УДК 621.396
DOI https://doi.org/10.32782/2663-5941/2026.1.1/17

Семенова О.О.
https://orcid.org/0000-0001-5312-9148
Вінницький національний технічний університет

Войцеховська О.О.
https://orcid.org/0000-0001-8504-1204
Вінницький національний технічний університет

Джус А.В.
https://orcid.org/0009-0005-3583-5766
Вінницький національний технічний університет

Кузняк В.П.
https://orcid.org/0009-0001-1775-420X
Вінницький національний технічний університет

РОЗРОБЛЕННЯ ТА ОПТИМІЗАЦІЯ НЕЧІТКОГО КОНТРОЛЕРА ДЛЯ ОЦІНЮВАННЯ ІНДЕКСУ ДОВІРИ В ІНТЕРНЕТІ РЕЧЕЙ

У статті запропоновано підхід до оцінювання індексу довіри до пристроїв в мережах Інтернету речей на основі обчислювального інтелекту, а саме нечіткої логіки та еволюційної оптимізації. Актуальність дослідження зумовлена зростанням кількості пристроїв Інтернету речей, які функціонують у потенційно складному середовищі, де традиційні методи забезпечення безпеки та оцінювання довіри часто є недостатньо ефективними. Оцінювання довіри розглядається як важливий механізм підвищення надійності та безпеки мереж Інтернету речей. Запропонована у ході дослідження модель базується на нечіткому контролері типу Мамдані. Модель має три вхідні змінні, сформовані з мережевих параметрів датасету NSL-KDD, та одну вихідну змінну, що відповідає індексу довіри до пристрою Інтернету речей. Для всіх вхідних і вихідної змінних використано гаусові функції належності, що забезпечує плавність логічного висновку та стійкість до невизначеності даних. База правил складається з повного набору логічних правил, які формалізують експертні знання щодо поведінки довірених і зловмисних вузлів. Розроблений нечіткий контролер формує метрику довіри, що дозволяє класифікувати пристрої IoT як надійні, потенційно небезпечні або зловмисні. З метою підвищення точності оцінювання індексу довіри до пристрою Інтернету речей було здійснено оптимізацію параметрів розробленого нечіткого контролера за допомогою генетичного алгоритму та методу рою частинок. Для оцінювання якості моделей застосовано такий показник як середньоквадратична похибка між прогнозованими та еталонними значеннями індексу довіри. Результати комп'ютерного моделювання підтверджують, що оптимізовані нечіткі контролери суттєво перевершують базову модель за точністю, а підхід з використанням методу рою частинок продемонстрував найкращі показники ефективності. Запропонована модель може бути інтегрована у системи безпеки Інтернету речей для підвищення надійності взаємодії між пристроями.

Ключові слова: *Інтернет речей, телекомунікації, безпека, довіра, нечіткий контролер, генетичний алгоритм, метод рою частинок, оптимізація.*

Постановка проблеми. Стрімкий розвиток телекомунікаційних технологій зумовив масове впровадження високошвидкісних мереж зв'язку, що забезпечують безперервний обмін даними між великою кількістю пристроїв. Наразі широке впровадження Інтернету речей (Internet of Things, IoT) супроводжується появою великої кількості гетерогенних розумних пристроїв, що взаємодіють між собою у одній мережі. У таких умовах питання безпеки та надійності обміну даними

стає надзвичайно важливим, оскільки компрометація навіть невеликої кількості вузлів може спричинити суттєве погіршення роботи всієї системи. Існуючі підходи до оцінювання значення рівня довіри до пристроїв здебільшого спираються на статистичні методи, що або мають низьку точність, або потребують великих обсягів навчальних даних і значних обчислювальних ресурсів.

У зв'язку з цим актуальною є проблема розроблення інтелектуального підходу до оцінювання індексу довіри до пристроїв Інтернету речей, здатного ефективно працювати в умовах невизначеності даних.

Аналіз останніх досліджень і публікацій. Сучасні дослідження у галузі IoT стосуються підвищення точності, масштабованості та гнучкості мереж. Однак часто вони не враховують такі важливі аспекти, як цілісність, доступність та конфіденційність даних.

Основна увага до довіри та репутації в пристроях Інтернету речей зосереджена на довірі всередині архітектури, застосунках та пристроїв на всіх рівнях IoT. Покращення конфіденційності та автентифікації користувачів відіграють вирішальну роль у створенні розумного середовища, що стає можливим завдяки інтеграції довіри та репутації в передачу даних.

