УДК 004.7 DOI: 10.18372/2073-4751.85.21091

Волокита А. М., к.т.н.,
orcid.org/0000-0001-9069-5544,
artem.volokita@kpi.ua,
Меленчуков М. Є.,
orcid.org/0009-0005-6615-4306,
melenchukov.nikita@gmail.com

АДАПТИВНИЙ МЕТОД ВИБОРУ ЛІДЕРА В МОБІЛЬНИХ РОЗПОДІЛЕНИХ СИСТЕМАХ НА ОСНОВІ ІНТЕГРАЦІЇ ДИНАМІЧНОЇ ДОВІРИ

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Вступ

Сучасні інформаційно-керуючі комплекси, побудовані на базі мобільних автономних агентів (зокрема, рої БПЛА та літаючі ad-hoc мережі – FANET [1]), функціонують в умовах відсутності фіксованої інфраструктури як класичні розподілені системи [2]. Спроба реалізувати однорангову (peer-to-peer) архітектуру керування, де всі учасники є рівноправними, у таких мережах призводить до квадратичного зростання комунікаційних витрат $O(N^2)$. Це викликає перевантаження радіоканалу, колізії та неприпустиме зростання мережевих затримок. Відповіддю на ці виклики є введення динамічної ієрархії – вибір лідера, який лінеаризує інформаційні потоки, збирає дані та координує дії групи.

Впровадження механізму вибору лідера, вирішуючи проблему ефективності, водночас призводить до появи нових векторів загроз. У теорії алгоритмів існує поняття «візантійського» вузла [3] – це такий учасник мережі (дрон), який не просто виходить з ладу чи вимикається, а продовжує функціонувати, приховано імітуючи правильну роботу та свідомо надсилаючи суперечливі або хибні дані сусідам. Отримавши статус координатора, такий скомпрометований вузол може використати його для навмисної дезорганізації групи.

Метою роботи є розробка адаптивного методу вибору лідера, що об'єднує швидкість локальних алгоритмів кластеризації з надійністю динамічних систем оцінювання довіри, мінімізуючи ризики захоплення керування зловмисниками в умовах інформаційної протидії.

Огляд існуючих рішень

Проблема вибору надійного координатора в децентралізованих системах вивчалася з різних методологічних позицій. Базові алгоритми зваженої кластеризації (WCA), що розвиваються у сучасних роботах Y. Zhang та ін. [4], орієнтуються переважно на фізичні параметри (залишок батареї, ступінь вузла, мобільність), що робить їх беззахисними перед атаками маніпуляції даними.

Для подолання цієї вразливості було розроблено алгоритми на основі довіри (Trust-based WCA), зокрема в дослідженнях S. M. Salem та ін. [5]. Вони інтегрують репутаційні оцінки до процесу кластеризації. Однак їхнім "вузьким місцем" залишається використання статичних вагових коефіцієнтів або лінійних (адитивних) функцій корисності. У таких умовах виникає фундаментальна алгоритмічна дилема: адитивна природа функції

дозволяє скомпрометованому вузлу з вигідним топологічним розташуванням компенсувати штраф за низький рівень довіри.

Альтернативні блокчейн-орієнтовані підходи [6] та сучасні протоколи стійкості до візантійських відмов (Byzantine Fault Tolerance, BFT), такі як ACBFT [7], гарантують високу стійкість, проте вимагають надмірного обміну повідомленнями. Це вносить затримки, які є неприпустимими для систем реального часу з високою мобільністю. Сучасні біо-інспіровані методи кластеризації також страждають від повільної збіжності у високодинамічних мережах [8].

Відомі алгоритми вибору лідера з адаптивними вагами, що враховують надійність вузлів, мають суттєві обмеження: вони або є занадто обчислювально важкими (наприклад, великі архітектури Deep Learning) [10], або демонструють недостатню точність, оскільки адаптують лише математичну вагу коефіцієнта довіри [11]. Таким чином, невирішеною залишається проблема розробки легковагового методу вибору лідера, який би ефективно інтегрував у себе нейромережеві оцінки довіри для гнучкої адаптації не лише ваги репутації кандидата, але й самої суворості відбору залежно від змінного контексту поточної ситуації у мережі.

