правилами, кешуванням останнього валідного рішення та контрольованою деградацією функцій. Погіршення каналу саме по собі не є доказом компрометації вузла: політика має одночасно враховувати ідентичність, походження подій і фізичний контекст.

Згідно з критеріями, базова відстань 30 м не є кандидатом на межу, навіть якщо її p95 перевищує допоміжний рівень 100 мс. Для 40 м $R_T(40)$ = 351,8/189,4 = 1,86, а на 50 м умова зберігається: $R_T(50)$ = 525,9/189,4 = 2,78. Тому $D_T(d)$ уперше набуває значення 1 на 40 м і d_T^* = 40 м.

Для втрат базовий рівень на 30 м становить 0,27%. На 40 м ΔL = 0,59 відсоткового пункта, тому поріг не досягнуто. На 50 м ΔL = 9,34 відсоткового пункта, а на наступній відстані 60 м приріст становить 22,47 відсоткового пункта. Отже, $D_L(d)$ переходить із 0 до 1 на 50 м і d_L^* = 50 м.

Рис. 9 відображає виміряний бінарний індикатор $D_L(d)$ та допоміжну логістичну інтерполяцію

$$S(d) = \left[1 + e^{-\frac{d - dL*}{2{,}5}}\right]^{-1}. \quad (5)$$

Масштаб 2,5 м задано лише для плавного візуального переходу: функція $S(d)$ не апроксимує сирі прогони, не є оцінкою ймовірності та не використовується для визначення d_L^*. Тому доказовою основою межі залишаються виміряні медіани й умова стійкості на наступній відстані.

Для CPRS на основі ZT дві межі мають різний операційний зміст. На 40 м система вже повинна підвищити контроль свіжості телеметрії та підготувати локальний режим, тоді як від 50 м стійке зростання втрат обґрунтовує обмеження функцій, кешування останнього валідного рішення або безпечне передання керування. Погіршення каналу саме по собі не доводить компрометацію: остаточне рішення політики має враховувати ідентичність, контекст і походження подій.

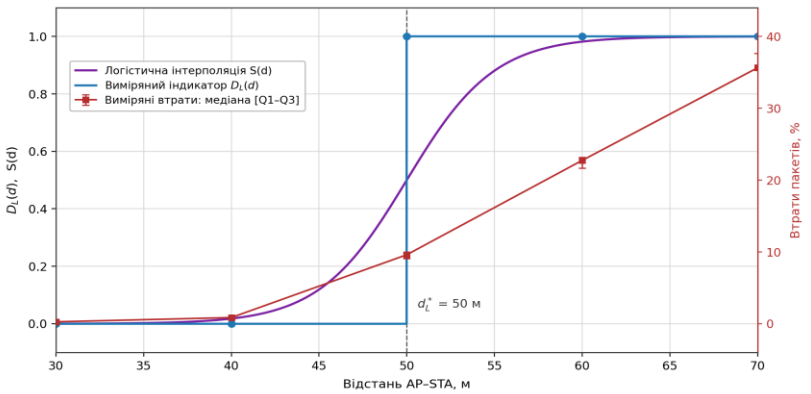

Рис. 9. Індикатор стійкої деградації втрат у діапазоні 30–70 м: виміряний перехід 0→1, виміряні медіани втрат із межами [Q_1–Q_3]

Отже, рис. 9 відокремлює виміряну межу стійкого зростання втрат від допоміжного способу її візуалізації. Перехід $D_L(d)$ до 1 є сигналом перевірити актуальність телеметрії та підготувати контрольоване обмеження функцій. Він не означає автоматичного визнання вузла скомпрометованим без урахування ідентичності, контексту місії та фізичного стану робота.

Конвеєр даних для подальшої валідації Zero Trust

Наявні траси ns-3 характеризують якість безпроводового зв'язку, але не охоплюють повний цикл прийняття та застосування політик ZT. Для подальшої валідації потрібен синхронізований конвеєр даних, у якому мережеві події, рішення безпеки й фізичний стан робота пов'язуються спільними ідентифікаторами 'TRACE_ID' і 'NODE_ID', часовою міткою та фазою місії. Така структура дає змогу відновити причинну послідовність від зміни каналу до рішення політики й реакції робота.

У конвеєрі типізовано три взаємопов'язані рівні даних:

1. Перший рівень містить показники зв'язку: aggregate goodput, p95 затримки, втрати пакетів, джиттер, події асоціації та доступність каналу. Ці записи показують, які дані були фактично доставлені та чи залишалися вони актуальними для рішення політики.

2. Другий рівень описує роботу засобів безпеки: автентифікацію, контекст запиту, оцінку довіри, рішення про дозвіл, обмеження або відмову, версію політики, місце її застосування та використання периферійного кешу.

3. Третій рівень фіксує фізичний стан робота: фазу місії, положення, тип команди, узгодженість показань датчиків, стан виконавчих механізмів, перехід до обмеженого режиму та час відновлення. Об'єднання трьох рівнів за спільними ключами дає змогу оцінити не лише кібербезпековий результат, а й його вплив на безпечність та виконання місії. Узагальнену структуру конвеєра наведено на рис. 10.

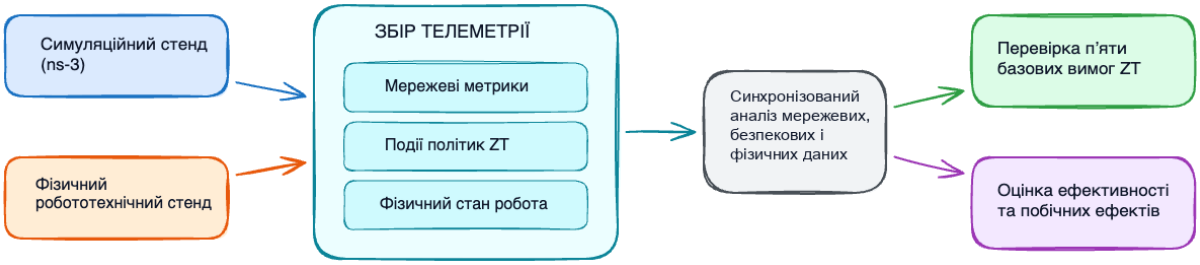

Рис. 10. Конвеєр телеметрії та доказів для подальших досліджень на базі ns-3 та робототехнічних випробувальних стендів

Конвеєр даних пов'язує мережеві метрики, події безпеки та фізичний стан робота. У наступних експериментах він дасть змогу окремо перевіряти п'ять базових вимог ZT. Ідентичність перевірятиметься за атрибутами суб'єкта й вузла; контекстна авторизація – за фазою місії та станом; сегментація – за зоною і точкою застосування політики. Надійність телеметрії оцінюватиметься за часом і повнотою доставки, а безпечне реагування – за фактичним переходом до обмеженого режиму та відновленням.

