УДК 004.7:004.056:627.7.05 DOI: 10.31673/2412-4338.2026.019021

Волокита Артем Миколайович
К. т. н, доцент, в.о.зав каф. ОТ
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ
ORCID ID 0000-0001-9069-5544
artem.volokita@kpi.ua

Меленчуков Микита Євгенович
Аспірант, асистент каф. ОТ
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ
ORCID ID 0009-0005-6615-4306
melenchukov.nikita@gmail.com

МЕТОД ДИНАМІЧНОЇ ОЦІНКИ ДОВІРИ ЗА ДОПОМОГОЮ МОДИФІКОВАНОГО ГІСТЕРЕЗИСУ У РОЯХ БПЛА

Анотація. *У статті досліджується проблема стабільності та безпеки функціонування мобільних комплексів, зокрема роїв безпілотних літальних апаратів (БПЛА), в умовах маніпуляцій даними. Децентралізовані мережі вразливі до On-Off атак, під час яких зловмисний вузол навмисно коливає рейтинг довіри навколо межі відключення. Це викликає дестабілізуючий ефект «миготіння» (flapping) станів мережі, що призводить до лавиноподібного зростання трафіку. Аналіз публікацій показує, що існуючі рішення концентруються на глобальних алгоритмах обчислення рівня загроз, залишаючи невирішеним питання стабілізації довіри на локальному рівні (рівні окремого вузла). Метою роботи є розробка математичної моделі, яка виступає базисом методу динамічного оцінювання довіри: механізму безперервного оновлення коефіцієнта довіри та постійної регуляції ефективної ваги вузлів за допомогою модифікованого гістерезису. Основний матеріал описує розроблений локальний модуль стабілізації, який діє як фільтр для зовнішніх адаптивних порогів. Наукова новизна підходу полягає в оригінальному застосуванні механізму гістерезису для завдань динамічної оцінки довіри, де він адаптований для умов, коли на його вхід подається змінний поріг безпеки. Математичний апарат управління довірою базується на експоненційному згладжуванні (EWMA) та гістерезисі. Введено рахунок тривалості відхилення і бінарний індикатор карантину, який ізолює вузол від прийняття рішень. Запропонована неперервна кусочно-лінійна функція деградації довіри забезпечує асиметричне штрафування зловмисника, нівелюючи спроби швидкого відновлення рейтингу. Для верифікації моделі проведено ізольоване імітаційне моделювання поведінки вузла за умов On-Off атаки. Результати доводять здатність модифікованого гістерезису самостійно блокувати маніпуляції порушника, повністю усуваючи ефект «миготіння». Висновки підтверджують, що проста мінливість довіри є вразливою без апарату стабілізації. Запропонована модель успішно перетворює нестабільну поведінку агентів у безпечну, безперервно керовану ефективну вагу, придатну для обчислення безпечного консенсусу в БПЛА. Перспективами досліджень є оптимізація взаємодії створеної локальної моделі з глобальними нейромережевими модулями у реальному часі.*

Ключові слова: *розподілені системи, БПЛА, динамічна довіра, модифікований гістерезис, безпека розподілених систем, On-Off атаки, безперервне оновлення довіри*

Volokyta Artem
PhD. Sc., associate professor, acting head of computer engineering department
National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute", Kyiv
ORCID ID 0000-0001-9069-5544
artem.volokita@kpi.ua

Melenchukov Mykyta
PhD student, assistant at the computer engineering department
National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute", Kyiv
ORCID ID 0009-0005-6615-4306
melenchukov.nikita@gmail.com

