УДК 004.738.5:004.056
DOI: https://doi.org/10.17721/AIT.2025.2.01

**Олена СІПКО, канд. техн. наук**
**ORCID ID: 0000-0003-1385-119X**
**e-mail: sipko.olena@knu.ua**

**Ольга КРАВЧЕНКО, канд. техн. наук, доц.**
**ORCID ID: 0000-0002-9669-2579**
**e-mail: olha.kravchenko@knu.ua**
**Київський національний університет імені Тараса Шевченка, Київ, Україна**

# МЕТОД КОНТЕКСТНО-ЗАЛЕЖНОГО ОЦІНЮВАННЯ НАДІЙНОСТІ В IoT-СИСТЕМАХ

**Вступ.** ***У роботі досліджено проблему оцінювання надійності вузлів у розподілених системах інтернету речей, що функціонують у динамічному середовищі з непередбачуваними умовами. Застосування класичних статистичних і структурних методів оцінювання надійності без урахування контекстних факторів призводить до зниження точності прогнозування відмов та ускладнює процес керування такими системами. Метою роботи є розроблення методу оцінювання надійності вузлів у розподілених IoT-системах з урахуванням контексту середовища для підвищення достовірності оцінювання стану вузлів та системи в цілому.***

**Методи.** ***Використано методи математичного моделювання, аналізу складних систем, імітаційного комп'ютерного моделювання, чисельної обробки даних, а також методи графового подання мережевих структур.***

**Результати.** ***Для досягнення поставленої мети розв'язано завдання формалізації надійності вузлів у вигляді контекстно-залежної моделі, що враховує фізичні, енергетичні й мережеві параметри середовища; розроблення механізму нормалізації контекстних параметрів та побудови функцій чутливості для різних типів впливів; формування інтегрального показника надійності шляхом зваженого агрегування часткових оцінок; реалізації алгоритму оцінювання у середовищі Python з використанням бібліотек NumPy, pandas і networkx; проведення серії імітаційних експериментів для аналізу динаміки надійності й масштабованості алгоритму. Отримані результати підтверджують підвищення точності оцінювання надійності порівняно з методами середнього часу напрацювання на відмову та марковськими моделями без урахування контексту.***

**Висновки.** ***Запропонований метод дозволяє підвищити достовірність оцінювання стану вузлів у розподілених IoT-системах і забезпечує адаптацію до змін середовища в режимі, близькому до реального часу. Метод може бути використаний у підсистемах моніторингу, діагностики та керування ресурсами IoT-мереж.***

**Ключові слова:** ***метадані, оптимізація, управління, інформація, динамічність, адаптивність, релевантність, продуктивність, якість, алгоритм, стиснення.***

## Вступ

Інтернет речей (IoT) є ключовою технологією сучасного цифрового суспільства, що забезпечує інтеграцію фізичних об'єктів у єдиний інформаційний простір. Кількість пристроїв, підключених до мереж IoT, зростає експоненційно, охоплюючи промисловість, енергетику, транспорт, медицину, сільське господарство та побутові застосування (Atzori et al., 2016; Sethi, & Sarangi, 2017; Al-Fuqaha et al., 2015). Разом із цим зростає складність архітектури таких систем, які функціонують у динамічному середовищі з непередбачуваними умовами.

Надійність вузлів у розподілених IoT-системах є одним із визначальних факторів їхньої ефективності. Вузли часто працюють у змінних контекстах – за різних температур, рівнів вологості, енергоспоживання, якості бездротового зв'язку чи навантаження обчислювальних ресурсів (Park, 2016; Xing et al., 2017). Класичні методи оцінювання надійності ґрунтуються переважно на статистичних або структурних моделях (напр., схемах надійності або показниках середнього часу безвідмовної роботи), які не враховують динамічну зміну контексту середовища (Dâmaso, Rosa, & Maciel, 2014). У результаті точність прогнозування відмов знижується, що впливає на стабільність роботи всієї IoT-системи.

Важливою особливістю сучасних IoT-систем є їхня здатність адаптуватися до контексту, тобто до набору факторів середовища, у якому працює вузол. Контекст може включати як фізичні параметри (температура, освітленість, рівень сигналу), так і логічні (тип застосунку, пріоритет трафіку, рівень довіри до сусідніх вузлів) (Perera et al., 2015). Тому виникає потреба у створенні методів оцінювання надійності, які враховують вплив контексту середовища в режимі реального часу.

