УДК 004.77:004.62]:502/504 DOI: 10.31673/2412-4338.2026.029117

Гавор Артур Станіславович
старший викладач кафедри Технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID 0009-0002-9705-1666
a.havor@duikt.edu.ua

Герцюк Микола Модестович
доктор філософії, доцент кафедри Технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID 0000-0003-2946-9673
m.gertsiuk@duikt.edu.ua

АЛГОРИТМ СТІЙКОЇ АГРЕГАЦІЇ ДАНИХ У РОЗПОДІЛЕНИХ МЕРЕЖАХ МОНІТОРИНГУ ДОВКІЛЛЯ НА ОСНОВІ МЕТОДУ ДОВІРЧОГО ЗВАЖУВАННЯ

Анотація. *Стаття присвячена розробці та комплексному аналізу алгоритму стійкої агрегації даних для децентралізованих IoT-мереж екологічного моніторингу. Збір та обробка багатовимірної інформації у таких масштабних розподілених мережах суттєво ускладнюється наявністю стохастичного шуму середовища та візантійських вузлів – зловмисних або апаратно несправних датчиків, які систематично або хаотично генерують аномальні показники. Метою цього дослідження є створення та емпірична оцінка математично обґрунтованого алгоритму, здатного підтримувати гомеостаз системи й гарантувати високу точність обчислень без використання єдиного центрального координатора, що усуває проблему єдиної точки відмови (Single Point of Failure). Дослідження охоплює глибокий аналіз вразливостей класичного алгоритму Mean-gossip і детальне обґрунтування запропонованого гібридного методу TWTMOM (Trust-Weighted Trimmed Median-of-Means). Цей підхід інноваційно поєднує багатовимірне статистичне відсікання аномалій за допомогою відстані Махаланобіса, агрегацію на основі медіани середніх (Median-of-Means) та адаптивну марковскую систему репутаційного зважування вузлів. Для практичної оцінки ефективності та масштабованості алгоритму було розроблено конкурентну програмну симуляцію мовою Golang, яка високоточно імітує роботу мережі з 1000 датчиків в умовах high-load. Порівняльний аналіз проводиться за критеріями стійкості до масованого отруєння даних та прихованого градієнтного дрейфу stealth-атак із вимірюванням рівня середньоквадратичної помилки (RMSE). Виявлено, що класичний метод має критичну вразливість вже за наявності 5-10% скомпрометованих вузлів. Натомість, розроблений алгоритм TWTMOM продемонстрував безпрецедентну надійність, зберігаючи мінімальний рівень математичної похилки навіть за умови одночасного деструктивного впливу до 40% аномальних датчиків у мережі. Результати дослідження підтверджують, що алгоритм TWTMOM є оптимальним і масштабованим рішенням для впровадження у критично важливих децентралізованих системах екологічного та індустріального моніторингу, де пріоритетами є беззаперечна кібербезпека, візантійська відмовостійкість та цілісність даних.*

Ключові слова: *IoT, моніторинг довкілля, агрегація даних, візантійська відмовостійкість, Median-of-Means, довірче зважування, кібербезпека.*

Artur S. Havor
Senior Lecturer of the Department Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID 0000-0003-2946-9673
a.havor@duikt.edu.ua

Mykola M. Gertsiuk
Ph.D., Associate Professor of the Department Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID 0000-0003-2946-9673
m.gertsiuk@duikt.edu.ua

ALGORITHM FOR STABLE DATA AGGREGATION IN DISTRIBUTED ENVIRONMENTAL MONITORING NETWORKS BASED ON THE TRUSTED WEIGHTING METHOD

Abstract. *This paper focuses on the development and comprehensive analysis of a stable data aggregation algorithm for decentralized IoT networks used in environmental monitoring. The collection and processing of multidimensional information in such large-scale distributed networks are significantly complicated by the presence of stochastic environmental noise and Byzantine nodes—malicious or hardware-faulty sensors that systematically or chaotically generate anomalous readings. The primary aim of this study is to create and empirically evaluate a mathematically grounded algorithm capable of maintaining system homeostasis and ensuring high computational accuracy without relying on a single central coordinator, thereby eliminating the Single Point of Failure problem. The research encompasses an in-depth vulnerability analysis of the classic Mean-gossip algorithm and a detailed justification of the proposed hybrid method, TWTMOM (Trust-Weighted Trimmed Median-of-Means). This approach innovatively combines multidimensional statistical anomaly trimming using the Mahalanobis distance, aggregation based on the Median-of-Means method,*

and an adaptive Markovian node reputation weighting system. To practically evaluate the algorithm's efficiency and scalability, a highly concurrent software simulation was developed using the Golang programming language, which accurately mimics the operation of a high-load network consisting of 1000 sensors. A comparative analysis was conducted based on the criteria of resilience to massive data poisoning and stealth gradient drift attacks, measuring the Root Mean Square Error (RMSE). The findings revealed that the classic method exhibits a critical vulnerability even with 5-10% compromised nodes. In stark contrast, the newly developed TWTMOM algorithm demonstrated unprecedented reliability, maintaining a minimal level of mathematical error even under the simultaneous destructive influence of up to 40% anomalous sensors in the network. The study results firmly confirm that the TWTMOM algorithm is an optimal and highly scalable solution for implementation in mission-critical decentralized environmental and industrial monitoring systems, where unquestionable cybersecurity, Byzantine fault tolerance, and data integrity are top priorities.

