https://doi.org/10.31891/2219-9365-2025-84-24
УДК 004.056:004.852:004.75

КОЗЕЛЬСЬКИЙ Олександр
Хмельницький національний університет
https://orcid.org/0009-0002-7157-6499
e-mail: oleksandr.kozelskiy@khmnu.edu.ua
САВЕНКО Богдан
Хмельницький національний університет
https://orcid.org/0000-0001-5647-9979
e-mail: savenko_bohdan@ukr.net

ВИЯВЛЕННЯ ЗЛОВМИСНИХ АТАК НА СЕНСОРИ ТА ПІДРОБКИ ТЕЛЕМЕТРІЇ В КІБЕРФІЗИЧНИХ СИСТЕМАХ НА ОСНОВІ МОДИФІКОВАНОГО ФІЛЬТРА КАЛМАНА

У роботі подано метод виявлення фальсифікацій та аномалій у сенсорних даних кіберфізичних систем на основі модифікованого фільтра Калмана з подієвим перемиканням режимів. Підхід орієнтований на протидію зловмисному програмному забезпеченню та комп'ютерним атакам, що реалізуються через підробку телеметрії, ін'єкції хибних даних і приховані сенсорні впливи в системах реального часу. Метод поєднує рекурсивне оцінювання стану з аналізом інновацій, що дає змогу відрізняти легітимні режимні зміни об'єкта керування від зловмисних втручань без паралельного виконання кількох моделей або фільтрів.

Запропонована подієво-адаптивна схема забезпечує оперативне перемикання динамічних моделей або придушення впливу підозрілих вимірювань, зберігаючи коректність оцінки стану за умов активних атак. Метод не потребує застосування машинного навчання чи ресурсоємних робастних алгоритмів, спираючись на компактні стохастичні моделі та лінійно-квадратичну обчислювальну складність, придатну для реалізації в ОС реального часу.

Експериментальні дослідження на платформі FreeRTOS підтвердили зниження кількості хибних спрацювань при частих режимних переходах, своєчасне виявлення атак на сенсори та стабільність оцінювання за мінімального навантаження на процесор, що забезпечує підвищення кіберстійкості й інформаційної безпеки вбудованих і кіберфізичних систем.

Ключові слова: кіберфізичні системи; атаки на сенсори; фальсифікація даних; виявлення аномалій; фільтр Калмана; адаптивне перемикання моделей; ОС реального часу.

KOZELSKYI Oleksandr, SAVENKO Bohdan
Khmelnytskyi National University

DETECTION OF MALICIOUS SENSOR ATTACKS AND TELEMETRY SPOOFING IN CYBER-PHYSICAL SYSTEMS BASED ON A MODIFIED KALMAN FILTER

This paper presents an event-adaptive method for detecting falsifications, anomalies, and malicious manipulations in sensor data of cyber-physical systems (CPS) operating in real time. The proposed approach is based on a modified Kalman filter with event-driven mode switching and is specifically aimed at counteracting cyber threats caused by malicious software and targeted computer attacks, including telemetry spoofing, false data injection, replay attacks, and stealthy sensor-level interference. Such attacks are particularly dangerous for embedded and control systems, as they may remain undetected while gradually degrading system performance or causing unsafe behavior.

The method integrates recursive state estimation with innovation-based statistical analysis, allowing the system to identify inconsistencies between predicted and measured signals. Unlike traditional multiple-model or bank-of-filters approaches, the proposed scheme enables reliable discrimination between legitimate changes in system operating modes and malicious disturbances without the need for parallel execution of several dynamic models. Event-triggered logic is used to adaptively switch system models or temporarily suppress suspicious measurements when abnormal innovations are detected, thereby maintaining estimation stability and accuracy under adversarial conditions.

A key advantage of the proposed solution is its low computational complexity and practical applicability. The method does not rely on machine learning algorithms, large training datasets, or computationally intensive robust estimation techniques. Instead, it employs compact stochastic models with linear–quadratic computational complexity, making it suitable for implementation in real-time operating systems and resource-constrained embedded platforms. This ensures predictable execution time and minimal impact on system latency.

Experimental validation was carried out on a FreeRTOS-based platform, simulating frequent mode transitions and various sensor attack scenarios. The results demonstrate a significant reduction in false alarms during normal operational changes, timely detection of malicious sensor behavior, and stable state estimation performance with minimal processor and memory overhead. Overall, the proposed approach enhances the cyber resilience, fault tolerance, and information security of embedded and cyber-physical systems used in safety- and mission-critical applications.

Keywords: cyber-physical systems; sensor attacks; data falsification; anomaly detection; Kalman filter; adaptive model switching; real-time operating systems

Стаття надійшла до редакції / Received 22.10.2025
Прийнята до друку / Accepted 22.11.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних кіберфізичних системах, що функціонують під керуванням операційних систем реального часу, зростання складності програмного забезпечення та щільності інтеграції компонентів ускладнює забезпечення достовірності сенсорних даних і стабільності процесів керування [1, 2]. Це є критичним у системах, де навіть короткочасне спотворення телеметрії може призвести до порушення алгоритмів керування або створити вікно вразливості для зловмисного програмного забезпечення та комп'ютерних атак [3]. Особливу небезпеку становлять атаки на сенсори та канали збору даних, зокрема ін'єкції хибних вимірювань і приховані фальсифікації сигналів, які можуть маскуватися під легітимні режимні зміни об'єкта [4].