Метою роботи є розроблення методу оцінювання надійності вузлів у розподілених IoT-системах із урахуванням контекстних факторів середовища, що дозволяє підвищити точність оцінки стану системи й забезпечити більш ефективне керування її ресурсами. Для досягнення цієї мети запропоновано контекстно-залежну модель надійності вузлів, яка поєднує структурний підхід із аналізом динамічних контекстних параметрів і дозволяє обчислювати інтегральний показник надійності у змінних умовах.

***Постановка задачі.*** Як зазначено у вступі, класичні підходи до оцінювання надійності вузлів у розподілених системах базуються переважно на статистичних характеристиках відмов або на структурному аналізі системи. Такі методи передбачають, що імовірність відмови елемента є сталою, а вплив зовнішніх факторів не враховується або моделюється через середні значення. Однак для IoT-систем це припущення є неприйнятним, оскільки вузли працюють у мінливих умовах середовища, а їхні характеристики можуть істотно змінюватися в часі (Chen, Wan, & Li, 2012; Xing, 2020).

Надійність вузла IoT визначається не лише його технічними параметрами, але й контекстом, у якому він функціонує. Наприклад, підвищення температури навколишнього середовища може впливати на стабільність передавача, коливання напруги – на ефективність джерела живлення, а зниження рівня сигналу – на частоту помилок у каналі зв'язку. Крім того, у розподілених системах надійність одного вузла впливає на надійність сусідніх вузлів через механізми маршрутизації, передачі даних або спільного доступу до ресурсів (Al-Fuqaha et al., 2015; Djedjig et al., 2020).

**© Сіпко Олена, Кравченко Ольга, 2025**



ISSN 2788-6603

Отже, для коректного оцінювання поточного стану вузлів необхідно враховувати не лише технічні показники (приміром, середній час напрацювання на відмову), але й контекстні фактори середовища, що мають динамічний характер.

У зв'язку з цим постає задача розробки методу оцінювання надійності вузлів у розподілених IoT-системах, який враховує вплив контекстних параметрів середовища та дозволяє оперативно оновлювати інтегральний показник надійності на основі поточних даних сенсорів і мережевих метрик.

Для формалізації задачі введемо такі позначення:

- $R_i(t)$ – поточна надійність вузла $i$ у момент часу $t$;
- $C_i(t) = \{c_1, c_2, \dots, c_n\}$ – вектор контекстних параметрів середовища для вузла $i$ (температура, рівень сигналу, завантаження процесора, енергозапас тощо);
- $f_i(C_i(t))$ – функція впливу контексту на зміну надійності;
- $R_i^0$ – базова (номінальна) надійність вузла без урахування контексту.

Таким чином, інтегральна оцінка надійності вузла у момент часу $t$ може бути подана як:

$$R_i(t) = R_i^0 \cdot f_i(C_i(t)), \tag{1}$$

де функція $f_i$ відображає вплив контексту на поточний стан вузла та нормується в межах $0 < f_i \leq 1$.

Задача полягає в побудові функціональної залежності $f_i(C_i(t))$, яка дозволяє динамічно враховувати зміну контекстних параметрів і визначати їхній ваговий внесок у загальну надійність вузла. Для цього необхідно:

1) визначити перелік релевантних контекстних параметрів середовища;
2) побудувати функціональну залежність між контекстом і надійністю вузла;
3) запропонувати алгоритм обчислення інтегрального показника надійності в реальному часі;
4) провести оцінювання точності запропонованого методу порівняно із традиційними моделями.

Наукова новизна роботи полягає в розробленні контекстно-залежного методу оцінювання надійності вузлів у розподілених IoT-системах, який уперше враховує вплив динамічних параметрів середовища на поточний стан вузла й дозволяє адаптивно оновлювати показник надійності в режимі реального часу. Такий підхід забезпечує підвищення точності оцінювання порівняно із традиційними статистичними методами та може бути використаний для прийняття рішень у системах управління довірою, самоорганізації та відновлення працездатності IoT-мереж.