Одним із підходів до оцінки довіри є методи, засновані на репутації, які спираються на показники, що збираються в розподілених середовищах. Як відомо, залежно від показників ефективності, що застосовуються для оцінки довіри та репутації IoT, розрізняють дві групи методів: традиційні схеми, засновані на управлінні довірою, та схеми управління довірою на основі штучного інтелекту.

Зокрема, в роботі [1] було розроблено централізовану схему управління довірою до пристроїв Інтернету речей, що передбачає обмін послугами між пристроями на базі сертифікатів довіри без проведення розрахунків довіри. У статті [2] для встановлення довіри до вузлів мережі запропоновано систему визначення їх репутації. Автори роботи [3] створили динамічну модель управління довірою, яка дозволяє вузлам мережі самостійно оцінювати поведінку своїх однорангових вузлів і призначати винагороди та штрафи. В дослідженні [4] була розроблена модель довіри, що інтегрує прямі та непрямі відомості про довіру для визначення значень довіри до пристроїв в IoT.

У сучасних дослідженнях значна увага приділяється застосуванню методів штучного інтелекту, зокрема нечіткої логіки, як ефективного інструменту для оцінювання довіри до пристроїв у мережах Інтернету речей. Так, у статті [5] розглядається поведінка користувача у моделі довіри для виявлення будь-яких аномальних закономірностей. У розробленій структурі використовувалася нечітка логіка для оцінки значень як всебічної, так і прямої довіри. Методика, представлена в роботі [6] базується на нечіткій логіці і спрямована на виявлення ненадійних вузлів. У роботі [7] запропонували схему управління довірою, яка побудована на принципах Байєсівського навчання та спільного фільтрування для забезпечення надійності.

Методи машинного навчання також широко застосовуються для оцінювання довіри шляхом аналізу надійності вузлів на основі довірчих характеристик. У наукових дослідженнях використовуються різні підходи, зокрема логістична регресія для класифікації ненадійних вузлів у мережах із втратами [17], дерева рішень для виявлення зловмисних дій [18], а також кластеризація K-середніх і регресійні моделі для поділу вузлів на надійні та ненадійні [19]. Перспективним напрямом є також застосування глибоких нейронних мереж для адаптивного управління довірою в мережах Промислового Інтернету речей, що забезпечує виявлення нових типів атак [20]. У роботі [21] було запропоновано використати метод LSTM (Long short-term memory, довга короткочасна пам'ять) для визначення порогу довіри на основі змін у поведінці та алгоритм багатоатрибутної оцінки для обчислення значень рівня довіри.

Таким чином, хоча на сьогодні існує значна кількість досліджень у сфері оцінювання довіри до пристроїв Інтернету речей, недостатня увага приділяється застосуванню гібридних методів, що поєднують декілька технологій обчислювального інтелекту та дозволяють використати їхні взаємні переваги для підвищення точності, що і зумовлює необхідність даного дослідження.

Постановка завдання. Метою статті є дослідження гібридного інтелектуального підходу до оцінювання індексу довіри в мережах Інтернету речей на основі технологій обчислювального інтелекту, зокрема нечіткої логіки та еволюційних алгоритмів.

Для досягнення мети пропонується розробити нечіткий контролер для оцінювання індексу довіри до пристроїв Інтернету речей. Для цього спочатку необхідно сформовано відповідні математичні моделі, що описують роботу контролера та процес нечіткого висновку, а також оптиміза-

цію його параметрів за допомогою еволюційних алгоритмів. Для дослідження ефективності, оптимізації та валідації запропонованої моделі буде використано середовище MATLAB.

Виклад основного матеріалу. ***Розроблення нечіткого контролера для оцінювання індексу довіри до пристроїв IoT.*** У даному дослідженні розробляється нечіткий контролер, який призначений для обчислення індексу довіри до пристроїв Інтернету речей.

Вхідні змінні розробленої моделі нечіткого контролера представляють собою кількісні характеристики поведінки вузла мережі IoT, сформовані на основі відповідних мережевих ознак датасету NSL-KDD. Цей датасет представляє собою загальнодоступний набір мережевих даних, містить характеристики мережевих з'єднань нормальної та аномальної поведінки, і широко використовується для дослідження методів виявлення атак і забезпечення безпеки в телекомунікаційних мережах.