DYNAMIC TRUST ASSESSMENT METHOD USING MODIFIED HYSTERESIS IN UAV SWARMS

Abstract. *The article investigates the problem of stability and security in the functioning of mobile complexes, particularly unmanned aerial vehicle (UAV) swarms, under conditions of data manipulation. Decentralized networks are vulnerable to On-Off attacks, during which a malicious node intentionally fluctuates its trust rating around the disconnection threshold. This causes a destabilizing effect of network state "flapping", leading to an avalanche-like increase in traffic. An analysis of publications shows that existing solutions concentrate on global algorithms for calculating threat levels, leaving the issue of trust stabilization at the local (node) level unresolved. The objective of the work is to develop a mathematical model that serves as the basis for a dynamic trust assessment method: a mechanism for continuous updating of the trust coefficient and constant regulation of the nodes' effective weight using modified hysteresis. The main material describes the developed local stabilization module, which acts as a filter for external adaptive thresholds. The scientific novelty of the approach lies in the original application of the hysteresis mechanism for dynamic trust assessment tasks, where it is adapted for conditions in which a variable security threshold is fed to its input. The mathematical apparatus for trust management is based on exponential smoothing (EWMA) and hysteresis. The deviation duration counter and a binary quarantine indicator, which isolates the node from decision-making, are introduced. The proposed continuous piecewise-linear trust degradation function provides asymmetric penalization of the attacker, neutralizing attempts at rapid rating recovery. To verify the model, an isolated simulation of the node's behavior under an On-Off attack was conducted. The results prove the ability of modified hysteresis to independently block the violator's manipulations, eliminating the "flapping" effect. The conclusions confirm that simple trust fluidity is vulnerable without a stabilization apparatus. The proposed model successfully transforms the unstable behavior of agents into a secure, continuously managed effective weight suitable for calculating a secure consensus in UAV swarms. Prospects for future research involve optimizing the real-time interaction of the created local model with global neural network models.*

Keywords: *distributed systems, UAVs, dynamic trust, modified hysteresis, cybersecurity, On-Off attacks, continuous trust update*

1. Вступ

Останніми роками спостерігається стрімкий розвиток технологій безпілотних літальних апаратів (БПЛА) та їх організаційний перехід від ізольованого використання до парадигми колаборативних роїв (Swarm) та літаючих ad-hoc мереж (FANET) [1]. Такі децентралізовані інформаційно-керуючі системи відкривають принципово нові можливості для виконання складних колективних завдань в умовах відсутності стабільної або довіреної наземної інфраструктури зв'язку [2]. Вони набули широкого застосування в моніторингу навколишнього середовища, пошуково-рятувальних операціях, доставці вантажів та військовій розвідці. Ключовою перевагою ройового інтелекту є його здатність до швидкої самоорганізації, гнучка масштабованість та висока відмовостійкість [3]. Навіть у разі фізичної втрати чи критичної відмови частини апаратів, рій здатний динамічно перерозподілити ролі та успішно продовжити виконання спільної місії.

Однак високий рівень автономності, самоорганізації та децентралізація управління створюють нові нетривіальні виклики у сфері кібербезпеки [4]. У традиційних ієрархічних мережах безпека зазвичай гарантується централізованими серверами автентифікації та жорсткою криптографією, що діє як захист периметра. У роях БПЛА кожен вузол (агент) виступає як рівноправний учасник мережі, який самостійно маршрутизує дані, збирає спостереження та бере участь у колективному прийнятті рішень (алгоритмах консенсусу) [5]. Якщо зловмисник отримує програмний чи апаратний доступ до управління одним із БПЛА (або захоплює його в полон), він автоматично стає авторизованим «внутрішнім» учасником мережі з легітимними ключами шифрування [6]. За таких умов класичні методи криптографічного захисту виявляються безсилими, оскільки порушник подолав зовнішній периметр безпеки [7].

Це зумовлює гостру необхідність зміни парадигми безпеки – переходу до безперервного моніторингу поведінки кожного агента зсередини рою [8]. Для цього застосовуються системи управління довірою (Trust Management), у яких кожен дрон оцінює надійність своїх сусідів на основі аналізу їхніх дій та інформаційного обміну [9]. Тим не менш, реалізація надійної оцінки довіри в середовищі без фіксованої топології стикається із проблемою інтелектуальних кібератак, які використовують недоліки самих алгоритмів формування довірчого рейтингу для його маніпулювання [10].

2. Постановка проблеми

Сучасні інформаційно-керуючі комплекси, побудовані на базі мобільних автономних агентів (зокрема, рої БПЛА та літаючі ad-hoc мережі – FANET), функціонують в умовах відсутності фіксованої інфраструктури, що вимагає постійної адаптації до змін топології. Існуючі алгоритми безпеки часто

покладаються на жорсткі пороги оцінки довіри, а спроби їх адаптації залишаються складними в реалізації [11].