**Методи**

Запропонований метод оцінювання надійності вузлів у розподілених IoT-системах ґрунтується на поєднанні структурного аналізу системи та динамічного врахування контекстних параметрів середовища. На відміну від традиційних статистичних підходів, які передбачають сталість імовірності відмов елементів і не враховують зміну умов роботи, запропонований підхід розглядає надійність вузлів як функцію, що змінюється в часі під впливом динамічних контекстних факторів (Feng et al., 2023). У реальних розподілених середовищах вузли IoT піддаються впливу численних зовнішніх і внутрішніх змінних, зокрема температури, вологості, рівня енергії, якості зв'язку, навантаження процесора, кількості переданих пакетів тощо. Саме ці параметри визначають їхню фактичну працездатність і частоту відмов (Dâmaso, Rosa, & Maciel, 2014; Djedjig et al., 2020; García-Martín, & Torralba, 2023; Saeed et al., 2021).

Основну математичну модель надійності було сформульовано вище, тому зараз увага зосереджується на процедурі нормування параметрів, побудові часткових функцій чутливості, визначенні вагових коефіцієнтів і реалізації дискретного алгоритму обчислення інтегрального показника.

Першим етапом методу є збір та попередня обробка контекстних параметрів, що характеризують поточний стан вузла й середовища його функціонування. Для забезпечення порівняності параметрів різної фізичної природи всі значення нормуються до інтервалу [0,1]. Нормалізація здійснюється за формулою:

$$c_j'(t) = \frac{c_j(t) - c_j^{min}}{c_j^{max} - c_j^{min}}, \tag{2}$$

де $c_j^{min}$ та $c_j^{max}$ задають діапазон допустимих значень параметра. Отримане нормалізоване значення інтерпретується як "ступінь відповідності умов" оптимальному режиму роботи вузла.

Після нормалізації кожен параметр оцінюється за допомогою часткової функції чутливості $g_j(c_j'(t))$. Ця функція відображає характер впливу параметра на працездатність вузла. Для параметрів зі сталою або приблизно лінійною залежністю відхилення від оптимального значення доцільно використовувати лінійну таку модель:

$$g_j\left(c_j'(t)\right) = 1 - \alpha_j \left|c_j'(t) - c_{j,opt}'\right|, \tag{3}$$

де $\alpha_j$ – коефіцієнт чутливості, а $c_{j,opt}'$ – нормоване оптимальне значення.

Для параметрів, що мають різке погіршення при відхиленні від норми (напр., температура або напруга), застосовується експоненційна залежність:

$$g_j\left(c_j'(t)\right) = e^{-\beta_j \left|c_j'(t) - c_{j,opt}'\right|}, \tag{4}$$

де $\beta_j$ визначає швидкість зниження працездатності.

У випадках, коли суттєві наслідки виникають після подолання певного порогу (приміром, критично низький рівень енергії), використовується логістична функція:

$$g_j\left(c_j'(t)\right) = \frac{1}{1 + e^{-\gamma_j \left|c_j'(t) - c_{j,th}'\right|}}, \tag{5}$$

де значення $c_{j,opt}'$ відповідає оптимальному рівню параметра, а $c_{j,th}'$ – граничному порогу стабільної роботи; $\gamma_j$ – це коефіцієнт крутизни (slope coefficient) логістичної кривої. Логістична функція має S-подібну форму. Якщо $\gamma_j$ велика, крива дуже крута – невелике відхилення від порогу $c_{j,opt}'$ різко змінює оцінку. Наприклад: батарея падає із 20 до 15 %, відповідно різко падає працездатність. Якщо $\gamma_j$ мала, крива більш полога – оцінка змінюється плавно. Приміром:

параметр, який не є критичним (напруга, яку компенсує стабілізатор). У нашому випадку $\gamma_j$ використовується для таких параметрів, як:

- рівень енергозапасу батареї;
- рівень доступної пам'яті;
- мережевий буфер перед переповненням;

тобто там, де існує поріг, після якого вузол швидко втрачає надійність.

Одержані значення часткових функцій відображають оцінку стану вузла щодо кожного контекстного параметра. Для отримання інтегральної оцінки впливу контексту ці значення агрегуються з використанням вагових коефіцієнтів:

$$f_i\big(C_i(t)\big) = \sum_{j=1}^{n} w_j g_j\left(c_j'(t)\right), \tag{6}$$

де $w_j$ – коефіцієнти важливості, що задовольняють умову

$$\sum_{j=1}^{n} w_j = 1, w_j \geq 0. \tag{7}$$

Вагові коефіцієнти можуть визначатися експертно або обчислюватися автоматично за допомогою методів багатокритеріального аналізу. Наприклад, при застосуванні методу аналізу ієрархій матриця попарних порівнянь дозволяє оцінити відносну важливість кожного параметра й отримати узгоджений вектор ваг $w_j$.