ОБГОВОРЕННЯ ТА РЕКОМЕНДАЦІЇ ДО ВПРОВАДЖЕННЯ

Запропоновані архітектурні наслідки розглядаються крізь усі п'ять вимог ZT – від перевірки ідентичності та контекстної авторизації до сегментації, контролю телеметрії й відновлення після порушення.

Наслідки впровадження моделі Zero Trust

Експеримент виявив двоетапний характер погіршення зв'язку. На 40 м p95 затримки зростає в 1,86 рази відносно бази, тоді як aggregate goodput залишається 99,210 Мбіт/с, а медіанні втрати не перевищують 0,86%. На 50 м починається стійке зростання втрат і зниження прикладної доставки.

На відміну від досліджень, у яких показники безпроводової мережі розглядаються лише як характеристики QoS [51–53], у цій роботі вони слугують вхідними умовами для політик ZT. Раннє зростання затримки обґрунтовує посилений контроль актуальності телеметрії. Стійке зростання втрат вимагає переходу до локальних правил та обмеженого режиму.

Поточні траси не дають змоги встановити механізм зростання p95. Його можливими причинами є накопичення черг, повторні передавання або зміна схеми модуляції та кодування, але це лише гіпотези. Для їх розмежування потрібні дані про заповнення черг, MAC-повтори, SNR та вибрану схему модуляції.

Застосування політик Zero Trust у кіберфізичних робототехнічних систем

Функції прийняття та застосування політик у CPRS розподіляються між роботом, периферійним шлюзом і хмарним рівнем. Централізоване рішення забезпечує цілісність політик, аудит і глобальний контекст загроз, однак залежить від безпроводового каналу. Локальне рішення зменшує затримку, але використовує обмежений контекст і бортові ресурси.

Тому доцільною є ієрархічна модель. Хмара формує та поширює політики, периферійний шлюз застосовує їх у локальній зоні й агрегує телеметрію, а робот виконує мінімальний набір перевірок. За втрати з'єднання він переходить до наперед визначеного безпечного режиму [10, 12, 15, 16, 60].

Мікросегментацію в CPRS потрібно визначати за функціональним призначенням компонентів і фізичним контекстом місії, а не лише за IP-адресацією. Межі доступу встановлюються для груп роботів, зон, тем і сервісів, потоків датчиків, каналів керування, оновлень та аварійних шляхів.

Рішення щодо доступу враховує ідентичність суб'єкта, його роль, стан робота, рівень ризику дії та актуальність телеметрії. Це обмежує латеральне переміщення без порушення необхідної координації [11, 17]. Розподіл рівнів і режимів деградації узагальнено в табл. 5.

Таблиця 5

Застосування політик Zero Trust у Cyber-Physical Robotic Systems визначає рівні архітектури та режими безпечної деградації

Рівень архітектури	Критерій прийняття рішення	Механізми застосування політик	Режим безпечної деградації
Робот	Команда відповідає ідентичності суб'єкта, поточному стану робота та обмеженням місії.	Локальна точка застосування політики контролює доступ до ROS, перевіряє команди та здійснює моніторинг безпеки.	Небезпечна команда відхиляється, рух обмежується, а робот переходить до безпечного стану.
Периферійний шлюз	Взаємодія суб'єкта з роботом обмежується визначеною зоною, місією та мережевим сегментом.	Точка застосування політики шлюзу фільтрує теми й сервіси, перевіряє телеметрію та зберігає кеш політик.	Кешована політика забезпечує продовження обмежених дій, ізоляцію підозрілого вузла та збереження аварійного каналу.
Хмарний рівень	Ідентичність, стан пристрою, рівень ризику та завдання узгоджуються з централізованою політикою.	Служби ідентичності, API керування, аудит, сервіс оновлень і розповсюдження політик забезпечують централізоване керування.	Відкликання облікових даних, ротація політик та ініціювання реагування на інцидент виконуються на хмарному рівні.
Операційна безпека	Сукупність подій використовується для виявлення аномалії, компрометації або латерального переміщення.	Кореляція подій, виявлення аномалій та оркестрація реагування формують контур операційної безпеки.	Підтвердження інциденту оновлює оцінку довіри та уточнює правила і політики.

Система показників охоплює всі п'ять вимог ZT, оскільки поєднує оцінювання ідентичності та авторизації, латерального переміщення, якості телеметрії, безпечної деградації та часу відновлення.

Покращення показників оцінки

Модель CPRS на основі підходу ZT слід оцінювати не лише за точністю виявлення. Показники безпеки повинні включати блокування несанкціонованих команд, зменшення латерального переміщення, правильність прийняття рішень щодо політики, стійкість до зловживання обліковими даними та час відновлення після компрометації. Метрики мережі повинні включати затримку, коливання, пропускну

здатність, втрату потоку, накладні витрати на керуючі повідомлення та затримку оновлення політики. Метрики робототехніки повинні включати виконання місії, частоту переходу в безпечний режим, причину відхилення команд, фізичне відхилення від запланованої траєкторії та частоту втручання оператора.

Оцінка також має включати показники невизначеності. У реальних CPRS механізм формування політики може діяти на основі неповних телеметричних даних, затриманих пакетів або суперечливих показань датчиків. Тому корисна модель довіри має повідомляти про рівень впевненості у своєму рішенні та зберігати обґрунтування цього рішення. Це особливо важливо для наукового внеску на рівні докторської дисертації, оскільки дозволяє відрізнити простий набір правил від моделі, яку можна аналізувати, тестувати та вдосконалювати.