***Keywords**: IoT, environmental monitoring, data aggregation, Byzantine fault tolerance, Median-of-Means, trust weighting, cybersecurity.*

1. Вступ

У сучасному світі інформаційних технологій розподілені мережі Інтернету речей (IoT) є основою для систем екологічного моніторингу. Вони забезпечують безперервний збір багатовимірних даних на великих територіях. Традиційні централізовані системи агрегації мають єдину точку відмови Single Point of Failure та є вразливими до перевантажень [1]. Водночас децентралізовані протоколи, засновані на обміні даними між сусідніми вузлами Gossip-протоколи, вирішують цю проблему, забезпечуючи горизонтальне масштабування.

Однак застосування класичних децентралізованих алгоритмів ускладнюється проблемою достовірності даних. Сенсори можуть виходити з ладу або ставати жертвами кібератак (Byzantine faults), навмисно транслюючи хибні показники атака отруєння даних [2]. Відмінності в підходах до фільтрації такого "шуму" суттєво впливають на точність усієї системи.

Одним із ключових аспектів цього дослідження є забезпечення стійкості процесу агрегації даних, що передбачає здатність мережі підтримувати високу точність обчислень після виникнення несправностей чи спроб компрометації, а також оптимізувати децентралізований консенсус без використання уразливого центрального координатора.

2. Постановка проблеми

Класичні децентралізовані протоколи агрегації мають критичну вразливість до візантійських відмов, оскільки єдиний скомпрометований вузол здатний екстремально змістити загальний консенсус мережі. Проблема ускладнюється багатовимірністю екологічної телеметрії, де просте усереднення або сортування не дозволяє ідентифікувати аномальні вектори стану. Таким чином, існує нагальна необхідність створення децентралізованого математичного апарату, здатного самостійно адаптуватися до рівня загрози та ізолювати шкідливий вплив без втручання оператора.

3. Аналіз останніх досліджень і публікацій

Еволюція методів агрегації даних вказує на поступовий перехід від наївних алгоритмів до складних візантійсько-відмовостійких (BFT) протоколів. Базові підходи, такі як просте усереднення (Simple Mean), мають нульову стійкість до отруєння даних, оскільки єдиний екстремальний викид здатний критично спотворити глобальний стан мережі. Як перша лінія захисту традиційно застосовується координатна медіана (Coordinate Median), що забезпечує стійкість до поодиноких викидів, проте втрачає ефективність при багатовимірних прихованих атаках через відсутність історичної пам'яті.

Для вирішення проблеми масованих візантійських збоїв сучасні дослідження розвиваються у двох паралельних напрямках, робастна статистика та репутаційні системи [3].

З боку робастної статистики широко застосовуються методи відсікання. Класичний алгоритм Alpha-Trimmed Mean [4] ефективно ізолює заздалегідь задану частку аномалій, проте зазнає математичного колапсу, коли кількість зловмисників перевищує поріг. Більш досконалі фреймворки, такі як GRANITE [5], доводять зниження впливу візантійських вузлів завдяки адаптивним правилам відсікання. У контексті захисту багатовимірних векторів стандартом де-факто став алгоритм Krum [6] – передовий BFT-протокол просторової кластеризації. Проте Krum має критичні недоліки для децентралізованих мереж [7]: квадратичну обчислювальну складність $O(N^2)$ та втрату переваг дисперсійного згладжування природного шуму, оскільки алгоритм обирає значення лише одного конкретного вузла, повністю відкидаючи вибірку інших. Водночас дослідження методу Median-of-Means (MoM) [8] підтверджують його високу здатність мінімізувати дисперсію за наявності екстремальних викидів без втрати корисних даних.

З іншого боку, репутаційні підходи (Trust-weighting), такі як RPV [9] або системи оцінки на базі RADAR [10], використовують історичну надійність вузлів для ізоляції зловмисників. Дослідження у сфері управління довірою в децентралізованих IoT-системах [11] демонструють високу емпіричну стійкість навіть за наявності значної частки скомпрометованих сенсорів.

Аналіз літератури виявляє наукову прогалину. Існуючі стійкі методи (Trimmed Mean, Krum) або потребують ручного налаштування статичних порогів, або є занадто обчислювально важкими для IoT. Наразі відсутня інтеграція методу Median-of-Means (MoM) [8] у децентралізовані середовища в комбінації з

багатовимірним просторовим відсіканням [12] та марковськими репутаційними оцінками [11], що працюють на Edge-рівні [7], що й зумовлює необхідність розробки гібридного алгоритму.