Після визначення часткових й агрегованих оцінок, інтегральний показник надійності вузла оновлюється у дискретні моменти часу. Оскільки контекстні параметри змінюються в реальному середовищі досить швидко, дискретне оновлення моделі дозволяє враховувати динаміку процесів і підтримувати актуальність оцінки. Обчислювальний цикл складається з таких етапів: збір параметрів, їх нормування, обчислення $g_j$, отримання агрегованого показника $f_i$ та подальше оновлення інтегральної оцінки згідно з основною моделлю.

З метою формалізації програмної реалізації запропонованого підходу наведено алгоритм його виконання в середовищі Python із використанням бібліотек NumPy, pandas і networkx.

***Алгоритм реалізації запропонованого методу***

1. Задати множину вузлів IoT-системи $V = \{1,2,\dots,N\}$, початкові значення надійності та перелік контекстних параметрів.
2. Побудувати орієнтований граф мережі у networkx; у вузлах зберігати надійність і поточні параметри.
3. Ініціалізувати структури pandas для збереження таблиць контексту та динаміки надійності.
4. Зчитати або сформувати дані контекстних параметрів для кожного вузла на поточному кроці моделювання.
5. Нормалізувати всі параметри за формулою масштабування до інтервалу $[0,1]$.
6. Обчислити часткові функції чутливості $g_j$ за відповідними формулами для кожного параметра.
7. Агрегувати часткові оцінки у значення $f_i\big(C_i(t)\big)$ шляхом зваженого підсумовування.
8. Оновити інтегральні значення надійності відповідно до базової моделі з "Постановки задачі".
9. Виявити вузли, для яких надійність стала меншою за порогове значення, сформувати підграф критичних вузлів.
10. Записати результати в таблиці та візуалізувати динаміку змін для аналізу.

Наведений алгоритм забезпечує послідовну реалізацію всіх етапів методу – від збору та нормалізації контекстних даних до формування інтегральної оцінки надійності вузлів і подальшого аналізу стабільності системи.

Система подається як орієнтований граф, у якому кожна вершина відповідає вузлу IoT-мережі, а ребра – каналам передачі даних. Контекстні параметри та оцінки надійності зберігаються як атрибути вузлів, що дозволяє синхронізувати топологію мережі та динаміку параметрів.

Застосований підхід допускає як централізовану, так і децентралізовану схему обчислень. У масштабних системах локальні агенти виконують проміжні оцінки для груп вузлів і передають агреговані дані глобальному контролеру, що істотно зменшує обсяг переданої інформації та затримки. Використання векторизованих операцій NumPy дозволило забезпечити ефективну обробку даних навіть для великої кількості вузлів.

У підсумку, запропонована реалізація формує адаптивну, масштабовану й обчислювально ефективну систему оцінювання надійності, придатну для використання у реальних розподілених IoT-середовищах із високою динамікою змін.

**Результати**

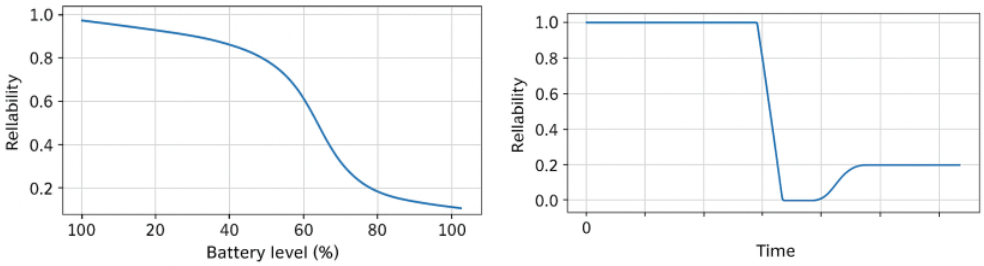
Для перевірки ефективності запропонованого методу оцінювання надійності було виконано серію обчислювальних експериментів у середовищі Python із використанням бібліотек NumPy, pandas та networkx. Моделювання проводилося для штучно згенерованих сценаріїв функціонування розподіленої IoT-мережі з різною кількістю вузлів і динамічними контекстними параметрами. Топологія мережі задавалася у вигляді орієнтованого графа з випадковим або кластеризованим розподілом з'єднань, а контекстні параметри формувалися як часові ряди з керованим рівнем шуму та стрибкоподібними збуреннями для відтворення реалістичних умов експлуатації.