Метрики ефективності комунікації та якості обслуговування (QoS)

У системах керування реального часу критичним параметром ефективності є часова затримка доставки повідомлень. Для оцінки фізичної ефективності кандидата формується базова метрика якості обслуговування $QoS_i(t)$.

Нехай i – індекс конкретного вузла (дрона), а t – поточний дискретний момент часу (раунд). Тоді нормалізований заряд батареї позначається як $E_i(t) \in [0,1]$, а нормалізований ступінь вузла (кількість прямих сусідів) – як $d_i(t) \in [0,1]$. Якщо $T_{avg}^i(t)$ – середній час доставки повідомлення від дрона i до решти учасників рою, а T_{max}^t – діаметр мережі, то функція фізичної ефективності набуває вигляду:

$$QoS_i(t) = w_1 E_i(t) + w_2 d_i(t) + + w_3 \left(1 - \frac{T_{avg}^i(t)}{T_{max}^t}\right) \quad (1)$$

де w_1, w_2, w_3 – вагові коефіцієнти ($w_1 + w_2 + w_3 = 1$). Компонент $\left(1 - T_{avg}^i(t)/T_{max}^t\right)$ забезпечує максимізацію функції для вузлів, які знаходяться в комунікаційному центрі групи.

Запропонований адаптивний метод вибору лідера

Для усунення вразливостей класичного алгоритму Trust-WCA запропоновано чітко розмежувати логіку базового розрахунку довіри та алгоритм кластеризації. Вважається, що система вже використовує зовнішній модуль динамічного оцінювання довіри $Trust_i^{final}(t)$ на основі рекурентної нейронної мережі типу LSTM (Long Short-Term Memory) [9]. Задачею запропонованого алгоритму вибору лідера є ефективна інтеграція цього показника у комплексну нелінійну функцію корисності, де він виступає фільтруючим множником.

Комплексна функція ваги кандидата $W_i(t)$ визначається наступним чином:

$$W_i(t) = QoS_i(t) \times Trust_i^{final}(t)^{\gamma(t)} \quad (2)$$

Головною інновацією запропонованого методу вибору лідера є не просто перехід до мультиплікативної логіки, а динамічність ваги експоненти $\gamma(t)$, яка обчислюється на основі загальної оцінки непевності/загрози в системі $\theta(t)$, що транслюється базовою підсистемою довіри:

$$\gamma(t) = a \cdot \theta(t) \quad (3)$$

де a – константа масштабування "жорсткості" системи. На відміну від відомих мультиплікативних моделей ранжування (які використовуються, наприклад, у нечітких системах або імовірнісних протоколах), де вагові коефіцієнти є фіксованими або залежать від інертної статистики, запропонований підхід використовує адаптивну оцінку контексту. Це дозволяє системі змінювати суворість відбору кандидатів динамічно: у безпечному середовищі ($\gamma \approx 1$) функція працює близько до лінійної і пріоритет надається фізичній ефективності, а в умовах загрози ($\gamma > 1$) функція штрафу стає суперадитивною і ключовою вимогою стає бездоганна репутація. Такий підхід нівелює вплив скомпрометованих вузлів значно ефективніше, ніж традиційні адитивні або статичні мультиплікативні методи, і гарантовано виключає підозрілий вузол з перегонів за лідерство, навіть якщо його топологічні параметри є ідеальними.

Для запобігання частій зміні лідера (ефекту "пінг-понгу"), що дестабілізує керування, впроваджено умову перемикання з порогом гістерезису. Якщо L_{t-1} – поточний лідер, вузол k переймає роль координатора лише за умови:

$$W_k(t) > W_{L_{t-1}}(t) + \Delta W$$

де ΔW – параметр інерційності системи.

Результати експериментів

Для комплексної оцінки ефективності розробленого методу застосовано підхід ретроспективного моделювання (рис. 1).