Актуальність цієї проблеми посилюється необхідністю виявлення прихованих сенсорних атак, реалізованих зловмисним програмним забезпеченням, з урахуванням динаміки режимів функціонування кіберфізичних систем, що розглядалося раніше[5].

Традиційні методи контролю достовірності даних, що базуються на статичних порогах або фіксованих моделях, у таких умовах не забезпечують надійного розрізнення між нормальними динамічними переходами та зловмисними впливами [6]. Більш складні підходи, зокрема багатомодельні фільтри, робастні алгоритми або методи машинного навчання, часто потребують значних обчислювальних ресурсів і є малопридатними для реалізації в ресурсно обмежених середовищах ОС реального часу [7].

У зв'язку з цим актуальною є проблема розроблення методів виявлення атак на сенсори та підробки телеметрії, здатних працювати в реальному часі, адаптуватися до змін режимів функціонування та не вимагати суттєвого зростання обчислювальних витрат. Розв'язання цієї проблеми є необхідною умовою підвищення кіберстійкості та інформаційної безпеки сучасних вбудованих і кіберфізичних систем [8].

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

В останні роки спостерігається активний розвиток досліджень, присвячених виявленню атак на сенсори та фальсифікації телеметрії в кіберфізичних системах і системах реального часу [9]. Основну увагу приділено атакам типу false data injection, sensor spoofing та прихованим маніпуляціям вимірювальними сигналами, які реалізуються за допомогою зловмисного програмного забезпечення та спрямовані на порушення коректності процесів оцінювання стану об'єкта [10,11]. Показано, що такі атаки можуть не виходити за межі допустимих значень і залишатися непоміченими простими пороговими механізмами контролю, водночас призводячи до деградації керування або небезпечних режимів роботи [12].

Значна частина робіт базується на модельно-орієнтованих підходах, зокрема використанні фільтра Калмана та аналізі інновацій як індикатора аномальної поведінки сенсорів [13]. Класичні схеми дозволяють виявляти суттєві відхилення між прогнозом і вимірюванням, однак у системах з інтенсивними режимними змінами вони часто генерують хибні спрацювання, оскільки не розрізняють легітимні динамічні переходи та зловмисні впливи [14]. Для зменшення цього ефекту запропоновано адаптивні та багатомодельні фільтри, зокрема алгоритми з перемиканням моделей і робастні методи на основі $H\infty$-оцінювання, проте їх застосування супроводжується істотним зростанням обчислювальної складності та вимог до ресурсів[15].

Окремий напрям досліджень пов'язаний із застосуванням машинного навчання для виявлення аномалій у сенсорних даних [16]. Такі підходи демонструють високу ефективність у задачах класифікації та виявлення складних шаблонів атак, однак потребують значних навчальних вибірок, не гарантують детермінованих часових характеристик і є обмежено придатними для впровадження в ОС реального часу та ресурсно обмежені кіберфізичні платформи [17]. Крім того, більшість ML-методів орієнтована на статистичні відхилення та не враховує фізичну модель об'єкта керування [18].

Додатково показано, що аналіз багатовимірних взаємозв'язків між задачами, ресурсами та сенсорними даними дозволяє підвищити ефективність виявлення скоординованих атак у кіберфізичних системах [19].

Таким чином, аналіз сучасних публікацій свідчить про відсутність легковагового модельно-орієнтованого підходу, здатного в реальному часі надійно виявляти сенсорні атаки, спричинені зловмисним програмним забезпеченням, і водночас розрізняти їх від нормальних режимних змін. Це обґрунтовує актуальність розроблення подієво-адаптивних методів на основі фільтра Калмана, орієнтованих на підвищення кіберстійкості та інформаційної безпеки кіберфізичних систем.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Запропонований підхід спрямований на виявлення атак на сенсори та підробки телеметрії в кіберфізичних системах, що працюють під керуванням ОС реального часу, за рахунок модифікованого фільтра Калмана з подієвим аналізом інновацій і адаптивним перемиканням режимів. На відміну від порогових схем та системи виявлення вторгнень на осонві класичного філтра Калмана, де будь-яке суттєве відхилення трактують як аномалію, запропонований метод розділяє дві принципово різні причини нев'язки: (1) легітимний режимний перехід об'єкта керування та (2) зловмисний вплив (зловмисне ПЗ/комп'ютерна атака), що реалізує ін'єкцію хибних даних або спуфінг сенсорів.

Динаміка об’єкта керування описується дискретною лінійною моделлю зі змінною структурою:

$$X_{x+1} = A^{(\sigma k)}x_k + B^{(\sigma k)}u_k + w_k, \quad (1)$$

$$y_k = C^{(\sigma k)}x_k + v_k, \quad (2)$$

де x_k – вектор стану, u_k – керування, y_k – вектор істинних вимірювань, $w_k \sim N(0, Q)$, $v_k \sim N(0, R)$ – випадкові збурення процесу та вимірювань відповідно, які вважаються гаусовими з нульовим середнім та відомими коваріаціями.