У базових експериментах розглядалися три ключові контекстні групи: фізичні (температура середовища), мережеві (рівень сигналу) та енергетичні (залишковий заряд батареї). Для кожного вузла задавалися допустимі діапазони та порогові значення, а вагові коефіцієнти визначалися за методом аналізу ієрархій і в типовому сценарії становили $w_{temp} = 0{,}3$, $w_{signal} = 0{,}4$, $w_{energy} = 0{,}3$. Крок дискретизації дорівнював $\Delta t = 1$ хв, загальна тривалість симуляції – 24 год.

Початково було проаналізовано реакцію моделі на керовану деградацію одного параметра за стабільних інших. Зокрема, енергозапас вузла зменшувався від 100 до 10 % за фіксованої температури та рівні сигналу. Отримана траєкторія інтегральної надійності засвідчила нелінійний характер змін: за рівнів заряду понад 40 % деградація була близькою до лінійної, тоді як у зоні 30–20 % спостерігалося різке падіння показника (рис. 1). Це узгоджується з очікуваною пороговою поведінкою енергетичного параметра та підтверджує доцільність використання логістичної функції впливу.



ISSN 2788-6603




(а) (б)

**Рис. 1. Траєкторія інтегральної надійності:**
**(а) динаміка надійності вузла при зменшенні рівня заряду батареї,**
**(б) реакція надійності вузла на стрибкоподібне зниження рівня сигналу**

В окремому сценарії досліджувалася чутливість моделі до раптових погіршень умов зв'язку. Для підмножини вузлів рівень сигналу знижувався ступінчасто на 15–20 дБ із подальшим відновленням. У відповідь інтегральна надійність синхронно зменшувалася разом зі збуренням і поверталася до номінальних значень після нормалізації каналу, демонструючи невелику інерційність – ефект "пам'яті стану". Така поведінка коректно відображає накопичувальний вплив попередніх умов і підтверджує здатність моделі адекватно реагувати на швидкі зміни середовища.

Для кількісного оцінювання ефективності запропонованого підходу результати контекстно-залежної моделі було зіставлено із двома базовими методами: традиційним показником середнього часу напрацювання на відмову (MTTF) та марковською моделлю без урахування контекстних параметрів. Як метрику якості використано середньоквадратичну похибку (RMSE) між прогнозованою надійністю та еталонними сценаріями відмов. Як показано на рис. 2, контекстна модель забезпечує найменше значення RMSE (0,16) порівняно з марковською моделлю (0,20) та методом MTTF (0,22). Відповідно, відносне зменшення похибки становить 27 % порівняно з MTTF та 20 % – порівняно з марковською моделлю, що підтверджує істотну перевагу врахування контекстних факторів у задачах оцінювання надійності вузлів в умовах змінного середовища. Це свідчить про кращу адаптацію до змін і точніше відображення реального стану вузлів у часі.

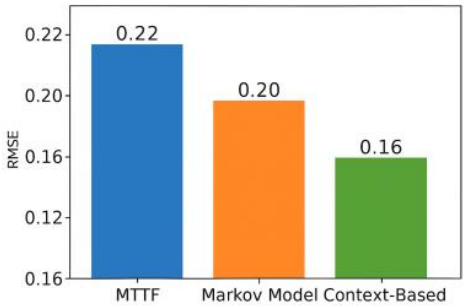



**Рис. 2. Порівняння точності методів за RMSE у динамічному середовищі**

Оцінювалася також масштабованість алгоритму для різної кількості вузлів $N = 50,100,500,1000$. Час обчислення одного кроку зростав лінійно відносно $N$, що відповідає теоретичній складності $O(N \cdot n)$, де $n$ – кількість контекстних параметрів. Навіть для $N = 1000$ середній час ітерації не перевищував сотих часток секунди на типовому ноутбуці, що підтверджує придатність методу для застосувань, близьких до реального часу. Децентралізований варіант реалізації з локальними агентами зменшив обсяг переданих до центрального вузла даних на 35–45 %, що є важливим для мереж із обмеженою пропускною здатністю.

