

DOI: 10.18372/2310-5461.71.21453
УДК 004.056.53

Р. В. Огієвич

аспірант кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
<https://orcid.org/0009-0003-7948-1125>
e-mail: ohiievych.r@fit.knu.ua;

І. І. Пархоменко

кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
<https://orcid.org/0000-0001-6889-9284>
e-mail: ivan.parkhomenko@knu.ua

АДАПТИВНА БАГАТОКРИТЕРІАЛЬНА ОПТИМІЗАЦІЯ RTCT-ПЕРЕВІРКИ В ДЕЦЕНТРАЛІЗОВАНИХ ОВЕРЛЕЙНИХ МЕРЕЖАХ

Вступ

Децентралізовані оверлейні мережі – однорангові (P2P) системи, інфраструктури Інтернету речей, mesh- та MANET-середовища, а також реєривень Web3-екосистем – будуються поверх фізичної інфраструктури як логічний рівень взаємодії вузлів без єдиного центру координації та довіреного органу сертифікації. У такій моделі вузол є цифровою ідентичністю, а не гарантовано унікальною фізичною сутністю. Відсутність централізованої довіри унеможливує просту перевірку відповідності «одна фізична сутність – один ідентифікатор» і відкриває простір для атаки Сивілли, за якої один суб'єкт породжує множину фіктивних ідентичностей задля непропорційного впливу на маршрутизацію, голосування чи розподілене зберігання [1].

Класичний результат Дж. Дусьора встановлює, що у відкритих системах неможливо гарантувати унікальність учасників без централізованого арбітра [1]. Похідні від атаки Сивілли, такі як отруєння таблиць розподіленого зберігання (DHT), затемнення вузла (Eclipse attack), штучне підсилення репутації чи утримання вигідної маршрутною позиції, реалізуються тим легше, чим дешевшим є створення й підтримання ідентичності. Тому захист доцільно зміщувати з разового контролю входу на контроль підтримання участі: ідентичність має не лише сплатити вартість приєднання, а й нести поточні витрати, доки залишається в мережі.

Цю логіку реалізує механізм випадкових часових челендж-токенів (Random Time Challenge-Tokens, RTCT): у випадкові, непрогнозовані моменти вузли отримують криптографічний челендж (головоломку), який мають розв'язати у вузькому

часовому вікні, після чого токен-відповідь анулюється [2]. Ефективність RTCT, однак, визначається не самим фактом перевірки, а вибором її параметрів – складності завдання, інтенсивності викликів і ширини вікна відповіді. Надмірно жорсткі параметри перевантажують чесні вузли й підвищують частку хибних відключень; надмірно м'які – не створюють для злоумисника відчутних поточних витрат. Це робить задачу налаштування параметрів RTCT ключовою для практичної придатності методу.

Аналіз останніх досліджень і публікацій

Спроби протидіяти атакам Сивілли пройшли декілька поколінь. Методи на основі соціальних графів, такі як SybilGuard чи SybilLimit, спираються на властивість швидкого змішування легітимного графа, яка руйнується засобами соціальної інженерії. Дворк і Наор запропонували перевірку ресурсів і клієнтські обчислювальні головоломки, реалізувавши принцип «вартості за дію»; такі схеми ефективні проти відмови в обслуговуванні, проте у контексті Сивілли виконують лише функцію контролю входу: після одноразової оплати подальша експлуатація майже безкоштовна [3]. SybilControl поєднав відкладене додавання вузлів із періодичною верифікацією обчислювальними головоломками, зробивши частку підконтрольної злоумиснику мережі пропорційною його обчислювальній потужності [4]; проте детермінований графік перевірок залишає вікно для часової оптимізації ресурсів атакуювальником.

Економічний погляд на стійкість децентралізованих систем розвинув Джон Будіш, показавши, що безпека типового консенсусу спирається на потокову вартість підтримання системи, а не на

разову вигоду від атаки [5]. Цей результат сформульовано на рівні консенсусу (атака 51 %), однак його логіку – перевагу поточних витрат над разовими – природно перенести на рівень контролю участі, де цінність атаки інша, а саме – маршрутно-топологічна. Саме таке перенесення покладено в основу криптоекономічної моделі RTCT [2].

Потрібний для RTCT інструментарій забезпечують такі роботи. Послідовні функції із затримкою, що перевіряється, (Verifiable Delay Functions) гарантують, що мінімальний час розв’язання не скорочується розпаралелюванням [6], а функції script послаблюють апаратну асиметрію між вузлами [7; 8]. Логічні годинники Лампорта впорядковують події в розподіленій системі без глобального годинника, але самі собою не доводять факту витраченого часу [9]. Споріднений підхід запропоновано в протоколі рандомізованого тесту уважності (Randomized Attention Test) для моніторингу валідаторів, що поєднує випадкову перевірку активності з економічними штрафами [10]; на відміну від нього, RTCT діє на мережевому рівні контролю участі, а не на рівні валідаторів консенсусу.