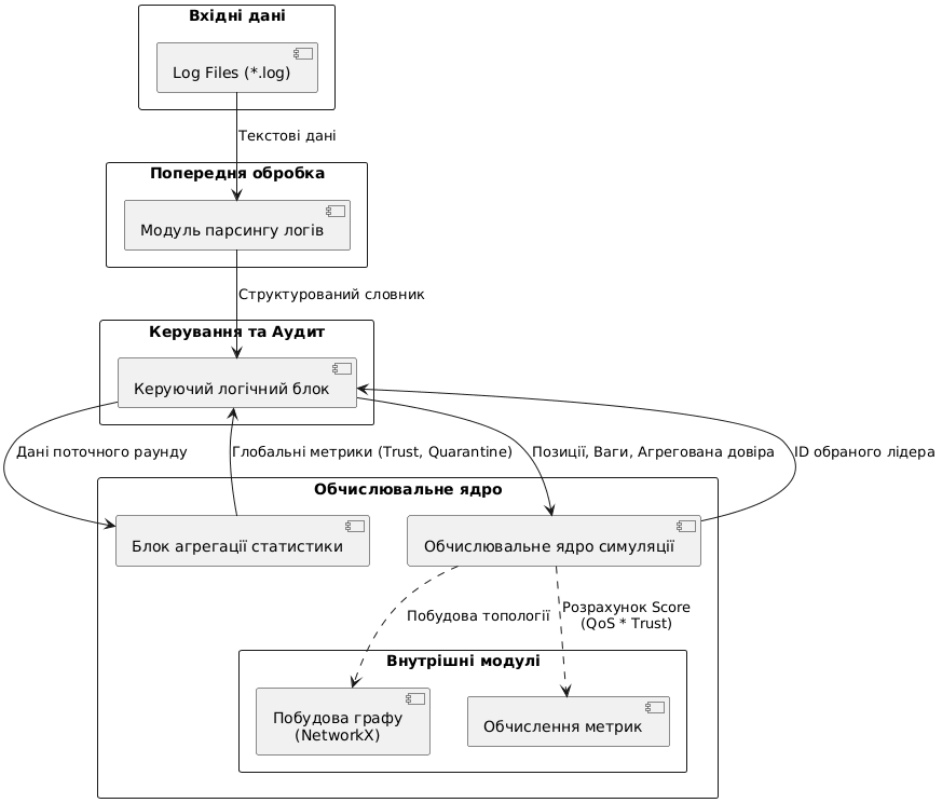

Рис. 1 – Архітектура аналітичного інструментарію

Цей підхід полягає у проведенні симуляцій на основі попередньо зібраних реальних або згенерованих логів (координат, станів батареї тощо). Це дозволило ізолювати логіку роботи алгоритму вибору від стохастичних (випадкових) флуктуацій мережевого середовища симулятора (ROS 2 +

Gazebo, рис. 1) та забезпечити абсолютну відтворюваність експериментів на одних і тих самих траєкторіях польоту рою за наявності скомпрометованих вузлів (рис. 2). Під час аналізу моделювалися граничні умови (знижена загальна вага довіри), щоб змусити систему балансувати між QoS та безпекою. Результати конкретних раундів (Таблиця 1) доводять гнучкість методу.

У Раунді 3 класичний метод Trust-WCA обрав лідером вузол з ідеальною топологічною оцінкою (1.000), ігноруючи його компрометацію (Статус 0). Натомість адаптивний метод пожертвував 5% QoS, обравши надійний Drone 8, тим самим зберігши безпеку мережі.

Аналіз повного масиву даних (понад 200 раундів симуляції) за конфліктуючими критеріями наведено у Таблиці 2.

.