4. Мета і задачі дослідження

Метою дослідження є розробка та математичне обґрунтування алгоритму стійкої агрегації даних для децентралізованих IoT-мереж екологічного моніторингу, який дозволяє підтримувати їхню відмовостійкість та гомеостаз навіть за умов впливу дестабілізуючих факторів, оптимізуючи баланс між кібербезпекою, точністю децентралізованого консенсусу та обчислювальною ефективністю. Це включає в себе аналіз вразливостей класичних методів агрегації, створення алгоритму для просторової фільтрації аномалій і марковського оновлення репутації вузлів, а також розробку конкурентної програмної симуляції для емпіричного моделювання різних сценаріїв кібератак у висококонкурентному середовищі.

Дане дослідження є важливим для розвитку майбутніх децентралізованих систем критичного екологічного та індустріального моніторингу, де забезпечення візантійської відмовостійкості та цілісності багатовимірних даних є критичним фактором для надійної та автономної роботи мережі без використання вразливого центрального координатора

5. Результати дослідження

Для вирішення проблеми візантійських збоїв запропоновано алгоритм TWTMOM, який працює локально на кожному вузлі мережі. Алгоритм функціонує як конвеєр із трьох математично обґрунтованих етапів.

Нехай $V = \{v_1, v_2, ..., v_n\}$ – множина сусідніх вузлів у графі мережі, кожен вузол i локально підтримує вектор репутаційних оцінок до своїх сусідів: $T_i = \{t_{i,1}, t_{i,2}, ..., t_{tj}\}$, де $t_{i,j} \in [0,1]$. Оскільки екологічна телеметрія є багатовимірною, одночасний вимір CO2, NO2, температури та вологості, показники кожного сусіднього вузла j представлені вектором стану x_j.

На першому етапі вузол здійснює первинну ізоляцію грубих аномалій. Коли вузол i отримує масив багатовимірних спостережень $X = \{x_1, x_2, ..., x_m\}$ від m сусідів, стає неможливим застосувати просте лінійне сортування для відсікання викидів. Замість цього для ідентифікації аномальних векторів стану застосовується статистична відстань Махаланобіса, яка враховує коваріаційні зв'язки між різними екологічними метриками:

$$D_M(x_j) = \sqrt{(x_j - \mu)^T \sum^{-1} (x_j - \mu)} \quad (1)$$

де μ – вектор математичних сподівань контрольованих параметрів, а Σ – коваріаційна матриця телеметричного простору.

Вузол обчислює $D_M(x_j)$ для кожного сусіда. Масив очищених даних X_{trim} та відповідний йому масив довіри T_{trim} формується шляхом відсікання вузлів, чия відстань перевищує критичний теоретичний поріг τ визначається за розподілом χ^2:

$$X_{trim} = \{x_j \in X \mid D_M(x_j) \le \tau\} \quad (2)$$

Це гарантує детерміноване ізолювання грубих аномалій ще до етапу консенсусної агрегації.

На другому етапі застосовується метод просторового групування. Відфільтровані значення X_{trim} випадковим чином розбиваються на K непересічних блоків (buckets) $B_1, B_2, ..., B_K$. Для кожного блоку обчислюється локальне зважене середнє μ_k:

$$\mu_k = \frac{\sum_{j \in B_K} t_{tj} \times x_j}{\sum_{j \in B_K} t_{tj}} \quad (3)$$

Довірче зважування нейтралізує вузли із сумнівною репутацією, які випадково пройшли етап відсікання Махаланобіса під час прихованих stealth-атак або градієнтного дрейфу. Після цього глобальний агрегований консенсус C_i розраховується як координатна медіана від отриманих локальних середніх:

$$C_i = Median(\mu_1, \mu_2, ..., \mu_k) \quad (4)$$

Фінальна агрегована медіана C_i вважається тимчасовим еталоном. На третьому етапі кожен сусід-відправник отримує штраф або заохочення залежно від того, наскільки його дані відхилялися від цього еталона. Вузол i розраховує евклідову відстань $d_j = |x_j - C_i|$ для кожного сусіда j. Репутація оновлюється за допомогою штрафної функції P_j з експоненційним загасанням:

$$P_j = \begin{cases} 1, & d_j \le \theta \\ e^{-\gamma(d_j - \theta)}, & d_j \ge \theta \end{cases} \quad (5)$$

Оновлений рівень довіри розраховується як зважена сума поточної поведінки та історичної пам'яті:

$$t_{ij} = \lambda \times t_{ij} + (1 - \lambda) \times P_j \quad (6)$$

де λ – фактор історичної пам'яті, θ – поріг допустимої дисперсії, γ – коефіцієнт жорсткості покарання.