Оцінювалася масштабованість алгоритму та стабільність часу виконання для різної кількості вузлів у мережі. На рис. 3 наведено розподіл часу виконання симуляцій та залежність тривалості обчислень від кількості вузлів.

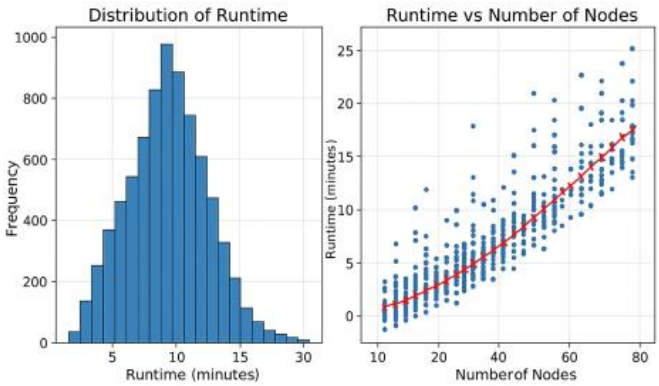



**Рис. 3. Розподіл часу виконання алгоритму та залежність тривалості обчислень від кількості вузлів мережі**

Ліва частина рисунка демонструє гістограму розподілу часу виконання, з якої видно, що більшість запусків зосереджена у проміжку до 10 хвилин із поступовим зменшенням частоти для більших значень. Це свідчить про загальну стабільність алгоритму та відсутність систематичних тривалих затримок обчислення.

Права частина рисунка ілюструє залежність часу виконання від кількості вузлів мережі у вигляді розсіювання результатів із трендовою кривою. Спостерігається зростання середнього часу виконання зі збільшенням кількості вузлів, однак характер залежності є поступовим і без різких стрибків. Це свідчить про те, що зі зростанням розміру системи обчислювальні витрати збільшуються прогнозовано, без деградації продуктивності.

Отримані результати підтверджують, що запропонований підхід демонструє прийнятну масштабованість і може використовуватися для моделювання й аналізу розподілених систем з великою кількістю вузлів. Відсутність аномальних піків у часових характеристиках та плавний характер тренду підтверджують стабільність роботи алгоритму в умовах зростаючого навантаження.

Нарешті, за інтегральними оцінками надійності виконано аналіз стійкості всієї мережі. У сценаріях із локальними відмовами одиничних вузлів система зберігала працездатність завдяки переналаштуванню маршрутів і перерозподілу навантажень. Водночас каскадні відмови, спричинені одночасною деградацією кількох параметрів у критичних вузлах, призводили до різкого падіння системної надійності, що коректно ідентифікувалося моделлю як передаварійний режим. Отже, інтегральний показник може застосовуватися не лише для локальної діагностики, а й для раннього виявлення ризиків на рівні всієї мережі.

**Дискусія і висновки**

У роботі запропоновано метод оцінювання надійності вузлів у розподілених IoT-системах із урахуванням контексту середовища, який дає змогу формувати інтегральний показник надійності з урахуванням динамічних змін умов експлуатації. На відміну від традиційних підходів, що ґрунтуються на статичних імовірнісних характеристиках або марковських моделях без урахування зовнішніх факторів, розроблений підхід дозволяє оперативно реагувати на зміну середовища функціонування вузлів і відображати реальний стан системи в часі.

Результати моделювання підтверджують ефективність контекстно-залежної оцінки: запропонований метод демонструє менші значення похибки порівняно з методом середнього часу напрацювання на відмову та марковською моделлю, що свідчить про підвищення точності прогнозування надійності у динамічних умовах. Показано, що урахування параметрів середовища, зокрема стану каналу зв'язку й енергетичних характеристик вузлів, істотно впливає на достовірність інтегральної оцінки та забезпечує адекватніше відображення реальної працездатності мережі.

Аналіз масштабованості підтвердив стабільну роботу алгоритму зі зростанням кількості вузлів у мережі: час виконання зростає поступово, без різких деградацій продуктивності, що підтверджує придатність методу для використання у середовищах із великою кількістю елементів. Характер розподілу часу виконання свідчить про відсутність систематичних затримок, що є важливою характеристикою для практичного застосування в системах, орієнтованих на обробку даних у режимі, близькому до реального часу.