Обмеження дослідження

Емпіричні висновки обмежені симуляцією однієї конфігурації: 20 однорідних нерухомих STA на кільці, 1 AP, однакове навантаження, співплощинне розміщення без перешкод, мобільності та зовнішніх завад. Після 80 м параметр моделі Nakagami змінюється з 1,5 на 0,75, тому далека ділянка кривих відображає одночасно збільшення відстані та інший режим завмирання. Виявлені межі 40 і 50 м лежать до цього переходу, однак не є універсальними радіусами працездатності для реальних робототехнічних систем.

p95 затримки обчислено лише за доставленими пакетами, тому за великих втрат виникає зміщення виживання: показник не характеризує пакети, які не були доставлені. Саме цим зумовлена немонотонність p95 у зоні 100–125 м, де частка доставлених пакетів падає нижче 10%, тому в цій зоні показник не є придатним входом для політики. Десять повторень, медіани та квартильні відхилення забезпечують відтворюваний опис саме цієї кампанії, але не замінюють довірчих інтервалів, перевірки гіпотез або фізичного стенда. Крім того, мережеві траси не перевіряють ідентифікацію, авторизацію чи сегментацію; для цього потрібні синхронізовані журнали політик, подій безпеки та фізичного стану робота.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропоновано трактувати ZT у CPRS як безперервну, контекстно-орієнтовану й відмовостійку архітектуру керування. Вона поєднує перевірювану ідентифікацію, контекстну авторизацію, сегментацію, контроль актуальності телеметрії та безпечне реагування з фізичним станом робота.

Експериментальна кампанія в ns-3 охопила 140 незалежних прогонів для 14 відстаней AP-STA та топології з 20 STA і однієї AP. На 40 м p95 затримки зріс у 1,86 рази відносно бази 30 м, хоча aggregate goodput залишався 99,210 Мбіт/с. На 50 м втрати досягли 9,61% і зберегли стійке зростання на наступній відстані. На 125 м aggregate goodput знизився до 0,387 Мбіт/с, а втрати зросли до 99,81%.

Отримані результати показують, що погіршення часових характеристик передує масовій втраті прикладних даних. Тому централізоване рішення політики потрібно доповнювати локальними правилами, контролем свіжості телеметрії та контрольованою деградацією функцій. Водночас мережеві метрики не доводять ефективність конкретного механізму ZT і не встановлюють універсальної безпечної відстані.

В рамках подальших досліджень та публікацій передбачено родовження роботи над обеднанням мережних метрик, журналів політик, подій безпеки та фізичний стан робота в єдиному конвеєрі даних. Це дасть змогу окремо перевірити всі п’ять вимог ZT і визначити, чи забезпечує обраний режим реагування не лише кібербезпеку, а й безпечне виконання місії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations. *Int. J. Inf. Secur., 21*, 115–158. https://doi.org/10.1007/s10207-021-00545-8
2. Pu, H., He, L., Cheng, P., Sun, M., & Chen, J. (2023). Security of Industrial Robots: Vulnerabilities, Attacks, and Mitigations. *IEEE Netw., 37*, 111–117. https://doi.org/10.1109/mnet.116.2200034
3. Haskard, A., & Herath, D. (2025). Secure Robotics: Navigating Challenges at the Nexus of Safety, Trust, and Cybersecurity in Cyber-Physical Systems. *ACM Comput. Surv., 57*, 1–48. https://doi.org/10.1145/3723050
4. Yu, Z., Gao, H., Cong, X., Wu, N., & Song, H. (2023). A Survey on Cyber-Physical Systems Security. *IEEE Internet Things J., 10*, 21670–21686. https://doi.org/10.1109/jiot.2023.3289625

6. Syed, N., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z. A., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access, 10*, 57143–57179. https://doi.org/10.1109/access.2022.3174679
7. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wirel. Commun. Mob. Comput., 2022*(1). https://doi.org/10.1155/2022/6476274
8. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *NIST Special Publication 800-207*. https://doi.org/10.6028/NIST.SP.800-207
9. Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust Maturity Model, Version 2.0. *CISA Guidance*. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model
10. Feng, X., & Hu, S. (2023). Cyber-Physical Zero Trust Architecture for Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Cyber Phys. Syst., 1*, 394–405. https://doi.org/10.1109/ticps.2023.3333850
11. Hasan, S., Amundson, I., & Hardin, D. S. (2023). Zero Trust Architecture Patterns for Cyber-Physical Systems. *SAE Tech. Pap. Ser.*. https://doi.org/10.4271/2023-01-1001
12. Bello, A., Diyan, M., & Asghar, I. (2025). Zero Trust Implementation for Legacy Systems using Dynamic Microsegmentation, Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC). In *2025 4th Int. Conf. on Computing and Information Technology (ICCIT)*, 181–189. https://doi.org/10.1109/iccit63348.2025.10989392
13. Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible Zero Trust Architecture for the Cybersecurity of Industrial IoT Infrastructures. *Ad Hoc Netw., 156*, 103414. https://doi.org/10.1016/j.adhoc.2024.103414
14. Paul, B., & Rao, M. (2022). Zero-Trust Model for Smart Manufacturing Industry. *Appl. Sci*. https://doi.org/10.3390/app13010221
15. Li, K., Li, C., Yuan, X., Li, S.-F., Zou, S., Ahmed, S. S., Ni, W., Niyato, D., Jamalipour, A., Dressler, F., & Akan, O. B. (2025). Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things. *IEEE Internet Things J., 12*, 46269–46293. https://doi.org/10.1109/jiot.2025.3603957
16. Mahmud, R., Jin, J., Kua, J., Afrin, M., Mistry, S., & Krishna, A. (2025). Trusted Microservice Orchestration for Secure Edge Computing in Industrial Cyber-Physical Systems. *IEEE Netw., 39*, 70–78. https://doi.org/10.1109/mnet.2025.3541032
17. Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity Solutions for Industrial Internet of Things-Edge Computing Integration: Challenges, Threats, and Future Directions. *Sens., 25*. https://doi.org/10.3390/s25010213
18. Zanasi, C., Marasco, I., & Colajanni, M. (2025). Graph based threat detection system for a microsegmentation Zero Trust Architecture. In *2025 IEEE Conf. on Dependable, Autonomic and Secure Computing (DASC)*, 31–39. https://doi.org/10.1109/dasc68382.2025.00012
19. Goerke, N., Timmermann, D., & Baumgart, I. (2021). Who Controls Your Robot? An Evaluation of ROS Security Mechanisms. In *2021 7th Int. Conf. on Automation, Robotics and Applications (ICARA)*, 60–66. https://doi.org/10.1109/icara51699.2021.9376468
20. Xia, L., Gao, X., & Shi, W. (2025). Investigating Security Threats in Multi-Tenant ROS 2 Systems. *2025 IEEE International Conference on Robotics and Automation (ICRA)*, 16441–16448. https://doi.org/10.1109/icra55743.2025.11127490
21. Shaik, A. K., Mohammadi, A., & Malik, H. A. M. (2025). A Systematic Review of Sensor Vulnerabilities and Cyber-Physical Threats in Industrial Robotic Systems. *IET Cyber Phys. Syst. Theory Appl., 10*. https://doi.org/10.1049/cps2.70023
22. Bhardwaj, A., Bharany, S., Rehman, A., Tejani, G. G., & Hussen, S. (2025). Securing Cyber-Physical Robotic Systems for Enhanced Data Security and Real-Time Threat Mitigation. *EURASIP J. Inf. Secur., 2025*. https://doi.org/10.1186/s13635-025-00186-7
23. Holdbrook, R., Odeyomi, O., Yi, S., & Roy, K. (2024). Network-Based Intrusion Detection for Industrial and Robotics Systems: A Comprehensive Survey. *Electron*. https://doi.org/10.3390/electronics13224440
24. Burg, A., Chattopadhyay, A., & Lam, K.-Y. (2018). Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-Things. *Proceedings of the IEEE, 106*(1), 38–60. https://doi.org/10.1109/JPROC.2017.2780172
25. Guo, P., Kim, H., Virani, N., Xu, J., Zhu, M., & Liu, P. (2017). Exploiting Physical Dynamics to Detect Actuator and Sensor Attacks in Mobile Robots. *arXiv:1708.01834*. https://doi.org/10.48550/arXiv.1708.01834
26. Ge, Y., & Zhu, Q. (2024). GAZETA: GAme-Theoretic Zero-Trust Authentication for Defense Against Lateral Movement in 5G IoT Networks. *IEEE Trans. Inf. Forensics Secur., 19*, 540–554. https://doi.org/10.1109/TIFS.2023.3326975