Завдяки цьому циклічному зворотному зв'язку, у наступних консенсусних епохах значення від вузлів, що постійно генерують аномалії, математично ігноруватимуться системою.

Для наочного відображення послідовності обчислень та логіки прийняття рішень на кожному з трьох етапів, на рис. 1 представлена детальна алгоритмічна блок-схема запропонованого конвеєра TWTMOM. Вона ілюструє повний життєвий цикл обробки телеметрії від моменту отримання даних до оновлення глобального стану та ініціалізації наступної епохи.

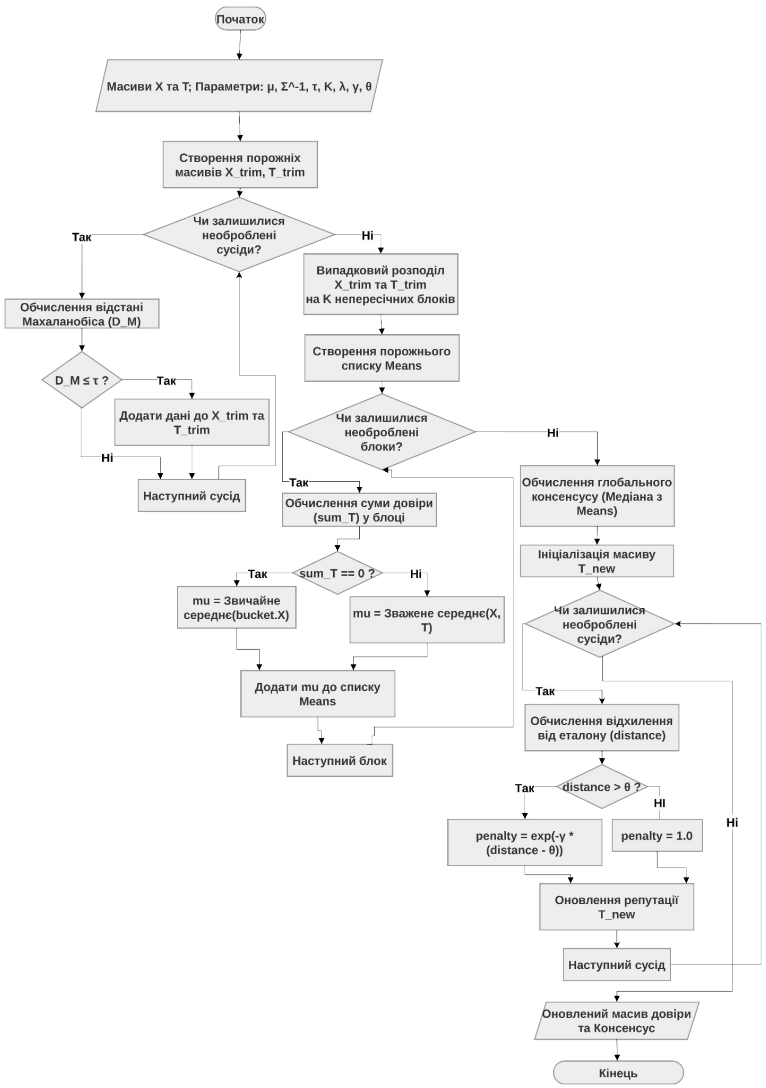

Рис. 1. Блок-схема конвеєра консенсусної агрегації алгоритму TWTMOM із просторовою фільтрацією Махаланобіса.

Для валідації математичної моделі та перевірки алгоритму в умовах, наближених до реальних high-load систем, ядро агрегації було реалізовано мовою програмування Golang. Вибір цієї мови зумовлений її високою ефективністю при роботі з пам'яттю та вбудованими механізмами конкурентності (goroutines), що є критично важливими для децентралізованих IoT-мережах.

Наведено фрагмент програмної реалізації головного конвеєра, який приймає багатовимірні матриці телеметрії та виконує просторове відсікання з подальшим зважуванням. Для оптимізації матричних обчислень застосовано пакети лінійної алгебри.

```
func Aggregate(X [][]float64, T []float64, muEnv []float64, sigmaInv *mat.Dense, tau, K, lambda, gamma, threshold float64) ([]float64, []float64) {
        var XTrim [][]float64
        var TTrim []float64
        // просторове відсікання Махаланобіса (Mahalanobis-based Trimming)
        for i, x := range X {
                dM := calculateMahalanobis(x, muEnv, sigmaInv)
                if dM <= tau {
                        XTrim = append(XTrim, x)
```

```
                        TTrim = append(TTrim, T[i])
                }
        }

        // медіана довірчо-зважених середніх (Trust-Weighted MoM)
        bucketsX, bucketsT := randomSplit(XTrim, TTrim, int(K))
        var means [][]float64
        for i := range bucketsX {
                sumT := sumElements(bucketsT[i])
                if math.Abs(sumT) < 1e-9 {
                        means = append(means, arithmeticMean(bucketsX[i]))
                } else {
                        means = append(means, weightedMean(bucketsX[i], bucketsT[i], sumT))
                }
        }
        C := coordinateMedian(means)
        // оновлення репутації (Trust Decay Update)
        TNew := make([]float64, len(X))
        for i, x := range X {
                distance := euclideanDistance(x, C)
                penalty := 1.0
                if distance > threshold {
                        penalty = math.Exp(-gamma * (distance - threshold))
                }
                TNew[i] = lambda*T[i] + (1.0-lambda)*penalty
        }

        return C, TNew
}
```