Атаки на сенсори та телеметричні канали моделюються у вигляді адитивної ін’єкції зловмисного сигналу у вимірювальний канал:

$$z_k = y_k + Га_k, \quad (2)$$

де z_k – вимірювання, доступні алгоритму оцінювання, a_k – вектор зловмисного впливу, що відображає фальсифікацію телеметрії або спуфінг сенсорів, Γ – матриця вибору скомпрометованих каналів. Така модель є характерною для атак типу false data injection та прихованих маніпуляцій вимірювальними сигналами.

Для активного режиму $\hat{\sigma}_{k-1}$ виконується стандартний цикл прогнозу та уточнення фільтра Калмана. На етапі прогнозу обчислюються:

$$\hat{x}_{k|k-1} = A^{(\hat{\sigma}_{k-1})}\hat{x}_{k-1|k-1} + B^{(\hat{\sigma}_{k-1})}u_{k-1}, \quad (4)$$

де $\hat{x}_{k|k-1}$ – прогнозована оцінка вектора стану, $A^{(\hat{\sigma}_{k-1})}$ — матриця переходу станів для попереднього режиму, $\hat{x}_{k-1|k-1}$ – апостеріорна оцінка стану на попередньому кроці, $B^{(\hat{\sigma}_{k-1})}$ – матриця керування; u_{k-1} – вектор керуючих впливів. Далі визначається коваріація похибки прогнозу:

$$P_{k|k-1} = A^{(\hat{\sigma}_{k-1})}P_{k-1|k-1}(A^{(\hat{\sigma}_{k-1})})^T + Q, \quad (5)$$

де $P_{k|k-1}$ – прогнозована коваріаційна матриця похибки, $P_{k-1|k-1}$ – апостеріорна коваріація на попередньому кроці; Q — коваріаційна матриця процесного шуму. Далі визначається інновація:

$$r_k = z_k - C^{(\hat{\sigma}_{k-1})}\hat{x}_{k|k-1}, \quad (6)$$

де r_k – вектор інновації, z_k – вектор поточних вимірювань, $C^{(\hat{\sigma}_{k-1})}$ – матриця вимірювань для відповідного режиму. Коваріація інновації має вигляд:

$$S_k = C^{(\hat{\sigma}_{k-1})}P_{k|k-1}(C^{(\hat{\sigma}_{k-1})})^T + R, \quad (7)$$

де S_k – коваріаційна матриця інновації, R – коваріаційна матриця вимірювального шуму. Для оцінювання узгодженості між моделлю та вимірюваннями використовується нормована квадратична форма інновації:

$$T_k = r_k^T r_k^{-1} r_k, \quad (8)$$

де T_k – статистика узгодженості, що кількісно характеризує відхилення вимірювань від прогнозу. За відсутності атак та режимних змін величина T_k має X^2-розподіл, що дозволяє сформувати статистичний критерій виявлення аномалій. Якщо

$$T_k > \tau_{anom}, \quad (9)$$

де τ_{anom} – порогове значення, фіксується невідповідність, яка потребує додаткового аналізу.фіксується подія невідповідності, яка потребує додаткового аналізу.

На відміну від класичних підходів, запропонований метод не інтерпретує кожну таку подію як атаку. З метою розрізнення легітимної зміни режиму та зловмисного впливу виконується перевірка альтернативних динамічних моделей, допустимих для поточного стану системи. Для кожного можливого режиму j обчислюється квазі-інновація:

$$r_k^{(j)} = z_k - C^{(j)}\hat{x}_{k|k-1}^{(j)}, \quad (10)$$

де $r_k^{(j)}$ – квазі-інновація для режиму, $C^{(j)}$ – матриця вимірювань відповідного режиму, $\hat{x}_{k|k-1}^{(j)}$ – прогнозована оцінка стану для режиму j та відповідна статистика:

$$T_k^{(j)} = (r_k^{(j)})^T (S_k^{(j)})^{-1} r_k^{(j)}. \quad (11)$$

де $T_k^{(j)}$ – значення статистики узгодженості для режиму j, $r_k^{(j)}$ – вектор квазі-інновації для режиму j, $S_k^{(j)}$ – коваріаційна матриця квазі-інновації для режиму j, $(S_k^{(j)})^{-1}$ – обернена коваріаційна матриця квазі-інновації, $(\cdot)^T$ – операція транспонування, k – дискретний індекс часу. Режим з мінімальним значенням $T_k^{(j)}$ вважається найбільш узгодженим з отриманими вимірюваннями. Якщо для такого режиму виконується умова $T_k^{(j*)} \leq \tau_{mode}$, відхилення інтерпретується як легітимна режимна зміна, і здійснюється перемикання моделі з відповідною адаптацією коваріації. У протилежному випадку подія класифікується як атака на сенсори або фальсифікація телеметрії, зумовлена зловмисним програмним забезпеченням чи комп’ютерною атакою. Для запобігання впливу атакованих вимірювань на оцінку стану застосовується механізм зниження довіри до сенсорних даних, який реалізується шляхом збільшення коваріації вимірювального шуму або тимчасового переходу до прогнозного режиму. Це дозволяє зберегти стабільність оцінювання та уникнути різких помилкових керуючих впливів у системах реального часу. Запропонований алгоритм має обчислювальну складність, близьку до класичного фільтра Калмана, оскільки перевірка альтернативних моделей виконується

лише у подієвих точках. Така властивість робить метод придатним для реалізації в ресурсно обмежених кіберфізичних системах і забезпечує детерміновані часові характеристики. У контексті кібербезпеки підхід реалізує модельно-орієнтований контроль цілісності телеметрії, що дозволяє ефективно виявляти приховані сенсорні атаки та підвищувати кіберстійкість систем реального часу.