27. Tushkanova, O., Levshun, D., Branitskiy, A., Fedorchenko, E., Novikova, E., & Kotenko, I. (2023). Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. *Algorithms, 16*, 85. https://doi.org/10.3390/a16020085
28. Moriano, P., Hespeler, S., Li, M., & Mahbub, M. (2024). Adaptive Anomaly Detection for Identifying Attacks in Cyber-Physical Systems: A Systematic Literature Review. *Artif. Intell. Rev., 58*. https://doi.org/10.1007/s10462-025-11292-w
29. Ji, R., Padha, D., Singh, Y., & Sharma, S. (2024). Review of Intrusion Detection System in Cyber-Physical System Based Networks: Characteristics, Industrial Protocols, Attacks, Data Sets and Challenges. *Trans. Emerg. Telecommun. Technol., 35*. https://doi.org/10.1002/ett.5029
30. Zhukabayeva, T., Ahmad, Z., Adamova, A., Karabayev, N., & Abdildayeva, A. (2025). An Edge-Computing-Based Integrated Framework for Network Traffic Analysis and Intrusion Detection to Enhance Cyber-Physical System Security in Industrial IoT. *Sens., 25*. https://doi.org/10.3390/s25082395
31. Manzoor, S., Yin, Y., Gao, Y., Hei, X., & Cheng, W. (2020). A Systematic Study of IEEE 802.11 DCF Network Optimization From Theory to Testbed. *IEEE Access, 8*, 154114–154132. https://doi.org/10.1109/access.2020.3018088
32. Venkateswaran, S. K., Tai, C.-L., Garnayak, R., Ben-Yehezkel, Y., Alpert, Y., & Sivakumar, R. (2024). IEEE 802.11ax Target Wake Time: Design and Performance Analysis in ns-3. In *2024 Workshop on ns-3*. https://doi.org/10.1145/3659111.3659115
33. Assasa, H., Grosheva, N., Ropitault, T., Blandino, S., Golmie, N., & Widmer, J. (2021). Implementation and Evaluation of a WLAN IEEE 802.11ay Model in Network Simulator ns-3. In *2021 Workshop on ns-3*. https://doi.org/10.1145/3460797.3460799
34. Hasan, S., Amundson, I., & Hardin, D. (2024). Zero-trust Design and Assurance Patterns for Cyber-Physical Systems. *J. Syst. Archit., 155*, 103261. https://doi.org/10.1016/j.sysarc.2024.103261
35. Botta, A., Rotbei, S., Zinno, S., & Ventre, G. (2023). Cyber Security of Robots: A Comprehensive Survey. *Intell. Syst. Appl., 18*, 200237. https://doi.org/10.1016/j.iswa.2023.200237
36. Campanile, L., Gribaudo, M., Iacono, M., Marulli, F., & Mastroianni, M. (2020). Computer Network Simulation with ns-3: A Systematic Literature Review. *Electron.* https://doi.org/10.3390/electronics9020272
37. Jeffrey, N., Tan, Q., & Villar, J. (2023). A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. *Electron.* https://doi.org/10.3390/electronics12153283
38. Puccetti, T., Nardi, S., Cinquilli, C., Zoppi, T., & Ceccarelli, A. (2024). ROSPaCe: Intrusion Detection Dataset for a ROS2-Based Cyber-Physical System and IoT Networks. *Sci. Data, 11*. https://doi.org/10.1038/s41597-024-03311-2
39. Manzoor, S., Manzoor, M., Manzoor, H., Adan, D. E., & Kayani, M. A. (2023). Which Simulator to Choose for Next Generation Wireless Network Simulations? NS-3 or OMNeT++. *IEEC 2023*. https://doi.org/10.3390/engproc2023046036
40. Pakhomov, M. V. (2026). *ns3-wifi6-zero-trust-cprs: ns-3 Simulation Environment and Traces for the 20 STA / 1 AP IEEE 802.11ax Campaign* [Source code]. GitHub. https://github.com/m1fril/ns3-wifi6-zero-trust-cprs
41. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sens., 24*. https://doi.org/10.3390/s24041328
42. Dattatreya, V., Adudhodla, M., Anupkant, S., Bande, V., Prasad, C. G. V. N., & Manellore, P. K. R. (2025). Edge-Forged Resilience: A Zero-Trust Security Architecture for Autonomous Cyber-Physical Systems in Industry 5.0. In *2025 6th Int. Conf. on Smart Electronics and Communication (ICOSEC)*, 1262–1268. https://doi.org/10.1109/icosec67334.2025.11459650
43. Kim, S., Park, K.-J., & Lu, C. (2022). A Survey on Network Security for Cyber-Physical Systems: From Threats to Resilient Design. *IEEE Commun. Surv. Tutor., 24*, 1534–1573. https://doi.org/10.1109/comst.2022.3187531
44. Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2021). Cybersecurity of Industrial Cyber-Physical Systems: A Review. *ACM Comput. Surv., 54*, 1–35. https://doi.org/10.1145/3510410
45. Nweke, L. O. (2021). A Survey of Specification-based Intrusion Detection Techniques for Cyber-Physical Systems. *Int. J. Adv. Comput. Sci. Appl., 12*. https://doi.org/10.14569/ijacsa.2021.0120506