Отже, у розробленому нечіткому контролері перша вхідна величина E (error) відображає частку з'єднань, під час яких були виявлені помилки у мережевих запитах. Високе значення цього показника свідчить про можливі ознаки сканування портів або спроби атаки типу флуд. Таким чином, даний показник є індикатором потенційно шкідливої активності в мережі.

Друга вхідна величина нечіткого контролера C (count) відображає кількість мережевих з'єднань, встановлених до хоста протягом останніх двох секунд. Високе значення цього параметра може свідчити про підозрілу активність, наприклад сканування або спроби перевантаження сервера. Цей показник допомагає виявляти аномальні патерни трафіку, характерні для атак.

Третя вхідна величина нечіткого контролера B (bytes) відображає кількість байтів, переданих від джерела до призначення під час мережевого з'єднання. Високі значення цього параметра можуть свідчити про інтенсивну передачу даних, що є типовим як для легітимних сервісів, так і для певних типів атак. Цей показник дозволяє аналізувати обсяг трафіку та виявляти нетипові або підозрілі патерни поведінки.

Вихідна величина нечіткого контролера – індекс довіри T (trust index) –відображає рівень надійності або безпечності пристрою в мережі Інтернету речей. Вона формується на основі аналізу вхідних показників і дозволяє визначати, наскільки можна покладатися на пристрій у рамках безпечності виконання його функцій. Значення індексу довіри можна використовувати для прийняття рішень щодо доступу, взаємодії або ізоляції пристрою в мережі.

Розглянемо математичні моделі, які описують функціонування розробленого нечіткого контролера. Позначимо вхідні змінні E, C, B як x_i і припустимо, що кожна з них нормалізована у діапазоні [0, 1], що запобігатиме домінуванню окремих характеристик.

Для опису можливих значень трьох вхідних параметрів використано по три гаусові функції належності, що відповідають лінгвістичним термам малий, середній, великий. Гаусова функція вибрана через її плавну форму та здатність забезпечувати неперервний перехід між станами. Математично кожна така функція належності визначається виразом

$$\mu_{A_{i,j}}(x_i) = \exp\left(-\frac{(x_i - c_{i,j})^2}{2\sigma_{i,j}^2}\right), \qquad (1)$$

де x_i – значення i-ї вхідної величини; $c_{i,j}$ – центр функції належності для терму j на вхідної величини i; $\sigma_{i,j}$ – ширина цієї функції.

Для опису вихідної величини використано п'ять гаусових функцій належності з такими лінгвістичними термами: дуже низький, низький, середній, високий, дуже високий. Вихідні функції належності описуються формулою

$$\mu_{B_k}(y) = \exp\left(-\frac{(y - c_k)^2}{2\sigma_k^2}\right). \qquad (2)$$

Тут параметри c_k та σ_k визначають форму вихідних нечітких множин для k -го терму.

Основою роботи нечіткого контролера є база правил нечіткого виведення. Кожне правило формулюється у вигляді:

$$\text{IF } x_1 \text{ is } A_{1,j_1} \text{ AND } x_2 \text{ is } A_{2,j_2} \text{ AND } x_3 \text{ is } A_{3,j_3} \text{ THEN } y \text{ is } B_k . \qquad (3)$$

Для кожного правила визначається ступінь його активації. Інтенсивність спрацювання правила обчислюється через мінімальний ступінь належності серед його вхідних умов:

$$\alpha_r = \min(\mu_{A_{1,j_1}}(x_1), \mu_{A_{2,j_2}}(x_2), \mu_{A_{3,j_3}}(x_3)) . \qquad (4)$$

Отримане значення α_r представляє собою вагу, з якою дане правило впливає на формування вихідної нечіткої множини. Далі виконується імплікація, яка полягає у відсіченні вихідної функції належності за рівнем активації:

$$\mu_{Y_r}(y) = \min(\alpha_r, \mu_{B_k}(y)) . \qquad (5)$$

На наступному етапі у контролері здійснюється агрегація усіх активованих правил. Агрегована функція належності формуються шляхом максимізації по всіх отриманих часткових вихідних значеннях:

$$\mu_Y(y) = \max_{r=1,\ldots,27} \mu_{Y_r}(y). \quad (6)$$

Останнім етапом є дефазифікація, яка в даному контролері виконується за методом центроїда. Таким чином, дефазифіковане значення індексу довіри розраховується за формулою:

$$y^* = \frac{\int_0^1 y\mu_Y(y)dy}{\int_0^1 \mu_Y(y)dy}. \quad (7)$$

Вихідне значення є якісною оцінкою довіри, що використовується у прийнятті рішень щодо доступу, взаємодії або ізоляції пристрою в мережі IoT.