Підготовка прототипу

Для експериментальної перевірки запропонованого методу було розроблено програмний прототип, інтегрований у середовище операційної системи реального часу FreeRTOS. Як апаратну платформу використано мікроконтролер STM32F407G-DISC1 на базі ядра ARM Cortex-M4, що забезпечує детерміноване виконання задач і відповідає типовим умовам функціонування вбудованих кіберфізичних систем. Архітектура прототипу передбачає реалізацію модифікованого фільтра Калмана у вигляді окремого програмного модуля, який виконується як періодична задача з фіксованим пріоритетом. У процесі підготовки прототипу виконано модифікацію стандартного циклу обробки сенсорних даних шляхом додавання блоку подієвого аналізу інновацій і логіки адаптивного перемикання режимів. Сенсорні вимірювання надходять до модуля оцінювання через буферизований інтерфейс, що дозволяє імітувати як нормальні умови функціонування, так і сценарії атак підробки телеметрії. Для відтворення зловмисних впливів реалізовано програмний інжектор, який формує адитивні викривлення вимірювань відповідно до заданих профілів атак. Особливу увагу приділено оптимізації обчислювальних витрат і використанню статичної пам'яті, що відповідає вимогам ОС реального часу. Усі параметри моделей, коваріації шумів і порогові значення визначалися до запуску системи, що забезпечило детермінованість виконання алгоритму. Така організація прототипу дозволила провести коректну експериментальну оцінку ефективності методу в умовах, наближених до реальних сценаріїв експлуатації кіберфізичних систем.

Проведення експериментів і порівняння ефективності

Експериментальні дослідження було проведено з метою кількісної оцінки ефективності запропонованого методу виявлення атак на сенсори та підробки телеметрії в кіберфізичних системах, а також його порівняння з базовими модельно-орієнтованими підходами. Випробування виконувалися на програмно-апаратному прототипі під керуванням FreeRTOS на мікроконтролерній платформі ARM Cortex-M4 із тактовою частотою 168 МГц. Період дискретизації сенсорних даних становив 10 мс. У межах експериментів було реалізовано **легітимні режимні переходи** об'єкта керування і **атаки на сенсори**, що включали ін'єкцію хибних даних, поступову фальсифікацію телеметрії та приховані спотворення вимірювань.

Для порівняння було використано такі фільтри:

– класичний фільтр Калмана з пороговим аналізом інновацій;

– адаптивний фільтр Калмана зі зміною коваріації вимірювального шуму;

– запропонований подієво-адаптивний метод, комбінований фільтр Калмана;

– $H\infty$ фільтр;

– ETKF (ансамблевий фільтрів Калмана).

Під час запуску експерименту кожен цикл навігаційної задачі формував повний вектор оцінок, проте в журнал записувалися лише кожні соті результати. Таке зменшення частоти логування не впливає на репрезентативність, стрибки висоти на п'ять метрів і разові імпульсні атаки ±300–500 м залишаються добре помітними навіть за дискретизації 1 Гц, а при цьому розмір файлів і візуальна читабельність кривих значно поліпшуються. Висока внутрішня частота забезпечує коректну роботу фільтрів у реальному часі, тоді як раз на секунду збережених даних достатньо для цілей аналізу й публікації. На рис. 2 показано графічно, а на рис.3 – таблично типовий приклад фільтрів у ситуації, коли на 20-й секунді і на 38-й секунді відбувається заплановане зниження висоти БПЛА, законний стрибок рівня (перехід на новий режим). Після переходів на новий режим фільтри кожний по своєму підлаштовуються до нового рівня – повільно виходячи на рівень, накопичуючи похибку, криві класичного КФ і ККФ рухаються однаково