Дослідження проводилось в умовах висококонкурентного середовища, симулювалася мережа з 1000 сенсорів температури, протягом 100 епох. Критерієм якості виступала середньоквадратична помилка відносно еталонного не деградованого значення.

Оцінка здійснювалася за двома основними векторами атак:

1. Зловмисні вузли транслюють аномальні показники зі зміщенням у 50 одиниць.
2. Зловмисники поступово збільшують значення, намагаючись непомітно змістити консенсус, маскуючись під природну дисперсію середовища.

Таблиця 1.

Порівняння середньоквадратичної помилки при різній концентрації шкідливих вузлів

Метод агрегації	**0%**	**5%**	**10%**	**15%**	**20%**	**30%**	**40%**	**50%**
Simple Mean	0.01	2.51	5.00	7.49	10.01	15.01	20.00	24.99
Alpha-Trimmed Mean	0.01	0.04	0.08	0.13	0.21	8.46	16.71	24.99
Coordinate Median	0.01	0.04	0.07	0.10	0.15	0.30	0.49	25.04
Krum (BFT)	0.01	0.02	0.01	0.01	0.01	0.02	0.01	40.01
TWTMOM (Запропоновано)	0.01	0.01	0.02	0.02	0.02	0.03	0.02	25.09

У Таблиці 1 представлено розширені результати дослідження помилки при поступовому збільшенні концентрації зловмисних вузлів від 0% до 50% від загального розміру мережі.

Для наочної візуалізації стійкості алгоритмів, було проведено порівняльне дослідження п'яти методів агрегації. На рис. 2 представлено графік залежності середньоквадратичної помилки від відсотка

скомпрометованих вузлів. Оскільки деградація необастних методів має експоненціальний характер, вісь ординат (RMSE) відображено у логарифмічному масштабі.

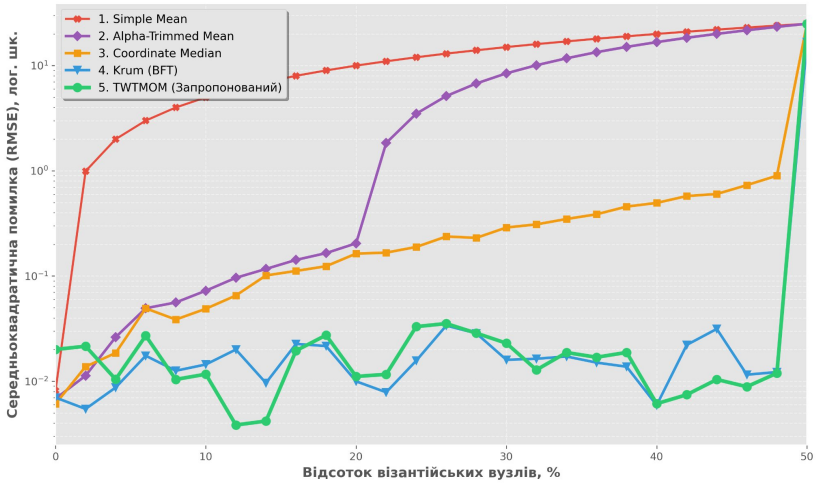

Рис. 2. Динаміка зростання помилки агрегації залежно від частки візантійських вузлів у мережі

Метод Simple Mean втрачає гомеостаз вже при 5% атакуючих вузлів. Алгоритм Alpha-Trimmed Mean працює бездоганно до закладеного порогу відсікання у 20%, після чого математично «ламається» і його похибка стрімко зростає. Алгоритм Krum демонструє стабільність протягом усього вектора атаки, але має відносно високу базову похибку через вибір лише одного вектора з усієї вибірки, що нівелює переваги статистичного усереднення. По-перше, Krum має квадратичну обчислювальну складність $O(N^2D)$, що робить його запуск на Edge-вузлах практично неможливим для великих мереж. По-друге, Krum завжди обирає значення лише одного конкретного датчика, відкидаючи 99.9% легітимної вибірки, через що у багатовимірному просторі його похибка дисперсії не зменшується від усереднення. По-третє, він вимагає заздалегідь відомої точної кількості зловмисників. Натомість запропонований алгоритм TWTMOM працює за лінійний час O(N), не потребує знання частки атакуючих, і формує плато стійкості аж до критичної позначки у 40-50% зловмисників, ідеально об'єднуючи робастність до викидів із математичною мінімізацією дисперсії.