Оптимізація нечіткого контролера. Оскільки робота нечіткого контролера значною мірою залежить від правильності та релевантності функцій належності та бази правил, з метою підвищення точності його функціонування було виконано оптимізацію розробленої моделі шляхом застосування еволюційних алгоритмів, а саме – генетичного та рою частинок. Отже, об'єктом оптимізації був набір параметрів нечіткого контролера, зокрема центри та ширини гаусових функцій належності для кожної вхідної та вихідної змінної, а також коефіцієнти бази правил.

Спочатку була здійснена оптимізація параметрів нечіткого контролера за допомогою генетичного алгоритму (ГА). У даному випадку кожна хромосома ГА кодує повний набір значень центрів і стандартних відхилень гаусових функцій належності для всіх вхідних та вихідної змінних. Крім того хромосома також кодує структуру нечітких правил. Хромосома може бути представлена як вектор виду:

$$\mathbf{P} = [\theta_{MF}, \theta_{rules}], \quad (8)$$

де θ_{MF} містить параметри c і σ усіх гаусових фукнцій, θ_{rules} – кодування бази правил.

Оскільки розроблений нечіткий контролер містить 27 правил, то база правил кодується вектором:

$$\mathbf{R} = r_1, r_2, \ldots, r_{27}. \quad (9)$$

Розгорнута формулу хромосоми, що містить усі параметри функцій належності та всі правила виглядає так:

$$\mathbf{P} = [c_{E,1}, \sigma_{E,1}, c_{E,2}, \sigma_{E,2}, c_{E,3}, \sigma_{E,3}, c_{C,1}, \sigma_{C,1}, c_{C,2}, \sigma_{C,2}, c_{C,3}, \sigma_{C,3}, c_{B,1}, \sigma_{B,1}, c_{B,2}, \sigma_{B,2}, c_{B,3}, \sigma_{B,3}, c_{T,1}, \sigma_{T,1}, c_{T,2}, \sigma_{T,2}, c_{T,3}, \sigma_{T,3}, c_{T,4}, \sigma_{T,4}, c_{T,5}, \sigma_{T,5}, r_1, r_2, \ldots, r_{27}]. \quad (10)$$

Таким чином, у процесі оптимізації нечіткого контролера не лише налаштовується форма його функцій належності, але й можлива реконфігурація логіки його роботи.

Оцінювання якості кожної хромосоми здійснюється за допомогою функції пристосованості. У даному дослідженні якість контролера визначається через середньоквадратичну помилку між отриманими значеннями і значеннями індексу довіри з навчальної вибірки:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(y_i^{pred} - y_i^{true}\right)^2}. \quad (11)$$

Основною метою оптимізації є мінімізація цієї метрики, а отже, пошук оптимального набору параметрів:

$$\theta^* = \arg\min_\theta RMSE(\theta). \quad (12)$$

Тут ГА здійснює еволюційний пошук оптимальної конфігурації параметрів, що дозволяє ефективно досліджувати простір рішень і уникати локальних мінімумів, тобто вионується глобальний пошук оптимальних параметрів.

У даній роботі також досліджено застосування ще одного методу еволюційної оптимізації – методу рою частинок (МРЧ). Кожна частинка репрезентує один можливий набір параметрів нечіткого контролера. Як і в генетичному алгоритмі, параметри кодуються як набір значень центрів та стандартних відхилень гаусових функцій належності, а також коефіцієнтів бази правил. Нехай $\mathbf{S}_i(t)$ позначає позицію і-тої частинки на ітерації t. Вона містить повний набір оптимізованих параметрів:

$$\mathbf{S}_i(t) = [\theta_{MF}(t), \theta_{rules}(t)]. \quad (13)$$

Кожна частинка також оцінюється за функцією пристосованості RMSE. МРЧ прагне знайти таке положення частинок, яке мінімізує RMSE, тобто:

$$\theta^* = \arg\min_\theta RMSE(\theta). \quad (14)$$

Таким чином, МРЧ поступово коригує параметри нечіткого контролера, що дозволяє швидше знаходити оптимальні рішення.

Комп'ютерне моделювання. Для дослідження розробленого нечіткого контролера для оцінювання індексу довіри в Інтернеті речей було використано програмний пакет MATLAB, який зарекомендував себе як один із найпотужніших інструментів для моделювання як інтелектуальних так і телекомунікаціних систем.