46. Tan, S., Guerrero, J., Xie, P., Han, R., & Vasquez, J. (2020). Brief Survey on Attack Detection Methods for Cyber-Physical Systems. *IEEE Syst. J., 14*, 5329–5339. https://doi.org/10.1109/jsyst.2020.2991258
47. Xing, W., & Shen, J. (2024). Security Control of Cyber-Physical Systems under Cyber Attacks: A Survey. *Sens., 24*. https://doi.org/10.3390/s24123815
48. Ferrag, M., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl., 50*. https://doi.org/10.1016/j.jisa.2019.102419
49. Da Silva, E. F., Santoso, F., & Zheng, L. (2025). A Deep Learning-Based Intrusion Detection System for Safeguarding ROS 2-Powered Unmanned Ground Vehicles Against DoS Attacks. In *2025 Int. Joint Conf. on Neural Networks (IJCNN)*, 1–9. https://doi.org/10.1109/ijcnn64981.2025.11229203
50. Santoso, F., & Finn, A. (2023). A Data-Driven Cyber-Physical System Using Deep-Learning Convolutional Neural Networks: Study on False-Data Injection Attacks in an Unmanned Ground Vehicle Under Fault-Tolerant Conditions. *IEEE Trans. Syst. Man Cybern. Syst., 53*, 346–356. https://doi.org/10.1109/tsmc.2022.3170071
51. Fernandez, I., Neupane, S., Chakraborty, T., Mitra, S., Mittal, S., Pillai, N., Chen, J., & Rahimi, S. (2024). A Survey on Privacy Attacks Against Digital Twin Systems in AI-Robotics. In *2024 IEEE 10th Int. Conf. on Collaboration and Internet Computing (CIC)*, 70–79. https://doi.org/10.1109/cic62241.2024.00019
52. Alauthman, A., & Shraa, T. (2025). Performance Evaluation and Latency Optimization of Wi-Fi 7 in High-Density Wireless Environments. *Int. J. Electr. Electron. Eng. Telecommun.*. https://doi.org/10.18178/ijeetc.14.6.354-364
53. Ahrar, E. M., Wilhelmi, F., Galati-Giordano, L., Imputato, P., Menth, M., & Avallone, S. (2025). R-TWT in Wi-Fi 7 and Beyond: Enabling Bounded Latency, Energy Efficiency, and Reliability. In *2025 IEEE 30th Int. Conf. on Emerging Technologies and Factory Automation (ETFA)*, 1–8. https://doi.org/10.1109/etfa65518.2025.11205686
54. Alauthman, A., & Shraa, T. (2025). Deep Reinforcement Learning-Driven Dynamic Spectrum Access in Dense Wi-Fi Environments. *IEEE Access, 13*, 178663–178680. https://doi.org/10.1109/access.2025.3621489
55. Yang, S., Guo, J., & Rui, X. (2024). Formal Analysis and Detection for ROS2 Communication Security Vulnerability. *Electron*. https://doi.org/10.3390/electronics13091762
56. Soriano, E., Martin, F., & Guardiola, G. (2024). Implementing a Robot Intrusion Prevention System (RIPS) for ROS 2. *arXiv:2412.19272*. https://arxiv.org/abs/2412.19272
57. Santoso, F., & Finn, A. (2024). Trusted Operations of a Military Ground Robot in the Face of Man-in-the-Middle Cyberattacks Using Deep Learning Convolutional Neural Networks: Real-Time Experimental Outcomes. *IEEE Trans. Dependable Secur. Comput., 21*, 2273–2284. https://doi.org/10.1109/tdsc.2023.3302807
58. Zailan, N. S. B., Ong, L.-Y., & Lim, H. (2026). NAVBOT25: Dataset for ROS-Based Autonomous Robot Navigation. *Data Br., 65*. https://doi.org/10.1016/j.dib.2026.112617
59. Yaseen, Y. A., Almomani, I., & Al-Akhras, M. (2025). A Survey of Security Threats and Defense Mechanisms in ROS2-Based Internet of Drones Systems. In *2025 Int. Conf. on Computer and Applications (ICCA)*, 1–6. https://doi.org/10.1109/icca66035.2025.11430817
60. Papoutsakis, M., Hatzivasilis, G., Michalodimitrakis, E., Ioannidis, S., Michael, M. K., Savva, A. D., Nikolaou, P., Stokkou, E., & Bozdemir, G. (2025). SESAME: Automated Security Assessment of Robots and Modern Multi-Robot Systems. *Electron*. https://doi.org/10.3390/electronics14050923
61. Muriithi, G., Papari, B., Arsalan, A., Timilsina, L., Muriithi, A., Buraimoh, E., Khan, A., Ozkan, G., Edrington, C. S., & Papari, A. (2025). Zero Trust Architecture for Electric Transportation Systems: A Systematic Survey and Deep Learning Framework for Replay Attack Detection. *IEEE Open J. Veh. Technol., 6*, 2171–2194. https://doi.org/10.1109/ojvt.2025.3592041