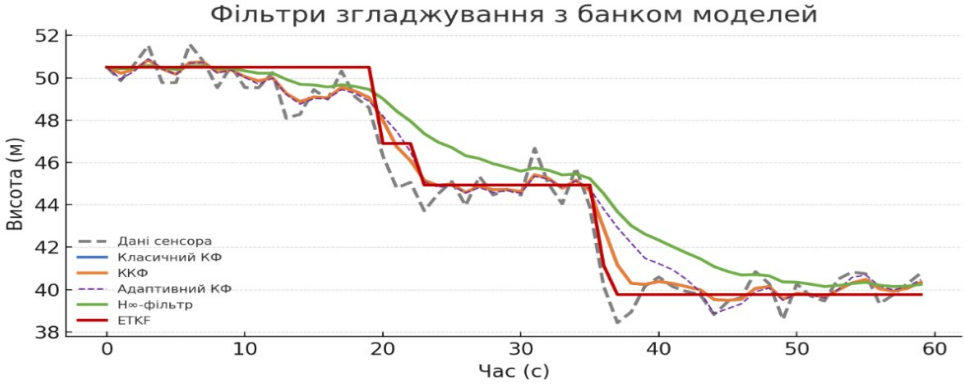

Рис. 1: графік порівняння поведінки фільтрів при режимних змінах

Таблиця. 1

Порівняння поведінки фільтрів при режимних змінах

Метод	**Хибні спрацювання (за 1 хв)**	**Середньо-квадратичне Відхилення(м)**	**Навантаження CPU (%)**	**Опис навантаження**
Класичний фільтр Калмана	9	0,75	~3	Постійне оновлення, але формули прості.
адаптивний фільтр Калмана	0	1,04	~6	Постійно змінює Змінює Q/R, постійні обчислення навантажують CPU
Комбінований фільтр Калмана (пропонований)	0	0,75	~3.5	Змінює Q/R, оцінює нев'язку, перемикає моделі — трохи складніше за простий ФК
H∞ фільтр	9	1,46	~8	Мінімакс-оптимізація, складна матрична алгебра кожного кроку.
ETKF	10	0,55	~2	оновлення лише при перевищенні порогу, економія.

Для кількісного порівняння ефективності методів оцінювання стану було використано інтегральний показник, який узагальнює три ключові критерії: точність оцінювання, обчислювальне навантаження та частоту хибних спрацювань. Перед обчисленням інтегрального показника всі часткові критерії було нормалізовано, що дозволило забезпечити їх порівнюваність. За умови рівнозначної ваги критеріїв визначено інтегральну оцінку ефективності кожного з розглянутих методів.

Для комбінованого фільтра Калмана середньоквадратична похибка: $\boldsymbol{E}_{\text{СКП}} = \frac{\boldsymbol{X_{max}}}{\boldsymbol{X}_{\text{ккф}}} = \frac{1.46}{0.75}$=1.9466666666666668. Середнє значення процесора (%): $\boldsymbol{E_{CPU}} = \frac{\boldsymbol{X_{max}}}{\boldsymbol{X}_{\text{ккф}}} = \frac{8}{3.5}$= 2.2857142857142856. Хибні спрацювання (%): $\boldsymbol{E_{Er}} = \frac{\boldsymbol{X_{max}}}{\boldsymbol{X}_{\text{ккф}}} = \frac{0}{10}$ - ділення на нуль неможливе, тоді робим максимальне значення = 10 Інтегральний показник: $I = \text{w}_{CPU}E_{CPU} + \text{w}_{\text{СКП}}E_{\text{СКП}} + \text{w}_{\boldsymbol{Er}}E_{\boldsymbol{Er}}$, де $\text{w}_{CPU} + \text{w}_{\text{СКП}} + \text{w}_{\boldsymbol{Er}} = 1$. Для рівнозначної важливості беремо $\text{w}_{CPU} = \text{w}_{\text{СКП}} = \text{w}_{\boldsymbol{Er}} = \frac{1}{3}$ .I $= \frac{1}{3}(1.9466666666666667 + 2.2857142857142856 + 10) = 4.744126984126984 \approx 4.74$.

Для класичного фільтра Калмана середньоквадратична похибка: $E_{\text{СКП}} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{1.46}{0.75}$=1.9466666666666667. Середнє значення процесора (%): $E_{CPU} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{8}{3}$ = 2.6666666666666667. Хибні спрацювання (%): $E_{Er} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{9}{10}$ = 1.1111111111111112. Інтегральний показник: $I = \text{w}_{CPU}E_{CPU} + \text{w}_{\text{СКП}}E_{\text{СКП}} + \text{w}_{Er}E_{Er}$, де $\text{w}_{CPU} + \text{w}_{\text{СКП}} + \text{w}_{Er} = 1$. Для рівнозначної важливості беремо $\text{w}_{CPU} = \text{w}_{\text{СКП}} = \text{w}_{Er} = \frac{1}{3}$. $I = \frac{1}{3}(E_{CPU} + E_{\text{СКП}} + E_{Er}) = \frac{1}{3}(1.9466666666666676 + 2.6666666666666667 + 1.1111111111111111) \approx 1{,}91$

Для адаптивного фільтра Калмана середньоквадратична похибка: $E_{\text{СКП}} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{1.46}{1.04}$ = 1.4038461538461537. Середнє значення процесора (%): $E_{CPU} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{8}{6}$ = 1.3333333333333333. Хибні спрацювання (%): $E_{Er} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{0}{10}$ - ділення на нуль неможливе, тоді робим максимальне значення = 10. Інтегральний показник: $I = \text{w}_{CPU}E_{CPU} + \text{w}_{\text{СКП}}E_{\text{СКП}} + \text{w}_{Er}E_{Er}$, де $\text{w}_{CPU} + \text{w}_{\text{СКП}} + \text{w}_{Er} = 1$. Для рівнозначної важливості беремо $\text{w}_{CPU} = \text{w}_{\text{СКП}} = \text{w}_{Er} = \frac{1}{3}$. $I = \frac{1}{3}(E_{CPU} + E_{\text{СКП}} + E_{Er}) = \frac{1}{3}(1.4038461538461537 + 1.3333333333333333 + 10) = 4.245726495726496 \approx 4.26$