Запропонований метод є універсальним і може бути інтегрований у різні архітектури IoT-систем, включаючи централізовані та децентралізовані структури із застосуванням крайових обчислень. Його використання відкриває можливості для побудови підсистем моніторингу, діагностики та прогнозування відмов, а також для прийняття обґрунтованих рішень щодо оптимізації функціонування мережі.

Подальші дослідження доцільно спрямувати на розширення набору контекстних параметрів, використання методів машинного навчання для автоматичного налаштування вагових коефіцієнтів, а також на експериментальну перевірку методу в умовах реальних IoT-розгортань.

**Внесок авторів:** Олена Сіпко – розробка методів і методології дослідження, опис результатів і написання висновків; Ольга Кравченко – огляд літературних джерел, збір даних і проведення експериментальних досліджень..

**Джерела фінансування.** Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

**Список використаних джерел**

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials,* 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Atzori, L., Iera, A., & Morabito, G. (2016). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

Chen, M., Wan, J., & Li, F. (2012). Machine-to-machine communications: Architectures, standards, and applications. *KSII Transactions on Internet and Information Systems*, 6(2), 447–474. https://doi.org/10.3837/tiis.2012.02.002

Dâmaso, A., Rosa, N., & Maciel, P. (2014). *Reliability of wireless sensor networks*. Sensors, 14(9), 15760–15785. https://doi.org/10.3390/s140915760

Djedjig, N., Tandjaoui, D., Romdhani, I., & Medjek, F. (2020). Trust-aware and cooperative routing protocol for IoT security. *Journal of Information Security and Applications*, 52, 102467. https://doi.org/10.1016/j.jisa.2020.102467

Feng, Q., Guo, X., Sun, B., Dui, H., Ren, Y., Hai, X., Yang, D., & Wang, Z. (2023). Reliability modeling of dynamic spatiotemporal IoT considering autonomy and cooperativity based on multiagent. *IEEE Internet of Things Journal*, 11(3), 4712–4721. https://doi.org/10.1109/JIOT.2023.3299975

García-Martín, J. P., & Torralba, A. (2023, August). *Energy consumption analytical modeling of NB-IoT devices for diverse IoT applications. Computer Networks, 232*, 109855. https://doi.org/10.1016/j.comnet.2023.109855

Park, J.-H. (2016). All-terminal reliability analysis of wireless networks of redundant radio modules. *IEEE Internet of Things Journal,* 3(2), 219–230. https://doi.org/10.1109/JIOT.2015.2496259

Perera, C., Liu, C. H., Jayawardena, S., & Chen, M. (2015). A survey on Internet of Things from industrial market perspective. *IEEE Access*, 2, 1660-1679. https://doi.org/10.1109/ACCESS.2015.2389854

Saeed, U., Lee, Y.-D., Jan, S. U., & Koo, I. (2021). CAFD: Context-aware fault diagnostic scheme towards sensor faults utilizing machine learning. *Sensors*, 21(2), 617. https://doi.org/10.3390/s21020617

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 9324035. https://doi.org/10.1155/2017/9324035

Xing, L. (2020). Reliability in Internet of Things: Current status and future perspectives. *IEEE Internet of Things Journal*, 7(8), 6704–6721. https://doi.org/10.1109/JIOT.2020.2993216



ISSN 2788-6603

Xing, L., Tannous, M., Vokkarane, V. M., Wang, H., & Guo, J. (2017). Reliability modeling of mesh storage area networks for Internet of Things. *IEEE Internet of Things Journal*, 4(6), 2047–2057. https://doi.org/10.1109/JIOT.2017.2749375

**Refeences**

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials,* 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Atzori, L., Iera, A., & Morabito, G. (2016). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, 56, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

Chen, M., Wan, J., & Li, F. (2012). Machine-to-machine communications: Architectures, standards, and applications. *KSII Transactions on Internet and Information Systems*, 6(2), 447–474. https://doi.org/10.3837/tiis.2012.02.002

Dâmaso, A., Rosa, N., & Maciel, P. (2014). *Reliability of wireless sensor networks*. Sensors, 14(9), 15760–15785. https://doi.org/10.3390/s140915760