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Mykhailo V. Pakhomov
Ph.D. student of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID 0009-0007-7343-6912
m.pakhomov.asp@kubg.edu.ua

Volodymyr Y. Sokolov
Ph.D., associate professor
associate professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

ADAPTATION OF ZERO TRUST ARCHITECTURE FOR CYBER-PHYSICAL ROBOTIC SYSTEMS: BASIC REQUIREMENTS AND WIRELESS CHANNEL RESILIENCE LIMITS

Abstract. The problem of applying the Zero Trust approach to the security of Cyber-Physical Robotic Systems is analyzed. It is substantiated that the close interaction of network computing, sensors, actuators and physical control systems forms a single risk plane, where the compromise of identification data, telemetry or communication channels threatens both information leakage and dangerous physical incidents. The research area covers industrial and mobile robots, unmanned aerial vehicles, service and collaborative robots, the functioning of which depends on cyber components capable of influencing physical behavior. Within the framework of the architecture development, five basic Zero Trust requirements were formulated: verifiable identification, contextual authorization, network segmentation, assessment of telemetry relevance and reliability, as well as adaptive response with limited operation and local fault tolerance. To determine the limits of the stability of the wireless control channel, simulation modeling was performed in the ns-3 environment (IEEE 802.11ax WiFi 6 standard, one access point, 20 client stations). Based on the analysis of 140 routes (distances 30–125 m, total load 100 Mbps), the aggregate useful throughput (aggregate goodput), p95 delay, and packet loss percentage were estimated. A two-stage nature of the communication channel degradation was revealed: the early time degradation limit was recorded at a distance of 40 m (p95 delay jump to 351.8 ms with almost no loss), and the limit of stable loss degradation was recorded at 50 m (losses of 9.61%). At a critical distance of 125 m, goodput decreases to 0.387 Mbps with losses of 99.81%. It was established that the obtained wireless communication stability limits are decisive for telemetry delivery and response mode selection, but in isolation do not guarantee the implementation of Zero Trust. For comprehensive validation of the zero-trust architecture, a pipeline for synchronized analysis of network metrics, security events, and the physical state of the robot is proposed.

Keywords: Zero Trust, cybersecurity, cyber-physical system, robotic system, ns-3, resilience, wireless communication, continuous verification, authorization, security policy.

REFERENCES

1. Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations. *Int. J. Inf. Secur., 21*, 115–158. https://doi.org/10.1007/s10207-021-00545-8
2. Pu, H., He, L., Cheng, P., Sun, M., & Chen, J. (2023). Security of Industrial Robots: Vulnerabilities, Attacks, and Mitigations. *IEEE Netw., 37*, 111–117. https://doi.org/10.1109/mnet.116.2200034
3. Haskard, A., & Herath, D. (2025). Secure Robotics: Navigating Challenges at the Nexus of Safety, Trust, and Cybersecurity in Cyber-Physical Systems. *ACM Comput. Surv., 57*, 1–48. https://doi.org/10.1145/3723050
4. Yu, Z., Gao, H., Cong, X., Wu, N., & Song, H. (2023). A Survey on Cyber-Physical Systems Security. *IEEE Internet Things J., 10*, 21670–21686. https://doi.org/10.1109/jiot.2023.3289625

5. Syed, N., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z. A., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access, 10*, 57143–57179. https://doi.org/10.1109/access.2022.3174679
6. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wirel. Commun. Mob. Comput., 2022*(1). https://doi.org/10.1155/2022/6476274
7. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *NIST Special Publication 800-207*. https://doi.org/10.6028/NIST.SP.800-207
8. Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust Maturity Model, Version 2.0. *CISA Guidance*. https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model
9. Feng, X., & Hu, S. (2023). Cyber-Physical Zero Trust Architecture for Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Cyber Phys. Syst., 1*, 394–405. https://doi.org/10.1109/ticps.2023.3333850
10. Hasan, S., Amundson, I., & Hardin, D. S. (2023). Zero Trust Architecture Patterns for Cyber-Physical Systems. *SAE Tech. Pap. Ser.*. https://doi.org/10.4271/2023-01-1001
11. Bello, A., Diyan, M., & Asghar, I. (2025). Zero Trust Implementation for Legacy Systems using Dynamic Microsegmentation, Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC). In *2025 4th Int. Conf. on Computing and Information Technology (ICCIT)*, 181–189. https://doi.org/10.1109/iccit63348.2025.10989392
12. Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible Zero Trust Architecture for the Cybersecurity of Industrial IoT Infrastructures. *Ad Hoc Netw., 156*, 103414. https://doi.org/10.1016/j.adhoc.2024.103414
13. Paul, B., & Rao, M. (2022). Zero-Trust Model for Smart Manufacturing Industry. *Appl. Sci*. https://doi.org/10.3390/app13010221
14. Li, K., Li, C., Yuan, X., Li, S.-F., Zou, S., Ahmed, S. S., Ni, W., Niyato, D., Jamalipour, A., Dressler, F., & Akan, O. B. (2025). Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things. *IEEE Internet Things J., 12*, 46269–46293. https://doi.org/10.1109/jiot.2025.3603957
15. Mahmud, R., Jin, J., Kua, J., Afrin, M., Mistry, S., & Krishna, A. (2025). Trusted Microservice Orchestration for Secure Edge Computing in Industrial Cyber-Physical Systems. *IEEE Netw., 39*, 70–78. https://doi.org/10.1109/mnet.2025.3541032
16. Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity Solutions for Industrial Internet of Things-Edge Computing Integration: Challenges, Threats, and Future Directions. *Sens., 25*. https://doi.org/10.3390/s25010213
17. Zanasi, C., Marasco, I., & Colajanni, M. (2025). Graph based threat detection system for a microsegmentation Zero Trust Architecture. In *2025 IEEE Conf. on Dependable, Autonomic and Secure Computing (DASC)*, 31–39. https://doi.org/10.1109/dasc68382.2025.00012
18. Goerke, N., Timmermann, D., & Baumgart, I. (2021). Who Controls Your Robot? An Evaluation of ROS Security Mechanisms. In *2021 7th Int. Conf. on Automation, Robotics and Applications (ICARA)*, 60–66. https://doi.org/10.1109/icara51699.2021.9376468
19. Xia, L., Gao, X., & Shi, W. (2025). Investigating Security Threats in Multi-Tenant ROS 2 Systems. *2025 IEEE International Conference on Robotics and Automation (ICRA)*, 16441–16448. https://doi.org/10.1109/icra55743.2025.11127490
20. Shaik, A. K., Mohammadi, A., & Malik, H. A. M. (2025). A Systematic Review of Sensor Vulnerabilities and Cyber-Physical Threats in Industrial Robotic Systems. *IET Cyber Phys. Syst. Theory Appl., 10*. https://doi.org/10.1049/cps2.70023
21. Bhardwaj, A., Bharany, S., Rehman, A., Tejani, G. G., & Hussen, S. (2025). Securing Cyber-Physical Robotic Systems for Enhanced Data Security and Real-Time Threat Mitigation. *EURASIP J. Inf. Secur., 2025*. https://doi.org/10.1186/s13635-025-00186-7
22. Holdbrook, R., Odeyomi, O., Yi, S., & Roy, K. (2024). Network-Based Intrusion Detection for Industrial and Robotics Systems: A Comprehensive Survey. *Electron*. https://doi.org/10.3390/electronics13224440
23. Burg, A., Chattopadhyay, A., & Lam, K.-Y. (2018). Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-Things. *Proceedings of the IEEE, 106*(1), 38–60. https://doi.org/10.1109/JPROC.2017.2780172
24. Guo, P., Kim, H., Virani, N., Xu, J., Zhu, M., & Liu, P. (2017). Exploiting Physical Dynamics to Detect Actuator and Sensor Attacks in Mobile Robots. *arXiv:1708.01834*. https://doi.org/10.48550/arXiv.1708.01834
25. Ge, Y., & Zhu, Q. (2024). GAZETA: GAme-Theoretic Zero-Trust Authentication for Defense Against Lateral Movement in 5G IoT Networks. *IEEE Trans. Inf. Forensics Secur., 19*, 540–554. https://doi.org/10.1109/TIFS.2023.3326975