Дослідження показують, що проста «мінливість» (динаміка) показника довіри у часі не вирішує проблему надійності, а навпаки, створює вразливість до On-Off атак [12]. Зловмисник може навмисно коливати свій рейтинг навколо межі відключення, викликаючи ефект «миготіння» вузлів у системі (flapping) [13]. Це призводить до лавиноподібного зростання службового трафіку для постійної реконфігурації кворуму.

3. Аналіз останніх досліджень і публікацій

Питання організації безпечної взаємодії в децентралізованих мережах БПЛА активно досліджуються у сучасній літературі. Значна частина робіт присвячена побудові безпечного середовища на базі концепції Zero Trust та гібридних криптографічних протоколів [8, 9]. Проте ці методи ефективні переважно для захисту від зовнішніх зловмисників і не вирішують проблему внутрішніх скомпрометованих вузлів. Тому фокус досліджень змістився у бік систем управління довірою (Trust Management) [10].

Більшість сучасних підходів до управління довірою зосереджується на застосуванні статичних рейтингів або складних адаптивних порогів [11]. Окремим викликом залишається виявлення навмисних маніпуляцій, зокрема On-Off атак, для яких пропонуються методи аналізу варіативності поведінки вузлів [12]. Водночас існуючі адаптивні методи найчастіше пропонують глобальні (загальномережеві) алгоритми обчислення загального рівня загроз, зокрема на базі нейромереж [14] або комбінованих моделей консенсусу [13]. Хоча існують рішення для згладжування метрик довіри на базі методів експоненційного прогнозування [15], вони розглядаються переважно ізольовано та не забезпечують захисту від ефекту «миготіння». Таким чином, існуючі системи залишають поза увагою математичні механізми неперервної стабілізації довіри на локальному рівні кожного окремого вузла.

Невирішеною частиною загальної проблеми залишається розробка стійкого математичного апарату, здатного стабілізувати показники довіри при динамічно змінних адаптивних порогах та ефективно перешкоджати маніпуляціям типу On-Off без надмірного обчислювального навантаження.

4. Мета і задачі дослідження

Метою статті є розробка математичної моделі, яка виступає базисом методу динамічного оцінювання довіри: механізму безперервного оновлення коефіцієнта довіри та постійної регуляції ефективної ваги репутації вузлів за допомогою модифікованого гістерезису.

5. Результати дослідження

5.1 Модель системи та архітектура динамічної оцінки

У пропонованій архітектурі динамічне оцінювання розглядається як дворівневий комплекс: генерація первинного сигналу загроз (глобальний рівень мережі) та управління індивідуальною вагою вузла (локальний рівень) [13].

Миттєве значення довіри $x_{i(t)}$ (або базове спостереження $s_{i(t)}$) може генеруватися зовнішнім інтелектуальним модулем (наприклад, нейромережею), який також здатний розраховувати адаптивні пороги безпеки (глобальну θ) залежно від поточного рівня загроз [14]. Архітектура глобального рівня (генерації загального сигналу) виходить за межі цього дослідження.

Дана робота зосереджена на **локальному модулі управління** – модифікованому гістерезисі. Він виступає фільтром, який приймає зовнішні пороги безпеки та «шумні» показники $x_{i(t)}$, здійснюючи постійну регуляцію ваги кожного агента.

5.2 Математична модель безперервного оновлення довіри та регуляції ваги

Аби вирішити проблему одноразової оцінки, застосовується математичний апарат управління сигналом довіри. Безперервне оновлення довіри дрона i у момент часу t виконується за правилом експоненційного згладжування (EWMA), що дозволяє плавно враховувати історичний контекст [15]:

$$trust_i(t) = \alpha s_i(t) + (1-\alpha) trust_i(t-1) \#(1)$$

де $s_i(t)$ – нове спостереження, $\alpha \in (0,1]$ – коефіцієнт чутливості.

На відміну від звичайного гістерезису, який лише перемикає стани «увімкнено/вимкнено», модифікований механізм запроваджує постійну регуляцію ваги через введення цільових порогів (які

можуть задаватися зовнішньою системою): τ_{warn} (поріг попередження) та $\tau_{quarantine}$ (поріг глибокого недовіри, $\tau_{quarantine} < \tau_{warn}$).