Для перевірки стійкості алгоритму до прихованих атак, симулювався градієнтний дрейф показників від 0.0 до 15.0 °C.

Таблиця 2.

Рівень агрегаційної помилки при градієнтній атаці

Крок дрейфу	**0.0**	**2.5**	**5.0**	**7.5**	**10.0**	**12.5**	**15.0**
Simple Mean	0.04	0.73	1.48	2.22	2.96	3.72	4.50
Alpha-Trimmed Mean	0.03	0.53	0.93	1.34	1.74	2.17	2.60
Coordinate Median	0.02	0.29	0.27	0.30	0.27	0.27	0.27
Krum (BFT)	0.01	0.35	0.62	0.81	1.15	1.30	1.61
TWTMOM (Запропоновано)	0.03	0.57	0.01	0.03	0.02	0.01	0.03

Для оцінки поведінки системи в динаміці, було змодельовано процес прихованої GIGO-атаки протягом 100 консенсусних епох (рис. 3) за наявності 30% скомпрометованих вузлів. Зловмисні датчики застосовували градієнтний дрейф, плавно збільшуючи похибку на кожній епосі, маскуючись під природні коливання середовища.

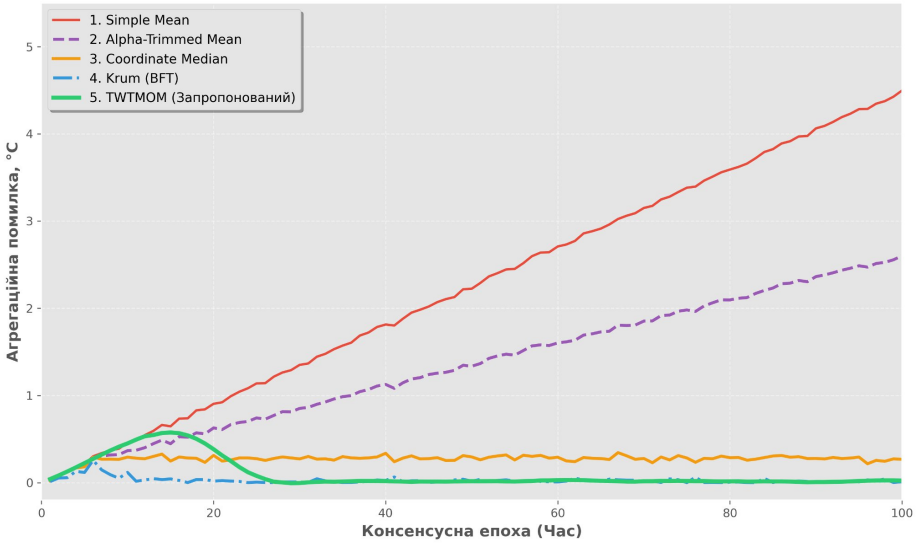

Рис. 3. Еволюція помилки агрегації у часі під час градієнтної stealth-атаки

На графіку (рис. 3.) видно ключовий недолік статичних робастних методів. Хоча Coordinate Median, Alpha-Trimmed Mean та Krum мають вбудовані механізми захисту від різких викидів, вони позбавлені історичної "пам'яті", тому лінійно акумулюють похибку в міру зростання градієнтного дрейфу. Додатково, алгоритми на кшталт Krum вимагають статично заданого ліміту атакуючих f, тому в динамічних сценаріях, коли зловмисники поступово нарощують дрейф, такі методи починають деградувати. Натомість крива запропонованого алгоритму TWTMOM демонструє абсолютно іншу динаміку. Завдяки механізму марковської системи оновлення довіри (Trust Score), на перших епохах до 20-ї TWTMOM проходить адаптаційний період, калібруючи репутацію вузлів через експоненційні штрафні функції. Після цього вага атакуючих датчиків зводиться до нуля, крива помилки стабілізується і утримується на мінімальному еталонному рівні незалежно від подальшого зростання сили атаки.

Для підтвердження внутрішньої механіки алгоритму, на рис. 4 наведено динаміку зміни рівня довіри Trust Score для легітимних та візантійських вузлів протягом тієї ж самої атаки.