Загальний вигляд запропонованого нечіткого контролера в середовищі MATLAB подано на рис. 1,а. що ілюструє структуру моделі.

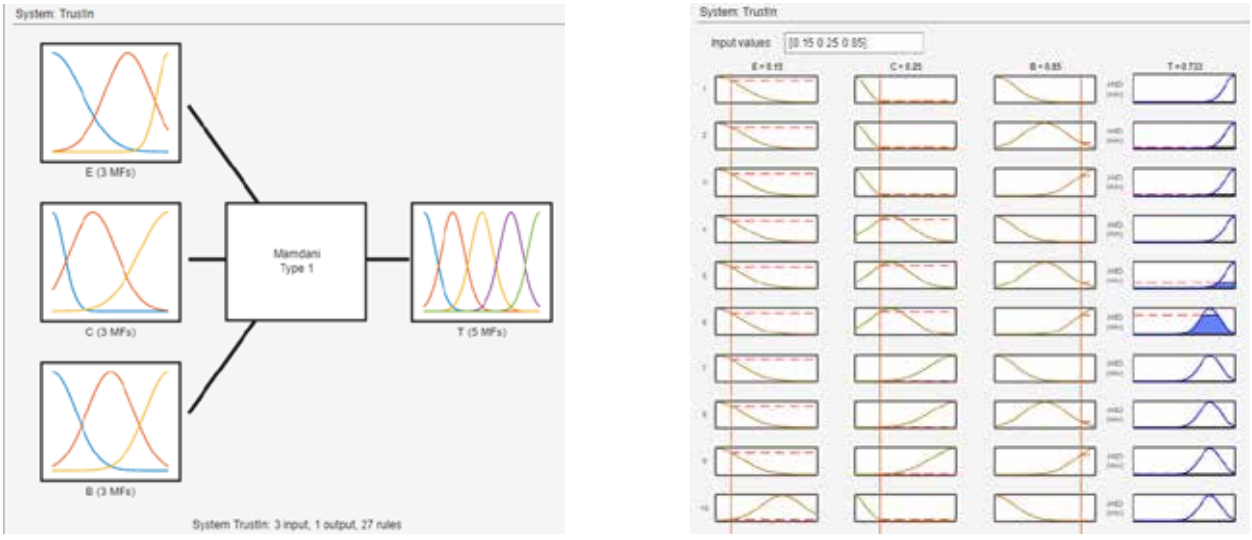
У процесі моделювання нечіткого контролера у програмі MATLAB спочатку були введені вхідні та вихідні змінні із відповідним визначенням діапазонів значень та параметризацією функцій належності для кожної з них. На цьому етапі було проведено ретельне налаштування гаусових функцій належності, що визначали лінгвістичні терми для вхідних та вихідної змінних. Після цього було створено повну базу нечітких правил, що встановлює логічні відповідності між різними комбінаціями вхідних даних та бажаною реакцією контролера. Формування цієї бази передбачало врахування поведінкових закономірностей трафіка в Інтернеті речей. Наступним кроком стало налаштування методів агрегування, імплікації та дефаззифікації відповідно до обраної моделі контролера.

Для дослідження точності роботи розробленого нечіткого контролера була проведена серія комп'ютерних експериментів у програмному середовищі MATLAB. Експерименти передбачали моделювання поведінки контролера за різних комбінацій значень вхідних параметрів, що дозволило охопити широкий спектр можливих сценаріїв функціонування мережі IoT. На рис. 1,б. подано приклад результату моделювання роботи розробленого контролера.

Метою оптимізації є мінімізація середньоквадратичної помилки між вихідними значеннями індексу довіри, згенерованими контролером, та еталонними даними, що дозволить підвищити точність розробленої моделі.