Щоб уникнути «миготіння» станів, реалізується рахунок тривалості відхилення $c_i(t)$ та бінарний індикатор карантину $q_i(t) \in \{0,1\}$:

$$c_i(t) = \{c_i(t-1) + 1, \text{якщо } trust_i(t) < \tau_{quarantine} \ (0, c_i(t-1) - 1) \text{ , інакше } \#(2)$$

Карантин вмикається при стійкому відхиленні не менше ніж протягом m кроків ($q_i(t) = 1$, якщо $c_i(t) \geq m$). Для повернення з карантину вимагається стабільно висока довіра протягом r послідовних кроків вище порогу $\tau_{release}$.

Завершує метод динамічного оцінювання формула композиції стану карантину та неперервної функції довіри, яка математично закріплює постійну регуляцію ефективної ваги репутації $\widetilde{\omega_i}(t)$:

$$\widetilde{\omega_i}(t) = \Big(1 - q_i(t)\Big) \cdot f\big(trust_i(t)\big) \#(3)$$

де $f(x)$ – безперервна кусочно-лінійна функція деградації довіри:

$$f(x) = \{\ 0, \quad x\ \leq \tau\_\{quarantine\}\ \frac{\tau_{warn}}{\tau_{warn} - \tau_{quarantine}}\big(x - \tau_{quarantine}\big), \tau_{quarantine} < x < \tau_{warn}\ x, \quad x \geq \tau_{warn}\ \#(4)$$

Такий апарат робить динамічну оцінку асиметричною: вузол плавно втрачає вагу при відхиленнях, але «затримується» на нулі (через q_i) при спробі різко відновити статус.

5.3 Моделювання та експериментальні результати

Для доведення ефективності запропонованого математичного апарату гістерезису як самостійного фільтра, було розроблено програмний симулятор дискретного часу та проведено ізольоване імітаційне моделювання поведінки окремого вузла під час On-Off атаки.

Згідно з принципами ізоляції компонентів, динамічна зміна зовнішніх порогів безпеки була навмисно зафіксована у найвразливішій (крайовій) позиції, а серія спостережень генерувалася штучно для відтворення агресивної моделі порушника. Це дозволило на рівні окремого ізольованого вузла довести внесок виключно розробленого механізму гістерезису у стабілізацію системи, виключивши вплив зовнішніх систем.

Особливу увагу під час тестування було приділено трьом ключовим етапам:

1. періоду початкової нормальної активності, де вузол накопичує довіру;
2. фазі різкого падіння якості даних (початок On-Off маніпуляції);
3. спробам порушника швидко відновити свій статус короткими «сплесками» коректної поведінки.

На графіку (рис. 1), що послідовно відображає ці три етапи моделювання, поведінка базової системи звичайного відключення (без гістерезису) демонструє некеровану динаміку – хаотичні стрибки ефективної ваги між 0 та 1, що викликає дестабілізуюче «миготіння» (flapping).

Натомість використання розробленого алгоритму зумовлює суворе асиметричне штрафування: при падінні $trust(t)$ нижче межі, гістерезис повністю обнуляє ефективну вагу порушника (перехід у стан карантину). Навіть при подальших короткочасних позитивних сигналах від зловмисника, швидкого відновлення статусу не відбувається завдяки параметру інерції r, який вимагає тривалої та стабільної зразкової поведінки для зняття блокування.