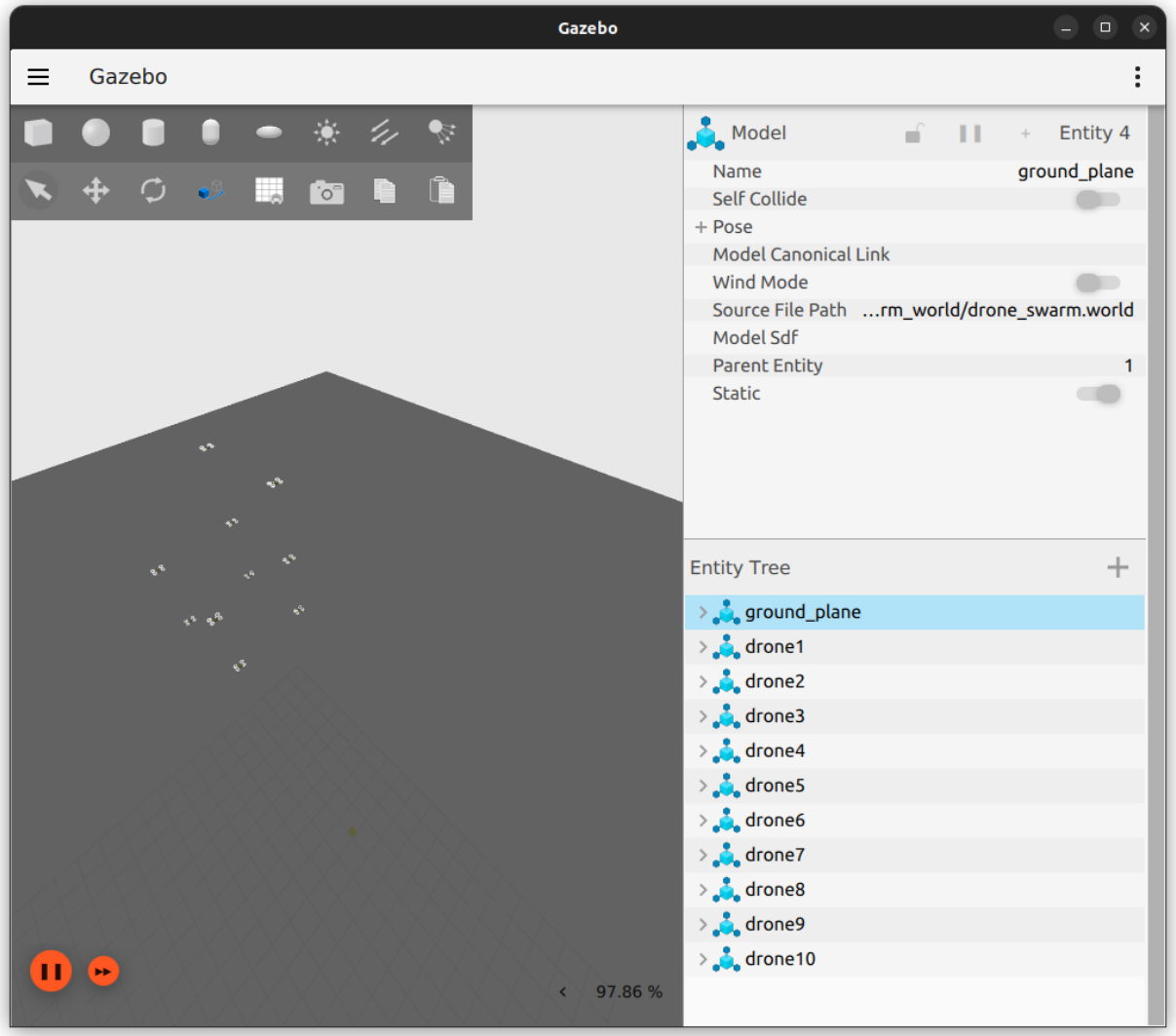

Рис. 2 – Симуляція польоту рою з 10 дронів у кубічній формації

Результати моделювання підтверджують, що використання динамічної експоненти дозволило знизити частоту обрання зловмисників лідером на 11.6%. Всупереч очікуванням про деградацію QoS, коефіцієнт топологічної ефективності зріс на 0.8%. Це свідчить про те, що превентивна ізоляція деструктивних агентів забезпечує кращу та стабільнішу структуру мережі в довгостроковій перспективі