26. Tushkanova, O., Levshun, D., Branitskiy, A., Fedorchenko, E., Novikova, E., & Kotenko, I. (2023). Detection of Cyberattacks and Anomalies in Cyber-Physical Systems: Approaches, Data Sources, Evaluation. *Algorithms, 16*, 85. https://doi.org/10.3390/a16020085
27. Moriano, P., Hespeler, S., Li, M., & Mahbub, M. (2024). Adaptive Anomaly Detection for Identifying Attacks in Cyber-Physical Systems: A Systematic Literature Review. *Artif. Intell. Rev., 58*. https://doi.org/10.1007/s10462-025-11292-w
28. Ji, R., Padha, D., Singh, Y., & Sharma, S. (2024). Review of Intrusion Detection System in Cyber-Physical System Based Networks: Characteristics, Industrial Protocols, Attacks, Data Sets and Challenges. *Trans. Emerg. Telecommun. Technol., 35*. https://doi.org/10.1002/ett.5029
29. Zhukabayeva, T., Ahmad, Z., Adamova, A., Karabayev, N., & Abdildayeva, A. (2025). An Edge-Computing-Based Integrated Framework for Network Traffic Analysis and Intrusion Detection to Enhance Cyber-Physical System Security in Industrial IoT. *Sens., 25*. https://doi.org/10.3390/s25082395
30. Manzoor, S., Yin, Y., Gao, Y., Hei, X., & Cheng, W. (2020). A Systematic Study of IEEE 802.11 DCF Network Optimization From Theory to Testbed. *IEEE Access, 8*, 154114–154132. https://doi.org/10.1109/access.2020.3018088
31. Venkateswaran, S. K., Tai, C.-L., Garnayak, R., Ben-Yehezkel, Y., Alpert, Y., & Sivakumar, R. (2024). IEEE 802.11ax Target Wake Time: Design and Performance Analysis in ns-3. In *2024 Workshop on ns-3*. https://doi.org/10.1145/3659111.3659115
32. Assasa, H., Grosheva, N., Ropitault, T., Blandino, S., Golmie, N., & Widmer, J. (2021). Implementation and Evaluation of a WLAN IEEE 802.11ay Model in Network Simulator ns-3. In *2021 Workshop on ns-3*. https://doi.org/10.1145/3460797.3460799
33. Hasan, S., Amundson, I., & Hardin, D. (2024). Zero-trust Design and Assurance Patterns for Cyber-Physical Systems. *J. Syst. Archit., 155*, 103261. https://doi.org/10.1016/j.sysarc.2024.103261
34. Botta, A., Rotbei, S., Zinno, S., & Ventre, G. (2023). Cyber Security of Robots: A Comprehensive Survey. *Intell. Syst. Appl., 18*, 200237. https://doi.org/10.1016/j.iswa.2023.200237
35. Campanile, L., Gribaudo, M., Iacono, M., Marulli, F., & Mastroianni, M. (2020). Computer Network Simulation with ns-3: A Systematic Literature Review. *Electron.* https://doi.org/10.3390/electronics9020272
36. Jeffrey, N., Tan, Q., & Villar, J. (2023). A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems. *Electron.* https://doi.org/10.3390/electronics12153283
37. Puccetti, T., Nardi, S., Cinquilli, C., Zoppi, T., & Ceccarelli, A. (2024). ROSPaCe: Intrusion Detection Dataset for a ROS2-Based Cyber-Physical System and IoT Networks. *Sci. Data, 11*. https://doi.org/10.1038/s41597-024-03311-2
38. Manzoor, S., Manzoor, M., Manzoor, H., Adan, D. E., & Kayani, M. A. (2023). Which Simulator to Choose for Next Generation Wireless Network Simulations? NS-3 or OMNeT++. *IEEC 2023*. https://doi.org/10.3390/engproc2023046036
39. Pakhomov, M. V. (2026). *ns3-wifi6-zero-trust-cprs: ns-3 Simulation Environment and Traces for the 20 STA / 1 AP IEEE 802.11ax Campaign* [Source code]. GitHub. https://github.com/m1fril/ns3-wifi6-zero-trust-cprs
40. Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sens., 24*. https://doi.org/10.3390/s24041328
41. Dattatreya, V., Adudhodla, M., Anupkant, S., Bande, V., Prasad, C. G. V. N., & Manellore, P. K. R. (2025). Edge-Forged Resilience: A Zero-Trust Security Architecture for Autonomous Cyber-Physical Systems in Industry 5.0. In *2025 6th Int. Conf. on Smart Electronics and Communication (ICOSEC)*, 1262–1268. https://doi.org/10.1109/icosec67334.2025.11459650
42. Kim, S., Park, K.-J., & Lu, C. (2022). A Survey on Network Security for Cyber-Physical Systems: From Threats to Resilient Design. *IEEE Commun. Surv. Tutor., 24*, 1534–1573. https://doi.org/10.1109/comst.2022.3187531
43. Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2021). Cybersecurity of Industrial Cyber-Physical Systems: A Review. *ACM Comput. Surv., 54*, 1–35. https://doi.org/10.1145/3510410
44. Nweke, L. O. (2021). A Survey of Specification-based Intrusion Detection Techniques for Cyber-Physical Systems. *Int. J. Adv. Comput. Sci. Appl., 12*. https://doi.org/10.14569/ijacsa.2021.0120506