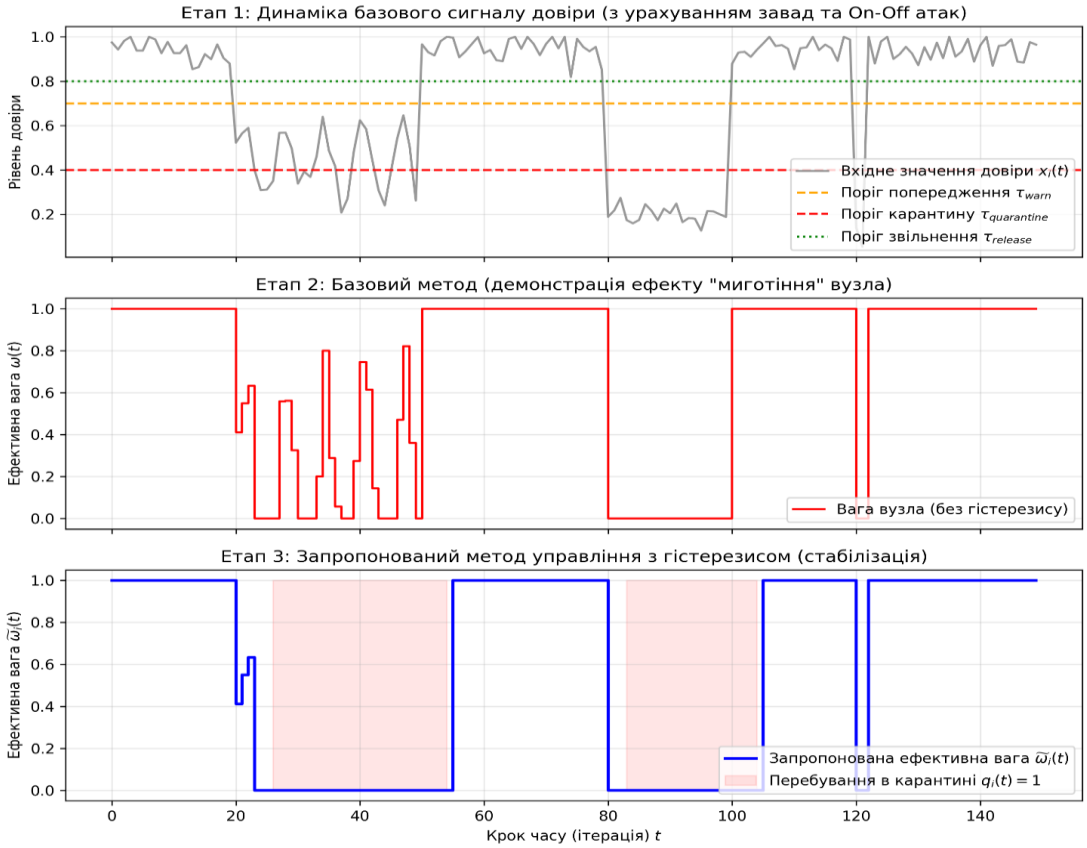

Рис. 1. Результати імітаційного моделювання: динаміка ваги вузла при On-Off атаці та стабілізація модифікованим гістерезисом

6. Висновки та перспективи подальших досліджень

У статті доведено, що ізольована мінливість (динаміка) метрик довіри без апарату їх стабілізації є вразливою до маніпуляцій і не може вважатися повноцінним методом динамічного оцінювання. Пропонується нова математична модель, яка виступає ядром методу динамічного оцінювання: модифікований гістерезис.

Наукова новизна полягає у специфіці застосування механізму гістерезису в розробленому методі динамічної оцінки довіри: він адаптований для роботи в умовах, коли на його вхід подається змінний адаптивний поріг безпеки, виступаючи для нього локальним фільтром. Це дозволяє реалізувати надійну композицію управління станом вузла та постійної регуляції ваги його репутації. Завдяки згладжуванню (EWMA) забезпечується безперервне оновлення коефіцієнта довіри, а інерційні параметри гістерезису (m та r) гарантують захист від On-Off атак. Метод успішно перетворює нестабільну поведінку агентів (яка може формуватися змінними адаптивними порогами) на безпечну, безперервно керовану ефективну вагу, придатну для обчислення безпечного консенсусу в роях БПЛА.

Перспективами подальших досліджень у даному напрямку є інтеграція розробленої локальної (вузлової) моделі модифікованого гістерезису із глобальними нейромережевими модулями для адаптивного управління динамічними порогами у реальному часі.

Внесок авторів Микита Меленчуков – концептуалізація; розробка математичної моделі та методики; написання програмного забезпечення (симулятора); збір і перевірка емпіричних даних; проведення ізольованого імітаційного моделювання; аналіз джерел та підготовка тексту статті; Артем Волокита – наукове керівництво; формулювання загального напрямку та мети дослідження; валідація отриманих результатів; загальна редакція та рецензування матеріалу статті.

Декларація про штучний інтелект

Під час підготовки цього рукопису автори не використовували технології штучного інтелекту або інші автоматизовані засоби генерації контенту для створення будь-яких структурних елементів статті.

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів та підтверджують, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Adaptive multi-granularity trust management scheme for UAV visual sensor security under adversarial attacks / H. Li et al. Computers & security. 2024. P. 104108. URL: https://doi.org/10.1016/j.cose.2024.104108 (date of access: 23.03.2026).