Питання адаптивного налаштування захисних параметрів ширше розглядають у межах концепції рухомої цілі (Moving Target Defense), де параметри системи навмисно змінюють у часі, щоб ускладнити розвідку й атаку [11; 12]. Для динамічного добору параметрів захисту дедалі частіше застосовують навчання з підкріпленням [13; 14], а строге обґрунтування оптимальності в задачах безпеки з обмеженнями спирається на умови Каруша–Куна–Таккера, як, наприклад, у задачах максимізації швидкості приховування для каналів МІМО [15]. Водночас узгодженого, аналітично обґрунтованого методу одночасного добору складності, інтенсивності та вікна відповіді для контролю участі в децентралізованих мережах у літературі не запропоновано.

Постановка завдання

Налаштування параметрів перевірки в системах контролю участі історично зводять до коригування єдиного параметра – складності обчислювального завдання. Канонічний приклад – алгоритми коригування складності (Difficulty Adjustment Algorithms) у proof-of-work системах, де складність регулюється за відхиленням фактичного часу породження блоку від цільового [16]. Такий підхід має три обмеження, критичні саме для рівня контролю участі.

По-перше, він керує лише складністю, залишаючи поза розглядом інтенсивність перевірок та вікно відповіді, тоді як стійкість до часового

мультиплексування фіктивних ідентичностей визначається насамперед співвідношенням часу розв’язання й ширини вікна. По-друге, коригування реагує на агреговане відхилення часу й нечутливе до апаратної гетерогенності вузлів: однакова складність для слабкого IoT-сенсора й потужного серверного вузла означає або надмірний бар’єр для перших, або відсутність бар’єра для других. По-третє, детерміноване правило коригування саме стає передбачуваним і піддається грі з боку раціонального зловмисника, що показано для DAA proof-of-work систем за високої еластичності пропозиції обчислень [16].

Контроль участі без постійного органу сертифікації потрібен інфраструктурам IoT і mesh, аварійним та тактичним MANET-мережам із високою динамікою складу учасників, а також реєр-рівню Web3 застосунків, де небажано спиратися на «важкий» глобальний консенсус для фільтрації фіктивних вузлів. У всіх цих середовищах апаратні можливості вузлів, рівень загроз і мережева динаміка змінюються в часі, тож фіксований або односкладовий механізм налаштування перевірки не забезпечує водночас стійкості до атак і прийнятних накладних витрат. Потрібен метод, який узгоджено добиратиме сукупність параметрів перевірки за кількома суперечливими критеріями та піддається аналітичному обґрунтуванню оптимальності.

Мета статті

Метою статті є удосконалення методу адаптивного налаштування параметрів захисних механізмів контролю участі в децентралізованих оверлейних мережах через перехід від детермінованого коригування лише складності до аналітичної багатокритеріальної оптимізації трійки параметрів RTCT-перевірки (складності, інтенсивності та вікна відповіді) з характеристикою оптимуму умовами Каруша–Куна–Таккера.

Для досягнення мети розв’язано такі завдання: формалізувати параметри RTCT-перевірки як вектор керування й описати їхній вплив на стійкість і накладні витрати; показати обмеження базового детермінованого коригування складності; побудувати багатокритеріальну постановку задачі добору параметрів і скаляризувати її зваженою згорткою; довести характеристикою оптимуму умовами першого порядку за припущень увігнутості показника стійкості й опуклості функцій накладних витрат; на модельному ілюстративному прикладі продемонструвати розв’язок і його порівняльну статистику; окреслити опціональну онлайн-реалізацію на основі Марковського процесу прийняття рішень і навчання з підкріпленням для нестационарних режимів.

Виклад основного матеріалу

Метод RTCT формалізують як кортеж (1), де N – множина вузлів; R_t – джерело випадковості; S_t – стохастичний вибір вузла для перевірки на основі процесу Пуассона; C_t – генерація членджу складності; m , τ_t – обчислення токена-відповіді; V_t – перевірка в межах вікна; Δ , P_t – санкційна функція [2].

$$\mathcal{R} = \langle N, R_t, S_t, C_t, \tau_t, V_t, P_t \rangle. \quad (1)$$

Непрогнозованість моментів перевірки задає властивість відсутності пам'яті Пуассонівського процесу: час очікування наступного членджу розподілений експоненційно (2), тож імовірність надходження виклику в наступний інтервал не залежить від історії, і зловмисник не може заздалегідь планувати «вікна простоя».

$$P(T > s + t \mid T > s) = P(T > t) = e^{-\lambda t}, \quad \lambda > 0. \quad (2)$$