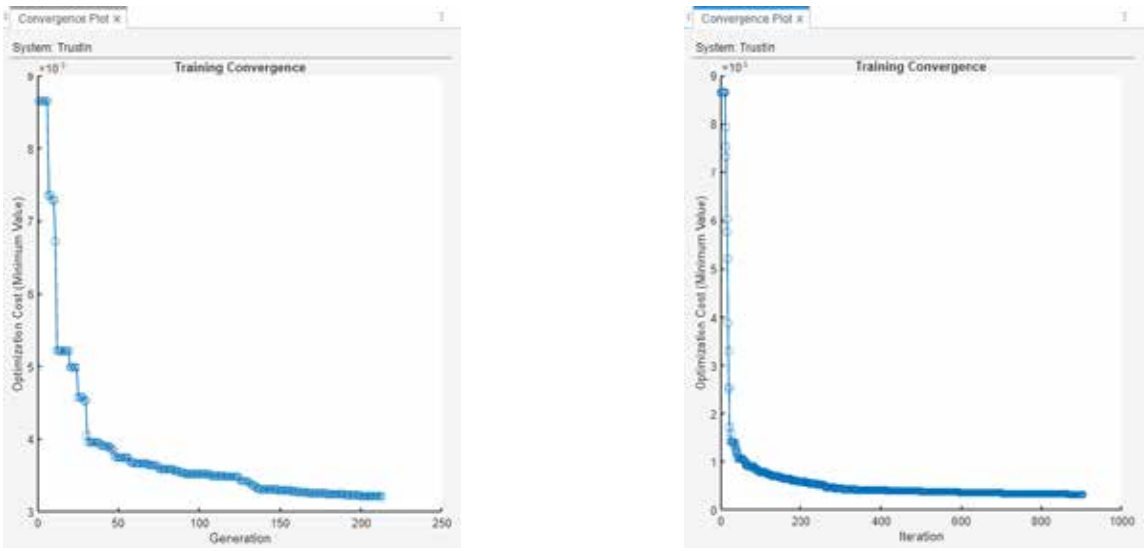
Спочатку було виконано оптимізацію параметрів нечіткого контролера за допомогою ГА. Графік, поданий на рис. 2,а та отриманий у середовищі MATLAB, відображає процес збіжності навчання під час оптимізації параметрів контролера за допомогою ГА. По осі абсцис на графіку відкладено номер покоління, тоді як по осі ординат представлено значення функції пристосованості, зокрема середньоквадратичної похибки RMSE. Зменшення значення RMSE зі збільшенням кількості поколінь свідчить про поступове покращення якості налаштування параметрів контролера. Наступним етапом дослідження був пошук оптимальних параметрів нечіткого контролера за допомогою методу рою частинок. Отриманий у середовищі MATLAB (рис. 2,б) графік оптимізації відображає динаміку збіжності алгоритму МРЧ у процесі мінімізації функції пристосованості. Крива збіжності поступово вирівнюється та стабілізується, що вказує на досягнення глобально найкращого або близького до нього розв'язку задачі оптимізації.

З метою перевірки точності розробленого нечіткого контролера у оцінюванні індексу довіри до пристроїв було здійснено валідацію всіх трьох моделей на основі незалежних тестових даних. Процедура валідації передбачала визначення вихідних значень контролера для кожного прикладу з тестового набору та подальше порівняння їх з еталонними значеннями, отриманими під час попереднього аналізу даних. Отримані у ході



а б

Рис. 1. Нечіткий контролер в програмі MATLAB: а – загальний вигляд; б – результат роботи



а б

Рис. 2. Процес оптимізації параметрів нечіткого контролера: а – за допомогою генетичного алгоритму; б – за допомогою методу рою частинок

графічні залежності ілюструють співвідношення між еталонними та змодельованими значеннями індексу довіри (рис. 3). На цих графіках було проведено візуальне зіставлення, яке дозволяє визначити наявність суттєвих розбіжностей між двома множинами даних.

Отримані результати свідчать, що для базової моделі нечіткого контролера відхилення між фактичними та прогнозованими значеннями є незначними, що підтверджує її здатність правильно визначати значення індексу довіри. Разом із тим, застосування генетичного алгоритму для оптимізації параметрів нечіткого контролера забезпечило помітне покращення точності, що відображено у більш тісному узгодженні між змодельованими та еталонними даними. Найкращі результати були отримані для моделі, оптимізованої методом рою частинок: вона демонструє мінімальні відхилення, що свідчить про високу ефективність МРЧ у задачах глобальної оптимізації нечітких систем. Таким чином, проведена валідація підтверджує працездатність розробленого контролера та доцільність подальшого використання його оптимізованої моделі як складової частини архітектури системи оцінювання довіри в IoT.