2. A novel distributed situation awareness consensus approach for UAV swarm systems / X. Hai et al. IEEE transactions on intelligent transportation systems. 2023. P. 1–12. URL: https://doi.org/10.1109/tits.2023.3300871 (date of access: 23.03.2026).

3. Continuous authentication for UAV delivery systems under zero-trust security framework / C. Dong et al. 2022 IEEE international conference on edge computing and communications (EDGE), Barcelona, Spain, 10–16 July 2022. 2022. URL: https://doi.org/10.1109/edge55608.2022.00027 (date of access: 23.03.2026).

4. Deep neural network and zero trust principles for intelligent drone management / S. Q. Abbas et al. 2024 IEEE 9th international conference on engineering technologies and applied sciences (ICETAS), Bahrain, Bahrain, 20–22 November 2024. 2024. P. 1–6. URL: https://doi.org/10.1109/icetas62372.2024.11120042 (date of access: 23.03.2026).

5. Kannan S., Venkataraman R., Ramachandran G. S. On-off attack detection in trust model using intra-daily variability for the IoT. Bulletin of electrical engineering and informatics. 2023. Vol. 12, no. 6. P. 3880–3888. URL: https://doi.org/10.11591/eei.v12i6.6110 (date of access: 23.03.2026).

6. Liao Z., Zhang L., Dong Z. UAV swarm exploration with byzantine fault tolerance. 2021 china automation congress (CAC), Beijing, China, 22–24 October 2021. 2021. URL: https://doi.org/10.1109/cac53003.2021.9727874 (date of access: 23.03.2026).

7. Reputation-Enhanced practical byzantine fault tolerance algorithm for node capture attacks on UAV networks / P. Onukak et al. Discover internet of things. 2025. Vol. 5, no. 1. URL: https://doi.org/10.1007/s43926-025-00164-y (date of access: 23.03.2026).

8. Saffre F., Hildmann H., Anttonen A. Force-Based Self-Organizing MANET/FANET with a UAV Swarm. Future internet. 2023. Vol. 15, no. 9. P. 315. URL: https://doi.org/10.3390/fi15090315 (date of access: 23.03.2026).

9. Sharma J., Mehra P. S. A survey of security challenges and existing prevention methods in FANET. Intelligent data analytics, iot, and blockchain. Boca Raton, 2023. P. 252–262. URL: https://doi.org/10.1201/9781003371380-24 (date of access: 23.03.2026).

10. Singh R. Simulation and evaluation of a hybrid trust–cryptographic protocol for UAV swarm communications. Simulation modelling practice and theory. 2025. P. 103230. URL: https://doi.org/10.1016/j.simpat.2025.103230 (date of access: 23.03.2026).

11. The essential role of cybersecurity in UAV swarm operations / F. M. Khan et al. Unmanned aerial vehicles swarm for protecting smart cities. Berkeley, CA, 2025. P. 403–441. URL: https://doi.org/10.1007/979-8-8688-1047-3_11 (date of access: 23.03.2026).

12. Trust based flying ad-hoc network: a survey / J. Kundu et al. IEEE access. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3419904 (date of access: 23.03.2026).

13. Trust prediction based on grey exponential smoothing method in VANETs / S. Zhang et al. 12th EAI international conference on mobile multimedia communications, mobimedia 2019, 29th - 30th jun 2019, weihai, china, Weihai, People's Republic of China, 29–30 June 2019. 2019. URL: https://doi.org/10.4108/eai.29-6-2019.2282065 (date of access: 23.03.2026).

14. Xie G., Zhou X., Gao J. Adaptive trust threshold model based on reinforcement learning in cooperative spectrum sensing. Sensors. 2023. Vol. 23, no. 10. P. 4751. URL: https://doi.org/10.3390/s23104751 (date of access: 23.03.2026).

15. Zhou S., Zhang G., Meng X. LocTrust: A local and global consensus-combined trust model in MANETs. Peer-to-Peer networking and applications. 2021. Vol. 15, no. 1. P. 355–368. URL: https://doi.org/10.1007/s12083-021-01250-y (date of access: 23.03.2026).

References

1. Adaptive multi-granularity trust management scheme for UAV visual sensor security under adversarial attacks / H. Li et al. Computers & security. 2024. P. 104108. URL: https://doi.org/10.1016/j.cose.2024.104108 (date of access: 23.03.2026).