Для H∞ фільтра середньоквадратична похибка: $E_{\text{СКП}} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{1.46}{1.46}$ = 1. Середнє значення процесора (%): $E_{CPU} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{8}{8}$ = 1. Хибні спрацювання (%): $E_{Er} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{10}{9}$ = 1.1111111111111112. Інтегральний показник: $I = \text{w}_{CPU}E_{CPU} + \text{w}_{\text{СКП}}E_{\text{СКП}} + \text{w}_{Er}E_{Er}$, де $\text{w}_{CPU} + \text{w}_{\text{СКП}} + \text{w}_{Er} = 1$. Для рівнозначної важливості беремо $\text{w}_{CPU} = \text{w}_{\text{СКП}} = \text{w}_{Er} = \frac{1}{3}$. $I = \frac{1}{3}(E_{CPU} + E_{\text{СКП}} + E_{Er}) = \frac{1}{3}(1 + 1 + 1.1111111111111112) = 3.1111111111111112 \approx 3.11$

Для ETKF фільтра середньоквадратична похибка: $E_{\text{СКП}} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{1.46}{0.55}$= 2.6545454545454543. Середнє значення процесора (%): $E_{CPU} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{8}{2}$ = 4. Хибні спрацювання (%): $E_{Er} = \frac{X_{max}}{X_{\text{ккф}}} = \frac{10}{10}$ = 1. Інтегральний показник: $I = \text{w}_{CPU}E_{CPU} + \text{w}_{\text{СКП}}E_{\text{СКП}} + \text{w}_{Er}E_{Er}$, де $\text{w}_{CPU} + \text{w}_{\text{СКП}} + \text{w}_{Er} = 1$. Для рівнозначної важливості беремо $\text{w}_{CPU} = \text{w}_{\text{СКП}} = \text{w}_{Er} = \frac{1}{3}$. $I = \frac{1}{3}(E_{CPU} + E_{\text{СКП}} + E_{Er}) = \frac{1}{3}(4 + 2.6545454545454543 + 1) = 2.5515151515151513 \approx 2.55$

Отже найбільший інтегральний показник ефективності у комбінованого фільтра Калмана $I \approx 4.74$. Це значення свідчить про збалансоване поєднання високої стійкості до аномалій і фальсифікацій телеметрії, прийнятної точності оцінювання стану та помірних обчислювальних витрат. Отриманий результат підтверджує, що метод є придатним для використання в операційних системах реального часу при роботі з потенційно зкомпрометованими цифровими сигналами. Для порівняння, класичний фільтр Калмана продемонстрував інтегральну оцінку ефективності на рівні $I \approx 1{,}91$, що пояснюється низькою стійкістю до прихованих атак і значною кількістю хибних спрацювань у разі режимних переходів. Адаптивний фільтр Калмана показав вищий рівень ефективності ($I \approx 4{,}26$), однак поступався запропонованому методу за показниками стійкості до фальсифікацій телеметрії. Для робастного $H\infty$-фільтра інтегральний показник становив $I \approx 3{,}11$, що відображає підвищену стійкість до збурень за рахунок збільшених обчислювальних витрат і зниження точності оцінювання. Метод розширеного ансамблевого фільтра Калмана (ETKF) забезпечив значення $I \approx 2{,}55$, демонструючи кращу адаптивність порівняно з класичним фільтром, але недостатню ефективність в умовах цілеспрямованих сенсорних атак. Підсумкове порівняння результатів показало, що запропонований комбінований фільтр Калмана має найвище значення інтегрального показника серед усіх розглянутих методів. Це підтверджує його перевагу з точки зору досягнення оптимального балансу між точністю оцінювання, стійкістю до аномалій і фальсифікацій телеметрії та обмеженим навантаженням на процесор. Отримані результати обґрунтовують доцільність застосування запропонованого підходу в операційних системах реального часу та кіберфізичних системах з підвищеними вимогами до надійності та обмеженими обчислювальними ресурсами.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У сукупності запропонований підхід реалізує програмний механізм модельно-орієнтованого захисту кіберфізичних систем від атак на сенсорні дані, що здійснюються зловмисним програмним забезпеченням або через компрометацію каналів зв'язку. На відміну від класичних систем виявлення вторгнень, орієнтованих на мережеві сигнатури або статистичні відхилення, метод базується на аналізі фізично обґрунтованих моделей системи, що підвищує його ефективність проти цілеспрямованих і малопомітних комп'ютерних атак у системах реального часу.