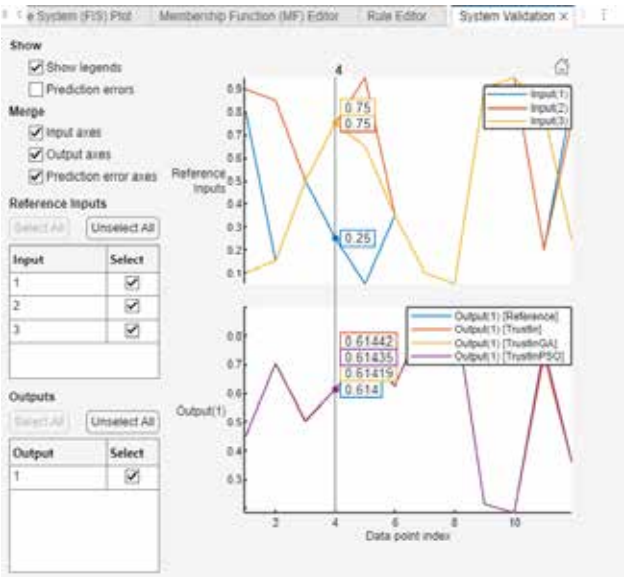


Рис. 3. Результати валідації роботи нечіткого контролера

Висновки. У представленій статті було розроблено, оптимізовано та досліджено нечіткий контролер для оцінювання індексу довіри до пристроїв в мережах Інтернету речей. Побудована модель контролера на основі системи Мамдані з трьома вхідними змінними та однією вихідною змінною продемонструвала здатність репрезентувати поведінку процесів систем безпеки та забезпечувати відображення взаємозв'язків між параметрами трафіку мереж IoT.

Проведені комп'ютерні експерименти у середовищі MATLAB підтвердили коректність структури функцій належності та побудованої бази нечітких правил. Валідація на тестових даних продемонструвала задовільний рівень точності моделі.

Для підвищення точності оцінювання було виконано оптимізацію параметрів розробленого нечіткого контролера за допомогою еволюційних алгоритмів.

Застосування генетичного алгоритму дозволило налаштувати параметри функцій належності та коефіцієнти правил, що привело до суттєвого зменшення середньоквадратичної помилки. Отримані результати продемонстрували помітне підвищення точності оцінювання довіри порівняно з неоптимізованою моделлю. Подальша оптимізація за допомогою методу рою частинок забезпечила ще кращі показники – МРЧ-оптимізований контролер досяг найменших відхилень від еталонних даних, забезпечивши найвищу точність та стабільність роботи під час валідації.

Узагальнюючи результати дослідження, можна зробити висновок, що використання нечіткої логіки у поєднанні з еволюційними методами оптимізації є ефективним підходом для розв'язання задачі оцінювання індексу довіри в Інтернеті речей. Розроблений контролер може бути використаний як складова інтелектуальних систем безпеки IoT, забезпечуючи високоточне прийняття рішень щодо безпечності та надійності конкретного пристрою.

Отримані результати свідчать про доцільність використання технологій обчислювального інтелекту, зокрема нечітких контролерів та еволюційних алгоритмів, для забезпечення безпеки та надійності IoT-пристроїв.

Подальші дослідження можуть бути спрямовані на розширення бази правил, врахування додаткових характеристик мережевого трафіку та інтеграцію нечіткого контролера з методами машинного навчання.

Список літератури:

1. Din I. Ud, Bano A., Awan K. A., Almogren A., Altameem A., Guizani M. LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things. *IEEE Internet of Things Journal,* 2023. Vol. 10. No. 4. Pp. 2776–2783. DOI: https://doi.org/10.1109/jiot.2021.3081422

2. Chen J., Tian Z., Cui X., Yin L., Wang X. Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing,* 2018. Vol. 10. No. 8. Pp. 3099–3107. DOI: https://doi.org/10.1007/s12652-018-0887-z

3. Hamdani S. W. A., Khan A. W., Iltaf N., Bangash J. I., Bangash Y. A., Khan A. Dynamic distributed trust management scheme for the Internet of Things. Turkish *Journal of Electrical Engineering and Computer Sciences*, 2021. Vol. 29. No. 2. Pp. 796–815, 2021. DOI: https://doi.org/https://doi.org/10.3906/elk-2003-5

4. Liu Y., Zhang C., Yan Y., Zhou X., Tian Z., Zhang J. A Semi-Centralized Trust Management Model Based on Blockchain for Data Exchange in IoT System. *IEEE Transactions on Services Computing*, 2023. Vol. 16. No. 2. Pp. 858–871. DOI: https://doi.org/10.1109/tsc.2022.3181668