Djedjig, N., Tandjaoui, D., Romdhani, I., & Medjek, F. (2020). Trust-aware and cooperative routing protocol for IoT security. *Journal of Information Security and Applications*, 52, 102467. https://doi.org/10.1016/j.jisa.2020.102467

Feng, Q., Guo, X., Sun, B., Dui, H., Ren, Y., Hai, X., Yang, D., & Wang, Z. (2023). Reliability modeling of dynamic spatiotemporal IoT considering autonomy and cooperativity based on multiagent. *IEEE Internet of Things Journal*, 11(3), 4712–4721. https://doi.org/10.1109/JIOT.2023.3299975

García-Martín, J. P., & Torralba, A. (2023, August). *Energy consumption analytical modeling of NB-IoT devices for diverse IoT applications. Computer Networks, 232*. 109855. https://doi.org/10.1016/j.comnet.2023.109855

Park, J.-H. (2016). All-terminal reliability analysis of wireless networks of redundant radio modules. *IEEE Internet of Things Journal,* 3(2), 219–230. https://doi.org/10.1109/JIOT.2015.2496259

Perera, C., Liu, C. H., Jayawardena, S., & Chen, M. (2015). A survey on Internet of Things from industrial market perspective. *IEEE Access*, 2, 1660-1679. https://doi.org/10.1109/ACCESS.2015.2389854

Saeed, U., Lee, Y.-D., Jan, S. U., & Koo, I. (2021). CAFD: Context-aware fault diagnostic scheme towards sensor faults utilizing machine learning. *Sensors*, 21(2), 617. https://doi.org/10.3390/s21020617

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, 9324035. https://doi.org/10.1155/2017/9324035

Xing, L. (2020). Reliability in Internet of Things: Current status and future perspectives. *IEEE Internet of Things Journal*, 7(8), 6704–6721. https://doi.org/10.1109/JIOT.2020.2993216

Xing, L., Tannous, M., Vokkarane, V. M., Wang, H., & Guo, J. (2017). Reliability modeling of mesh storage area networks for Internet of Things. *IEEE Internet of Things Journal*, 4(6), 2047–2057. https://doi.org/10.1109/JIOT.2017.2749375

**Отримано редакцією журналу / Received: 03.12.25**
**Прорецензовано / Revised: 26.12.25**
**Схвалено до друку / Accepted: 29.12.25**
**Опубліковано / Published: 06.05.26**

**Olena SIPKO, PhD (Engin.)**
**ORCID ID: 0000-0003-1385-119X**
**e-mail: sipko.olena@knu.ua**

**Olha KRAVCHENKO, PhD (Engin.), Assoc. Prof.**
**ORCID ID: 0000-0002-9669-2579**
**e-mail: olha.kravchenko@knu.ua**
**Taras Shevchenko National University of Kyiv, Kyiv, Ukraine**

## CONTEXT-AWARE RELIABILITY ASSESSMENT IN IOT SYSTEMS

**Background.** ***The paper addresses the problem of reliability assessment of nodes in distributed Internet of Things (IoT) systems operating in highly dynamic environments. The use of classical statistical reliability models and structural approaches without considering environmental and operational context leads to reduced accuracy of failure prediction and limited adaptability of IoT infrastructures. The aim of the paper is to develop a context-aware reliability assessment method for distributed IoT systems that improves the accuracy of node state evaluation under changing conditions.***

**Methods.** ***The research is based on methods of mathematical modeling, complex systems analysis, computer simulation, numerical data processing, and graph-based representation of network structures.***

**Results.** ***To achieve the stated goal, the following tasks were accomplished: development of a context-dependent reliability model that integrates physical, network, and energy-related parameters; design of a normalization procedure for heterogeneous context variables; construction of sensitivity functions for different impact factors; formation of an integral reliability index using weighted aggregation; software implementation of the proposed method in Python using NumPy, pandas, and networkx libraries; and experimental verification through simulation of distributed IoT environments. The obtained results demonstrate higher reliability estimation accuracy of the proposed method compared to traditional Mean Time To Failure approaches and context-independent Markov models.***

**Conclusions.** ***The developed context-aware method provides an adaptive reliability evaluation mechanism suitable for distributed IoT environments and supports real-time monitoring and decision-making tasks. The method can be utilized in IoT system diagnostics, failure prediction, and resource management subsystems.***

**Keywords:** ***Internet of Things, node reliability, context-aware model, computer simulation, distributed systems, reliability assessment.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.