У статті розглянуто проблему виявлення атак на сенсори та підробки телеметрії в кіберфізичних системах, що функціонують під керуванням операційних систем реального часу, в умовах дії зловмисного програмного забезпечення та цілеспрямованих комп'ютерних атак. Запропоновано модельно-орієнтований метод на основі модифікованого фільтра Калмана з подієво-адаптивним аналізом інновацій і перемиканням режимів, який дозволяє розрізняти легітимні динамічні зміни стану об'єкта керування та зловмисні впливи на сенсорні дані. На відміну від класичних підходів, запропонований метод не інтерпретує кожне відхилення вимірювань як атаку, що суттєво знижує кількість хибних спрацювань у системах з інтенсивними режимними переходами. Використання подієвої логіки та перевірки альтернативних моделей забезпечує своєчасне виявлення прихованих сенсорних атак і фальсифікацій телеметрії без застосування ресурсоємних алгоритмів машинного навчання або паралельних багатомодельних схем. Експериментальні дослідження на прототипі з використанням FreeRTOS підтвердили ефективність методу в умовах реального часу, збереження стабільності оцінювання стану та низьке додаткове навантаження на обчислювальні ресурси. Інтегральний показник ефективності найбільший у комбінованого фільтра Калмана $I \approx 4.74$. Отримані результати свідчать про доцільність застосування запропонованого підходу як програмного засобу підвищення кіберстійкості та інформаційної безпеки вбудованих і кіберфізичних систем. Подальші дослідження доцільно спрямувати на розширення класу моделей атак і інтеграцію методу з комплексними системами виявлення вторгнень у реальному часі.

Література

1. Xue, K. (2025). Securing Power Cyber-Physical Systems Against False Data Injection Attacks: Trends, Techniques, and Future Directions. Preprints. https://doi.org/10.20944/preprints202504.1907.v1.

2. Xing, W., & Shen, J. (2024). Security Control of Cyber–Physical Systems under Cyber Attacks: A Survey. Sensors, 24(12), 3815. https://doi.org/10.3390/s24123815.

3. Liu, W. (2025). Review of False Data Injection Attacks in Power CPS: Challenges, Detection, and Resilience Strategies. Preprints.org. https://www.preprints.org/manuscript/202505.0166/v1/download.

4. Das, S., Ghosh, A., & Chatterjee, D. (2025). Algorithmic detection of false data injection attacks in cyber-physical systems. arXiv. https://arxiv.org/abs/2511.18588.

5. КОЗЕЛЬСЬКИЙ, О., & САВЕНКО, О. (2025). ПРОАКТИВНИЙ МЕХАНІЗМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОС РЕАЛЬНОГО ЧАСУ З ВИКОРИСТАННЯМ ГІБРИДНОГО СТОРОЖОВОГО ТАЙМЕРА. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 459–466. https://doi.org/10.31891/2219-9365-2025-83-57.

6. Irfan, M. (2024). A survey on detection and localisation of false data injection attacks in smart grids. IET Cyber-Physical Systems: Theory & Applications. https://doi.org/10.1049/cps2.12093.

7. Quincozes, V. E., et al. (2025). Intrusion detection datasets for cyber-physical systems: Taxonomy, challenges and opportunities. Journal of Cybersecurity Research. http://doi.org/10.2139/ssrn.5247519.

8. Bo, X. (2025). A Review of Detection, Evolution, and Data Reconstruction Strategies for False Data Injection Attacks in Power Cyber-Physical Systems. Preprints. https://doi.org/10.20944/preprints202501.1098.v1.

9. Abshari, D., & Sridhar, M. (2025). A survey of anomaly detection in cyber-physical systems. arXiv. https://arxiv.org/pdf/2502.13256v1.

10. Shaharier Kabir, Nasif Hannan, Abu Shufian, Md Saniat Rahman Zishan, Proactive detection of cyber-physical grid attacks: A pre-attack phase identification and analysis using anomaly-based machine learning models, Array, Volume 27, 2025, 100441, ISSN 2590-0056, https://doi.org/10.1016/j.array.2025.100441.

11. Eslami, A., & Khorasani, K. (2025). Zero dynamics attack detection and isolation in cyber-physical systems with event-triggered communication. arXiv. https://arxiv.org/abs/2505.06070.

12. Fu, W., & Lu, W. (2024). Temporal false data injection attack and detection on cyber-physical systems. IET Cyber-Physical Systems: Theory & Applications. https://doi.org/10.1049/stg2.12141.

13. Moriano, P., Hespeler, S. C., Li, M., & Mahbub, M. (2025). Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review. Artificial Intelligence Review. https://doi.org/10.48550/arXiv.2411.14278.

14. Abbas Baba, S., & Chattopadhyay, A. (2024). Quickest detection of false data injection attack in distributed process tracking. arXiv. https://arxiv.org/abs/2402.09743.

15. Liu, X., & Chang, P. (2025). Adaptive FDI attack detection in nonlinear cyber-physical systems with uncertain parameters. International Journal of Robust and Nonlinear Control. https://doi.org/10.1002/rnc.70160.

16. Abrar M. Alajlan, Marwah M. Almasri, Autonomous Cyber-Physical System for Anomaly Detection and Attack Prevention Using Transformer-Based Attention Generative Adversarial Residual Network, Computers, Materials and Continua, Volume 85, Issue 3, 2025, Pages 5237-5262, ISSN 1546-2218, https://doi.org/10.32604/cmc.2025.066736.

17. Schummer, P., del Rio, A., Serrano, J., Jimenez, D., Sánchez, G., & Llorente, Á. (2024). Machine learning-based network anomaly detection: Design, implementation, and evaluation. AI, 5(4), 2967–2983. https://doi.org/10.3390/ai5040143.