2. A novel distributed situation awareness consensus approach for UAV swarm systems / X. Hai et al. IEEE transactions on intelligent transportation systems. 2023. P. 1–12. URL: https://doi.org/10.1109/tits.2023.3300871 (date of access: 23.03.2026).

3. Continuous authentication for UAV delivery systems under zero-trust security framework / C. Dong et al. 2022 IEEE international conference on edge computing and communications (EDGE), Barcelona, Spain, 10–16 July 2022. 2022. URL: https://doi.org/10.1109/edge55608.2022.00027 (date of access: 23.03.2026).

4. Deep neural network and zero trust principles for intelligent drone management / S. Q. Abbas et al. 2024 IEEE 9th international conference on engineering technologies and applied sciences (ICETAS), Bahrain, Bahrain, 20–22 November 2024. 2024. P. 1–6. URL: https://doi.org/10.1109/icetas62372.2024.11120042 (date of access: 23.03.2026).

5. Kannan S., Venkataraman R., Ramachandran G. S. On-off attack detection in trust model using intra-daily variability for the IoT. Bulletin of electrical engineering and informatics. 2023. Vol. 12, no. 6. P. 3880–3888. URL: https://doi.org/10.11591/eei.v12i6.6110 (date of access: 23.03.2026).

6. Liao Z., Zhang L., Dong Z. UAV swarm exploration with byzantine fault tolerance. 2021 china automation congress (CAC), Beijing, China, 22–24 October 2021. 2021. URL: https://doi.org/10.1109/cac53003.2021.9727874 (date of access: 23.03.2026).

7. Reputation-Enhanced practical byzantine fault tolerance algorithm for node capture attacks on UAV networks / P. Onukak et al. Discover internet of things. 2025. Vol. 5, no. 1. URL: https://doi.org/10.1007/s43926-025-00164-y (date of access: 23.03.2026).

8. Saffre F., Hildmann H., Anttonen A. Force-Based Self-Organizing MANET/FANET with a UAV Swarm. Future internet. 2023. Vol. 15, no. 9. P. 315. URL: https://doi.org/10.3390/fi15090315 (date of access: 23.03.2026).

9. Sharma J., Mehra P. S. A survey of security challenges and existing prevention methods in FANET. Intelligent data analytics, iot, and blockchain. Boca Raton, 2023. P. 252–262. URL: https://doi.org/10.1201/9781003371380-24 (date of access: 23.03.2026).

10. Singh R. Simulation and evaluation of a hybrid trust–cryptographic protocol for UAV swarm communications. Simulation modelling practice and theory. 2025. P. 103230. URL: https://doi.org/10.1016/j.simpat.2025.103230 (date of access: 23.03.2026).

11. The essential role of cybersecurity in UAV swarm operations / F. M. Khan et al. Unmanned aerial vehicles swarm for protecting smart cities. Berkeley, CA, 2025. P. 403–441. URL: https://doi.org/10.1007/979-8-8688-1047-3_11 (date of access: 23.03.2026).

12. Trust based flying ad-hoc network: a survey / J. Kundu et al. IEEE access. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3419904 (date of access: 23.03.2026).

13. Trust prediction based on grey exponential smoothing method in VANETs / S. Zhang et al. 12th EAI international conference on mobile multimedia communications, mobimedia 2019, 29th - 30th jun 2019, weihai, china, Weihai, People's Republic of China, 29–30 June 2019. 2019. URL: https://doi.org/10.4108/eai.29-6-2019.2282065 (date of access: 23.03.2026).

14. Xie G., Zhou X., Gao J. Adaptive trust threshold model based on reinforcement learning in cooperative spectrum sensing. Sensors. 2023. Vol. 23, no. 10. P. 4751. URL: https://doi.org/10.3390/s23104751 (date of access: 23.03.2026).

15. Zhou S., Zhang G., Meng X. LocTrust: A local and global consensus-combined trust model in MANETs. Peer-to-Peer networking and applications. 2021. Vol. 15, no. 1. P. 355–368. URL: https://doi.org/10.1007/s12083-021-01250-y (date of access: 23.03.2026).

Надійшла до редакції: 11.12.25
Прийнята до друку: 17.03.26
Опубліковано: 30.03.26