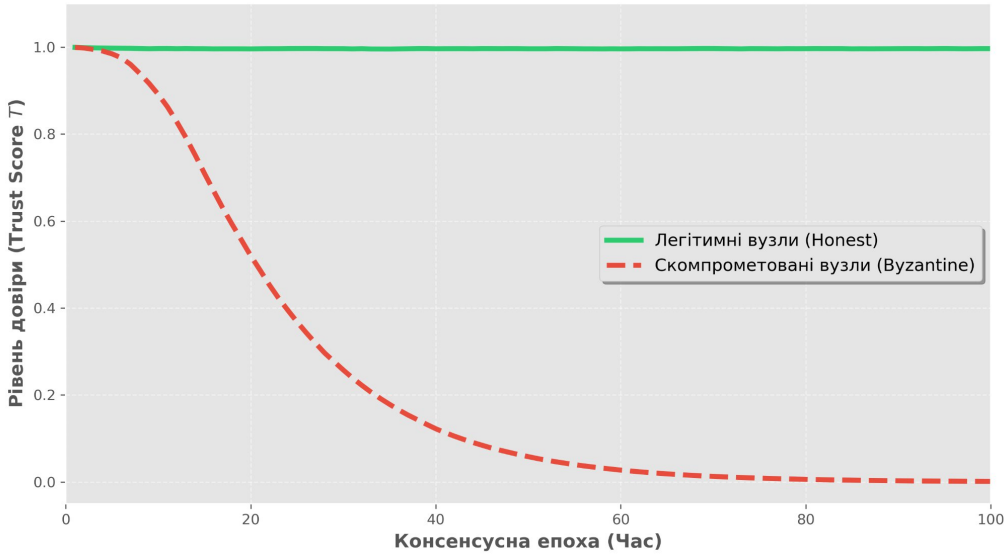

Рис. 4. Еволюція математичного рівня довіри легітимних та скомпрометованих вузлів під час GIGO-атаки

Експоненційна штрафна функція гарантує, що довіра до легітимних вузлів залишається стабільно високою, оскільки їхні показники лежать у межах допустимої дисперсії. Натомість репутація скомпрометованих вузлів стрімко падає до математичного нуля одразу після того, як градієнтний дрейф починає перевищувати рівень природного шуму. Саме ця диференціація дозволяє TWTMOM повністю ігнорувати отруєні дані на наступних епохах.

6. Висновки та перспективи подальших досліджень.

У дослідженні було проведено комплексний аналіз існуючих підходів до децентралізованої агрегації даних у розподілених IoT-мережах екологічного моніторингу. Аналіз існуючих методів показав, що жоден із них окремо не може повністю вирішити проблему візантійської відмовостійкості в умовах багатовимірних атак та прихованого дрейфу, однак поєднання робастної статистики та динамічних репутаційних систем дозволяє досягти безпрецедентної стійкості консенсусу.

Стандартні методи усереднення та просторової медіани демонструють високу ефективність у стабільних умовах, але їх математична вразливість призводить до стрімкої деградації системи вже за наявності 5–10% скомпрометованих вузлів. Алгоритми з фіксованим статистичним відсіканням, такі як Alpha-Trimmed Mean, забезпечують стабільність лише до заздалегідь визначеного порогу, після чого швидко акумулюють критичну похибку. Використання спеціалізованих BFT-протоколів, зокрема Krum, дозволяє підтримувати гомеостаз за високої концентрації зловмисників, проте їх квадратична обчислювальна складність та втрата переваг дисперсійного усереднення суттєво обмежують їх впровадження на малопотужних Edge-пристроях у великих мережах.

Перспективи подальших досліджень спрямовані на створення гібридних архітектур, що поєднують можливості алгоритму TWTMOM та блокчейн-технологій. Одним із ключових напрямів є розробка повноцінної інфраструктури розподілених реєстрів для забезпечення криптографічної імутабельності екологічної телеметрії на всіх етапах її життєвого циклу. Додатково актуальним є питання адаптації алгоритму до умов асинхронних мережевих затримок, що дозволить оптимізувати процес обміну даними в умовах нестабільного зв'язку.

Також варто приділити увагу створенню вдосконалених механізмів прогнозування багатовимірних stealth-атак на основі аналізу часових рядів, що суттєво підвищить кібербезпеку гетерогенних мереж у разі скоординованого зовнішнього втручання.

Таким чином, подальші дослідження мають бути спрямовані на розробку адаптивних багатофакторних підходів до обробки даних, що враховуватимуть багатовимірність телеметрії, динаміку топології мережі та нові вектори загроз, що дозволить значно покращити стійкість критично важливих систем екологічного та індустріального моніторингу.