18. Liu, Z., & Huang, D. (2025). False data injection attacks on data-driven algorithms in cyber-physical systems: Black-box methods and detection challenges. Engineering. https://doi.org/10.1016/j.eng.2024.11.025.

19. КОЗЕЛЬСЬКИЙ, О. (2025). МЕТОД ТЕНЗОРНОЇ ДЕКОМПОЗИЦІЇ ДЛЯ АДАПТИВНОГО РОЗПОДІЛУ РЕСУРСІВ У СИСТЕМАХ РЕАЛЬНОГО ЧАСУ. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, 82(2), 426–433. https://doi.org/10.31891/2219-9365-2025-82-61

References

1. Xue, K. (2025). Securing Power Cyber-Physical Systems Against False Data Injection Attacks: Trends, Techniques, and Future Directions. Preprints. https://doi.org/10.20944/preprints202504.1907.v1.

2. Xing, W., & Shen, J. (2024). Security Control of Cyber–Physical Systems under Cyber Attacks: A Survey. Sensors, 24(12), 3815. https://doi.org/10.3390/s24123815.

3. Liu, W. (2025). Review of False Data Injection Attacks in Power CPS: Challenges, Detection, and Resilience Strategies. Preprints.org. https://www.preprints.org/manuscript/202505.0166/v1/download.

4. Das, S., Ghosh, A., & Chatterjee, D. (2025). Algorithmic detection of false data injection attacks in cyber-physical systems. arXiv. https://arxiv.org/abs/2511.18588.

5. Kozelskyi, O., & Savenko, O. (2025). Proactive information security mechanism in real-time operating systems using a hybrid watchdog timer. *Measuring and Computing Devices in Technological Processes*, *(3)*, 459–466. https://doi.org/10.31891/2219-9365-2025-83-57.

6. Irfan, M. (2024). A survey on detection and localisation of false data injection attacks in smart grids. IET Cyber-Physical Systems: Theory & Applications. https://doi.org/10.1049/cps2.12093.

7. Quincozes, V. E., et al. (2025). Intrusion detection datasets for cyber-physical systems: Taxonomy, challenges and opportunities. Journal of Cybersecurity Research. http://doi.org/10.2139/ssrn.5247519.

8. Bo, X. (2025). A Review of Detection, Evolution, and Data Reconstruction Strategies for False Data Injection Attacks in Power Cyber-Physical Systems. Preprints. https://doi.org/10.20944/preprints202501.1098.v1.

9. Abshari, D., & Sridhar, M. (2025). A survey of anomaly detection in cyber-physical systems. arXiv. https://arxiv.org/pdf/2502.13256v1.

10. Shaharier Kabir, Nasif Hannan, Abu Shufian, Md Saniat Rahman Zishan, Proactive detection of cyber-physical grid attacks: A pre-attack phase identification and analysis using anomaly-based machine learning models, Array, Volume 27, 2025, 100441, ISSN 2590-0056, https://doi.org/10.1016/j.array.2025.100441.

11. Eslami, A., & Khorasani, K. (2025). Zero dynamics attack detection and isolation in cyber-physical systems with event-triggered communication. arXiv. https://arxiv.org/abs/2505.06070.

12. Fu, W., & Lu, W. (2024). Temporal false data injection attack and detection on cyber-physical systems. IET Cyber-Physical Systems: Theory & Applications. https://doi.org/10.1049/stg2.12141.

13. Moriano, P., Hespeler, S. C., Li, M., & Mahbub, M. (2025). Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review. Artificial Intelligence Review. https://doi.org/10.48550/arXiv.2411.14278.

14. Abbas Baba, S., & Chattopadhyay, A. (2024). Quickest detection of false data injection attack in distributed process tracking. arXiv. https://arxiv.org/abs/2402.09743.

15. Liu, X., & Chang, P. (2025). Adaptive FDI attack detection in nonlinear cyber-physical systems with uncertain parameters. International Journal of Robust and Nonlinear Control. https://doi.org/10.1002/rnc.70160.

16. Abrar M. Alajlan, Marwah M. Almasri, Autonomous Cyber-Physical System for Anomaly Detection and Attack Prevention Using Transformer-Based Attention Generative Adversarial Residual Network, Computers, Materials and Continua, Volume 85, Issue 3, 2025, Pages 5237-5262, ISSN 1546-2218, https://doi.org/10.32604/cmc.2025.066736.

17. Schummer, P., del Rio, A., Serrano, J., Jimenez, D., Sánchez, G., & Llorente, Á. (2024). Machine learning-based network anomaly detection: Design, implementation, and evaluation. AI, 5(4), 2967–2983. https://doi.org/10.3390/ai5040143.

18. Liu, Z., & Huang, D. (2025). False data injection attacks on data-driven algorithms in cyber-physical systems: Black-box methods and detection challenges. Engineering. https://doi.org/10.1016/j.eng.2024.11.025.

19. Kozelskyi, O. (2025). Tensor decomposition method for adaptive resource allocation in real-time systems. *Measuring and Computing Devices in Technological Processes*, *82*(2), 426–433. https://doi.org/10.31891/2219-9365-2025-82-61