Таблиця 1. Фрагмент порівняльного аналізу вибору лідера

Раунд	Theta	Drone ID	Trust	Dynamic QoS	Dynamic QoS Loss	Dynamic Status	Trust-WCA QoS	Trust-WCA QoS Loss	Trust-WCA Status
0	0.58	4	0.65	1	0	0	1	0	0
1	0.57	8	0.77	0.969	0.031	1	0.95	0.05	1
2	0.57	5	0.9	1	0	1	0.975	0	1
3	0.57	8	0.99	0.95	0.05	1	1	0	0
4	0.57	2	0.99	0.8	0	1	1	0	1
5	0.56	9	0.99	1	0	1	1	0	1
6	0.56	2	0.99	0.833	0	1	1	0	1
7	0.57	1	0.99	1	0	1	0.833	0.083	1
8	0.56	4	0.96	1	0	1	1	0	0
9	0.57	8	0.93	0.625	0.375	1	0.792	0.208	1
10	0.57	8	0.99	1	0	1	1	0	1
11	0.58	5	0.99	1	0	0	1	0	1
12	0.57	8	0.99	1	0	1	0.95	0.05	1
13	0.57	3	0.99	0.9	0	0	1	0	1
14	0.57	2	0.99	1	0	1	1	0	1
15	0.57	2	0.99	0.944	0	1	1	0	0
16	0.58	8	0.99	0.95	0.05	1	1	0	1
17	0.57	6	0.99	0.833	0.167	1	1	0	1
18	0.57	2	0.99	1	0	0	1	0	0
19	0.58	2	0.99	1	0	1	1	0	0
20	0.57	2	0.99	1	0	1	1	0	1

Таблиця 2. Аналіз інтегральних показників ефективності

Показник	Класичний метод (Trust-WCA)	Адаптивний метод (Запропонований)	Покращення
Liar Frequency (Частота помилок)	6.0%	5.3%	11.6% (відн.)
Коефіцієнт топологічної ефективності	0.9356	0.9434	0.8%
Avg Topology Loss	0.0344	0.0284	17.4% (відн.)

Висновки

У статті розроблено та обґрунтовано вдосконалений адаптивний метод вибору лідера на основі модифікованого алгоритму зваженої кластеризації. Інтеграція динамічного коефіцієнта довіри як змінної експоненти дозволяє реалізувати механізм «м'якої ізоляції» підозрілих вузлів. За результатами Trace-Driven Simulation доведено, що запропонований підхід забезпечує відносне зниження частоти перехоплення керування зловмисниками на 11,6% при одночасному покращенні топологічної ефективності мережі на 0,8%. Алгоритм відрізняється лінійною обчислювальною складністю $O(N)$ і є придатним для використання на бортових комп'ютерах БПЛА з обмеженими ресурсами.

Література

1. Chriki A., Touati H., Snoussi H. FANET: Communication, mobility models and security issues. Computer Networks. 2019. Vol. 163. P. 106877. DOI: 10.1016/j.comnet.2019.106877.

2. van Steen M., Tanenbaum A. S. Distributed Systems. 4th ed. Maarten van Steen, 2023. 600 p.

3. Kong L., Chen B., Hu F. LAP-BFT: Lightweight asynchronous provable Byzantine fault-tolerant consensus mechanism for UAV network. Drones. 2022. Vol. 6, No. 8. P. 187. DOI: 10.3390/drones6080187.

4. Zhang Y., Hu Z., Wang Z. et al. Survivability analysis of unmanned aerial vehicle network based on dynamic weighted clustering algorithm with dual cluster heads. Electronics. 2023. Vol. 12, No. 7. P. 1743. DOI: 10.3390/electronics12071743.

5. Salem S. M. et al. Enhancing MANET Security Through Long Short-Term Memory-Based Trust Prediction in Location-Aided Routing Protocols. IEEE Access. 2025. Vol. 13. P. 11077–11092. DOI: 10.1109/ACCESS.2025.3572619.

6. Fan C. et al. Performance Evaluation of Blockchain Systems: A Systematic Survey. IEEE Access. 2020. Vol. 8. P. 126927–126950. DOI: 10.1109/ACCESS.2020.3006078.