Список використаних джерел

1. Fasolo, E., Rossi, M., Widmer, J., & Zorzi, M. (2007). In-network aggregation techniques for wireless sensor networks: A survey. *IEEE Wireless Communications*, 14(2), 70–87. https://doi.org/10.1109/mwc.2007.358967
2. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
3. Quan, C., Han, Y. S., Geng, B., & Varshney, P. K. (2022). Reputation and audit bit based distributed detection in the presence of Byzantines. In *2022 56th Asilomar Conference on Signals, Systems, and Computers*. IEEE. https://doi.org/10.1109/ieeeconf56349.2022.10051853
4. Yin, D., Chen, Y., Ramchandran, K., & Bartlett, P. (2018). Byzantine-robust distributed learning: Towards optimal statistical rates. In *International Conference on Machine Learning (ICML)* (pp. 5650-5659). PMLR.
5. Xu, G., Lei, L., & Mao, Y. (2025). CBRFL: A framework for committee-based Byzantine-resilient federated learning. *Journal of Network and Computer Applications*, 238, Article 104165. https://doi.org/10.1016/j.jnca.2025.104165
6. Blanchard, P., El Mhamdi, E. M., Guerraoui, R., & Stainer, J. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent. *Advances in Neural Information Processing Systems (NIPS)*, 30, 119-129.
7. Yang, Y., et al. (2025). TRBFT: An Efficient Blockchain Consensus for Edge Computing-Enabled IoT Systems. *IEEE Internet of Things Journal*, 1-14. https://doi.org/10.1109/JIOT.2025.3880226
8. Lecué, G., & Lerasle, M. (2020). Robust machine learning by median-of-means: Theory and practice. *Annals of Statistics*, 48(2), 906–931. https://doi.org/10.1214/19-aos1828
9. Zhang, H., Wang, W., Jiao, X., Yang, M., & Wu, X. (2024). A resilient decentralized learning approach against Byzantine attack via reputation evaluation. In *2024 39th Youth Academic Annual Conference of Chinese Association of Automation (YAC)*. IEEE. https://doi.org/10.1109/yac63405.2024.10598443
10. Lavaur, L., Lechevalier, P.-M., Busnel, Y., Ludinard, R., & Pahl, M.-O. (2024). RADAR: Model quality assessment for reputation-aware collaborative federated learning. In *2024 43rd International Symposium on Reliable Distributed Systems (SRDS)* (pp. 222–234). IEEE. https://doi.org/10.1109/srds64841.2024.00030
11. Putra, G. D., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2020). Trust management in decentralized IoT access control system. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-9). IEEE. https://doi.org/10.1109/ICBC48266.2020.9169433
12. Garcia-Font, V., Garrigues, C., & Rifà-Pous, H. (2016). A comparative study of anomaly detection techniques for smart city wireless sensor networks. *Sensors*, 16(6), 868. https://doi.org/10.3390/s16060868

References

1. Fasolo, E., Rossi, M., Widmer, J., & Zorzi, M. (2007). In-network aggregation techniques for wireless sensor networks: A survey. *IEEE Wireless Communications*, 14(2), 70–87. https://doi.org/10.1109/mwc.2007.358967
2. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

3. Quan, C., Han, Y. S., Geng, B., & Varshney, P. K. (2022). Reputation and audit bit based distributed detection in the presence of Byzantines. In *2022 56th Asilomar Conference on Signals, Systems, and Computers*. IEEE. https://doi.org/10.1109/ieeeconf56349.2022.10051853

4. Yin, D., Chen, Y., Ramchandran, K., & Bartlett, P. (2018). Byzantine-robust distributed learning: Towards optimal statistical rates. In *International Conference on Machine Learning (ICML)* (pp. 5650-5659). PMLR.

5. Xu, G., Lei, L., & Mao, Y. (2025). CBRFL: A framework for committee-based Byzantine-resilient federated learning. *Journal of Network and Computer Applications*, 238, Article 104165. https://doi.org/10.1016/j.jnca.2025.104165

6. Blanchard, P., El Mhamdi, E. M., Guerraoui, R., & Stainer, J. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent. *Advances in Neural Information Processing Systems (NIPS)*, 30, 119-129.

7. Yang, Y., et al. (2025). TRBFT: An Efficient Blockchain Consensus for Edge Computing-Enabled IoT Systems. *IEEE Internet of Things Journal*, 1-14. https://doi.org/10.1109/JIOT.2025.3880226

8. Lecué, G., & Lerasle, M. (2020). Robust machine learning by median-of-means: Theory and practice. *Annals of Statistics*, 48(2), 906–931. https://doi.org/10.1214/19-aos1828

9. Zhang, H., Wang, W., Jiao, X., Yang, M., & Wu, X. (2024). A resilient decentralized learning approach against Byzantine attack via reputation evaluation. In *2024 39th Youth Academic Annual Conference of Chinese Association of Automation (YAC)*. IEEE. https://doi.org/10.1109/yac63405.2024.10598443

10. Lavaur, L., Lechevalier, P.-M., Busnel, Y., Ludinard, R., & Pahl, M.-O. (2024). RADAR: Model quality assessment for reputation-aware collaborative federated learning. In *2024 43rd International Symposium on Reliable Distributed Systems (SRDS)* (pp. 222–234). IEEE. https://doi.org/10.1109/srds64841.2024.00030

11. Putra, G. D., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2020). Trust management in decentralized IoT access control system. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-9). IEEE. https://doi.org/10.1109/ICBC48266.2020.9169433

12. Garcia-Font, V., Garrigues, C., & Rifà-Pous, H. (2016). A comparative study of anomaly detection techniques for smart city wireless sensor networks. *Sensors*, 16(6), 868. https://doi.org/10.3390/s16060868

Надійшла до редакції: 13.03.26
Прийнята до друку:12.06.26
Опубліковано:30.06.26