45. Tan, S., Guerrero, J., Xie, P., Han, R., & Vasquez, J. (2020). Brief Survey on Attack Detection Methods for Cyber-Physical Systems. *IEEE Syst. J., 14*, 5329–5339. https://doi.org/10.1109/jsyst.2020.2991258
46. Xing, W., & Shen, J. (2024). Security Control of Cyber-Physical Systems under Cyber Attacks: A Survey. *Sens., 24*. https://doi.org/10.3390/s24123815
47. Ferrag, M., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl., 50*. https://doi.org/10.1016/j.jisa.2019.102419
48. Da Silva, E. F., Santoso, F., & Zheng, L. (2025). A Deep Learning-Based Intrusion Detection System for Safeguarding ROS 2-Powered Unmanned Ground Vehicles Against DoS Attacks. In *2025 Int. Joint Conf. on Neural Networks (IJCNN)*, 1–9. https://doi.org/10.1109/ijcnn64981.2025.11229203
49. Santoso, F., & Finn, A. (2023). A Data-Driven Cyber-Physical System Using Deep-Learning Convolutional Neural Networks: Study on False-Data Injection Attacks in an Unmanned Ground Vehicle Under Fault-Tolerant Conditions. *IEEE Trans. Syst. Man Cybern. Syst., 53*, 346–356. https://doi.org/10.1109/tsmc.2022.3170071
50. Fernandez, I., Neupane, S., Chakraborty, T., Mitra, S., Mittal, S., Pillai, N., Chen, J., & Rahimi, S. (2024). A Survey on Privacy Attacks Against Digital Twin Systems in AI-Robotics. In *2024 IEEE 10th Int. Conf. on Collaboration and Internet Computing (CIC)*, 70–79. https://doi.org/10.1109/cic62241.2024.00019
51. Alauthman, A., & Shraa, T. (2025). Performance Evaluation and Latency Optimization of Wi-Fi 7 in High-Density Wireless Environments. *Int. J. Electr. Electron. Eng. Telecommun.*. https://doi.org/10.18178/ijeetc.14.6.354-364
52. Ahrar, E. M., Wilhelmi, F., Galati-Giordano, L., Imputato, P., Menth, M., & Avallone, S. (2025). R-TWT in Wi-Fi 7 and Beyond: Enabling Bounded Latency, Energy Efficiency, and Reliability. In *2025 IEEE 30th Int. Conf. on Emerging Technologies and Factory Automation (ETFA)*, 1–8. https://doi.org/10.1109/etfa65518.2025.11205686
53. Alauthman, A., & Shraa, T. (2025). Deep Reinforcement Learning-Driven Dynamic Spectrum Access in Dense Wi-Fi Environments. *IEEE Access, 13*, 178663–178680. https://doi.org/10.1109/access.2025.3621489
54. Yang, S., Guo, J., & Rui, X. (2024). Formal Analysis and Detection for ROS2 Communication Security Vulnerability. *Electron*. https://doi.org/10.3390/electronics13091762
55. Soriano, E., Martin, F., & Guardiola, G. (2024). Implementing a Robot Intrusion Prevention System (RIPS) for ROS 2. *arXiv:2412.19272*. https://arxiv.org/abs/2412.19272
56. Santoso, F., & Finn, A. (2024). Trusted Operations of a Military Ground Robot in the Face of Man-in-the-Middle Cyberattacks Using Deep Learning Convolutional Neural Networks: Real-Time Experimental Outcomes. *IEEE Trans. Dependable Secur. Comput., 21*, 2273–2284. https://doi.org/10.1109/tdsc.2023.3302807
57. Zailan, N. S. B., Ong, L.-Y., & Lim, H. (2026). NAVBOT25: Dataset for ROS-Based Autonomous Robot Navigation. *Data Br., 65*. https://doi.org/10.1016/j.dib.2026.112617
58. Yaseen, Y. A., Almomani, I., & Al-Akhras, M. (2025). A Survey of Security Threats and Defense Mechanisms in ROS2-Based Internet of Drones Systems. In *2025 Int. Conf. on Computer and Applications (ICCA)*, 1–6. https://doi.org/10.1109/icca66035.2025.11430817
59. Papoutsakis, M., Hatzivasilis, G., Michalodimitrakis, E., Ioannidis, S., Michael, M. K., Savva, A. D., Nikolaou, P., Stokkou, E., & Bozdemir, G. (2025). SESAME: Automated Security Assessment of Robots and Modern Multi-Robot Systems. *Electron*. https://doi.org/10.3390/electronics14050923
60. Muriithi, G., Papari, B., Arsalan, A., Timilsina, L., Muriithi, A., Buraimoh, E., Khan, A., Ozkan, G., Edrington, C. S., & Papari, A. (2025). Zero Trust Architecture for Electric Transportation Systems: A Systematic Survey and Deep Learning Framework for Replay Attack Detection. *IEEE Open J. Veh. Technol., 6*, 2171–2194. https://doi.org/10.1109/ojvt.2025.3592041

Отримано редакцією журналу / Received: 17.02.26
Прорецензовано / Revised: 26.02.26
Схвалено до друку / Accepted: 24.09.26

(cc) BY-NC-SA

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.