7. Wang J. et al. ACBFT: Adaptive chained Byzantine fault-tolerant consensus protocol for UAV ad hoc networks. IEEE Transactions on Vehicular Technology. 2025. Vol. 74, No. 7. P. 11324–11336. DOI: 10.1109/TVT.2025.3548281.

8. Arafat M. Y., Moh S. Bio-inspired approaches for energy-efficient localization and clustering in UAV networks. IEEE Access. 2019. Vol. 7. P. 16250–16269. DOI: 10.1109/ACCESS.2021.3053605.

9. Van Houdt G., Mosquera C., Nápoles G. A review on the long short-term memory model. Artificial Intelligence

Review. 2020. Vol. 53. P. 5929–5955. DOI: 10.1007/s10462-020-09838-1.

10. Ullah F. et al. Deep Trust: A Novel Framework for Dynamic Trust and Reputation Management in the Internet of Things (IoT)-Based Networks. IEEE Access. 2024. Vol. 12. P. 87407–87419. DOI: 10.1109/ACCESS.2024.3409273.

11. Zhang C. et al. Trust Attacks and Defense in the Social Internet of Things: Taxonomy and Simulation-Based Evaluation. Sensors. 2025. Vol. 25, No. 3. P. 7513. DOI: 10.3390/s25247513.

Волокита А. М., Меленчуков М. Є.

АДАПТИВНИЙ МЕТОД ВИБОРУ ЛІДЕРА В МОБІЛЬНИХ РОЗПОДІЛЕНИХ СИСТЕМАХ НА ОСНОВІ ІНТЕГРАЦІЇ ДИНАМІЧНОЇ ДОВІРИ

Розвиток мобільних розподілених систем, зокрема літаючих ad-hoc мереж (FANET), вимагає переходу до архітектур децентралізованого керування з вибором локальних лідерів. В умовах агресивного середовища класичні адитивні методи кластеризації (наприклад, Trust-WCA) виявляють вразливість перед скомпрометованими «візантійськими» вузлами (учасниками мережі, що навмисно діють деструктивно, імітуючи легітимну поведінку) з високими показниками радіоканалу. У роботі запропоновано адаптивний метод вибору лідера на основі нелінійної мультиплікативної функції. Застосування динамічної експоненти довіри, яка регулюється нейромережевим модулем типу LSTM залежно від рівня загрози, діє як фільтр («м'який гейт»), превентивно ізолюючи підозрілі вузли. За результатами ретроспективного моделювання (Trace-Driven Simulation) доведено відносне зниження частоти обрання скомпрометованих лідерів на 11,6% при одночасному покращенні топологічної ефективності мережі на 0,8%.

Ключові слова: *розподілені системи, FANET, вибір лідера, динамічна довіра, Trust-WCA, Trace-Driven Simulation.*

Volokyta A. M., Melenchukov M. E.

ADAPTIVE LEADER ELECTION METHOD IN MOBILE DISTRIBUTED SYSTEMS BASED ON DYNAMIC TRUST INTEGRATION

The development of mobile distributed systems, particularly Flying Ad-hoc Networks (FANETs), requires a transition to decentralized control architectures involving local leader election. Under hostile conditions, classical additive clustering methods (e.g., Trust-WCA) reveal vulnerabilities to compromised Byzantine nodes (participants that intentionally act destructively while simulating legitimate behavior) exhibiting high radio channel performance. This paper proposes an adaptive leader election method based on a non-linear multiplicative function. The application of a dynamic trust exponent, regulated by an LSTM neural network module depending on the threat level, acts as a filter ("soft gate"), preemptively isolating suspicious nodes. Based on Trace-Driven Simulation results, a relative decrease of 11.6% in the frequency of electing compromised leaders was proven, alongside a simultaneous 0.8% improvement in the network's topological efficiency.

Keywords: *distributed systems, FANET, leader election, dynamic trust, Trust-WCA, Trace-Driven Simulation.*

Стаття подана до редакції: 16/03/2026
Стаття прийнята до опублікування: 23/03/2026
Стаття опублікована: 27/04/2026