5. Alruwaythi M., Nygard K. E. Fuzzy Logic Approach Based on User behavior Trust in Cloud Security. 2019 IEEE International Conference on Electro Information Technology (EIT). *Brookings,* SD, USA, 20-22 May 2019. Pp. 1–6. DOI: https://doi.org/10.1109/eit.2019.8834173

6. Alshehri M. D., Hussain F. K. A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). *Computing*, 2018. Vol. 101, No. 7. Pp. 791–818. DOI: https://doi.org/10.1007/s00607-018-0685-7

7. Singh P., Kaur A., Batth R. S., Aujla G. S., Masud M. Service Versus Protection: A Bayesian Learning Approach for Trust Provisioning in Edge of Things Environment. *IEEE Internet of Things Journal*, 2022. Vol. 9. No. 22. Pp. 22061–22070. DOI: https://doi.org/10.1109/jiot.2021.3082272

8. Prathapchandran K., Janani T. A Trust-Based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression. *Journal of Physics: Conference Series,* 2021. Vol. 1850. No. 1. Pp. 012031. DOI: https://doi.org/10.1088/1742-6596/1850/1/012031

9. Kannimuthu P., Thangamuthu J. Decision Tree Trust (DTTrust)-Based Authentication Mechanism to Secure RPL Routing Protocol on Internet of Battlefield Thing (IoBT). *International Journal of Business Data Communications and Networking*, 2021. Vol. 17. No. 1. Pp. 1–24. DOI: https://doi.org/10.4018/ijbdcn.2021010101

10. Liu L., Xu X., Liu Y., Ma Z., Peng J. A Detection Framework Against CPMA Attack Based on Trust Evaluation and Machine Learning in IoT Network. *IEEE Internet of Things Journal,* 2021. Vol. 8. No. 20. Pp. 15249–15258. DOI: https://doi.org/10.1109/jiot.2020.3047642

11. Hassan M. M., Hassan Md. R., Huda S., V. H. C. de Albuquerque. A Robust Deep-Learning-Enabled Trust-Boundary Protection for Adversarial Industrial IoT Environment. *IEEE Internet of Things Journal*, 2021. Vol. 8. No. 12. Pp. 9611–9621. DOI: https://doi.org/10.1109/jiot.2020.3019225

12. Alghofaili Y., Rassam M. A. A Trust Management Model for IoT Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique. *Sensors*, 2022. Vol. 22. No. 2. Article 634. DOI: https://doi.org/10.3390/s22020634

Semenova O.O., Voitsekhovska O.O., Dzhus A.V., Kuzniak V.P. DEVELOPMENT AND OPTIMIZATION OF A FUZZY CONTROLLER FOR ESTIMATING THE TRUST INDEX IN THE INTERNET OF THINGS

The paper proposes an approach to evaluating the trust index of devices in Internet of Things (IoT) networks based on computational intelligence, specifically fuzzy logic and evolutionary optimization. The relevance of the study is driven by the rapid growth in the number of IoT devices operating in potentially complex and hostile environments, where traditional security mechanisms and trust assessment methods are often insufficient. Trust evaluation is considered a crucial mechanism for enhancing the reliability and security of IoT networks. The proposed model is based on a Mamdani-type fuzzy controller. It employs three input variables derived from network-related features of the NSL-KDD dataset and one output variable representing the trust index of an IoT device. Gaussian membership functions are used for all input and output variables, ensuring smooth inference and robustness to data uncertainty. The rule base consists of a complete set of logical rules that formalize expert knowledge regarding the behavior of trusted and malicious nodes. The developed fuzzy controller generates a trust metric that enables the classification of IoT devices as reliable, potentially dangerous, or malicious. To improve the accuracy of trust index evaluation, the parameters of the proposed fuzzy controller were optimized using a genetic algorithm and particle swarm optimization. Model performance was assessed using the root mean square error between the predicted and reference trust index values. The results of computer simulations confirm that the optimized fuzzy controllers significantly outperform the baseline model in terms of accuracy, with the particle swarm optimization approach demonstrating the highest effectiveness. The proposed model can be integrated into IoT security systems to enhance the reliability of interactions among devices.

Keywords: *Internet of Things, telecommunications, security, trust assessment, fuzzy controller, genetic algorithm, particle swarm, optimization.*

Дата першого надходження статті до видання: 12.01.2026
Дата прийняття статті до друку після рецензування: 09.02.2026
Дата публікації (оприлюднення) статті: 08.04.2026