Керованими є три параметри: складність m , інтенсивність викликів λ і вікно відповіді Δ . Їхній вплив різноспрямований (табл. 1). Стійкість дедлайну до мультиплексування визначається сиквенційністю завдання: для послідовних функцій час розв'язання t_{solve} не скорочується нарощуванням обладнання, що працює паралельно (3), тож вузьке вікно Δ змушує зловмисника тримати окремий обчислювальний потік на кожну фіктивну ідентичність [6]. Тут H – доступна обчислювальна потужність вузла (умовно нормована), $T_{seq}(m)$ – час виконання строго послідовної частини задачі складності m , $W(m)$ – загальний обсяг роботи (операцій), а параметр сиквенційності $\sigma \in [0, 1]$ інтерполює між повністю послідовним ($\sigma = 1$) і повністю паралельним ($\sigma = 0$) режимами.

$$t_{solve}(m, H, \sigma) = [T_{seq}(m)]^{\sigma} \cdot [W(m)/H]^{1-\sigma}. \quad (3)$$

Таблиця 1

Параметри RTCT-перевірки та їхній вплив

Параметр	Роль у перевірці	Підвищення стійкості	Вплив на чесні вузли
m (складність)	масштаб обчислювальної роботи на члендж ($\approx 2^m$ операцій)	експоненційне зростання поточної вартості атаки	зростання обчислювальних витрат на відповідь
λ (інтенсивність)	частота випадкових у часі викликів	лінійне зростання вартості утримання ідентичності	зростання комунікаційних та обчислювальних витрат
Δ (вікно відповіді)	допустимий час на обчислення відповіді	звуження ускладнює часове мультиплексування ідентичностей	звуження підвищує частку хибних відключень

Перенесена на рівень контролю участі умова безпеки набуває вигляду (4): сумарні витрати атакувальника на горизонті T – разовий якір входу C_0 , інтегральний потоковий член по k підтримуваних фіктивних ідентичностях з вартістю відповіді на члендж $\varphi(m, \Delta, \sigma)$ та інтенсивністю викликів $\lambda(t)$ і санкційні втрати C_{pen} – мають перевищувати цінність атаки V_A [2; 5]. Тут k – кількість підтримуваних атакувальником ідентичностей, $\varphi(m, \Delta, \sigma)$ – питома вартість обчислення токена-відповіді на один члендж за поточних значень складності, вікна і сиквенційності.

$$C_0 + \int_0^T k \lambda(t) \varphi(m(t), \Delta(t), \sigma) dt + C_{pen}(T) \geq V_A(T). \quad (4)$$

На кожен члендж раціональний зловмисник обирає менш витратний із двох виходів – відповісти (вартість φ) або відмовитися з подальшою регенерацією ідентичності (вартість C_{entry} – суку-

пні витрати на повторну реєстрацію нової ідентичності, включно з якорем входу C_0 та накладними витратами на повторне закріплення в маршрутних таблицях), тож ефективна вартість події дорівнює меншій з цих двох величин (5). Для позиційно залежних атак відмова знищує саму атаку через втрату місця в таблиці маршрутизації, і зловмисник змушений платити безперервно.

$$c_{eff} = \min\{\varphi(m, \Delta, \sigma), C_{entry}\}. \quad (5)$$

Лінійне масштабування ресурсу зловмисника з кількістю ідентичностей k обґрунтовується теорією масового обслуговування: k незалежних пуассонівських потоків агрегуються в потік інтенсивності $k\lambda$, і за жорсткого дедлайну необхідна паралельна сиквенційна потужність зростає як $k\lambda \cdot t_{solve}$ з поправкою порядку кореня на пікову одночасність (6), де z_{β} – квантиль стандартного нормального розподілу рівня довіри β (наприклад, $z_{\beta} \approx 1,96$ для $\beta = 0,975$), що задає допустиму

ймовірність прострочення хоча б одного члену в піку, – режим Холфіна–Уїтта [17]. Для чесного вузла відповідна потужність ≈ 1 , тож відношення масштабується як k . Отже, інтенсивність λ і складність m прямо визначають поточну вартість атаки, але водночас – і накладні витрати чесних вузлів, що й породжує потребу в оптимізації.

$$M_{adv} \gtrsim k\lambda t_{solve} + z_{\beta}\sqrt{k\lambda t_{solve}}. \quad (6)$$

Детерміноване коригування складності спирається на правило за ковзним середнім (7): нова складність дорівнює попередній, помноженій на відношення очікуваного часу до фактичного [16]. Метод керує єдиним параметром, реагує лише на агреговане відхилення часу й не враховує ані інтенсивності, ані вікна відповіді, ані гетерогенності вузлів; до того ж детерміноване правило передбачуване. Економічний аналіз DAA proof-of-work систем показує, що за високої еластичності пропозиції обчислень таке коригування може втрачати стабільність [16]. Це обґрунтовує перехід до багатопараметричного й багатокритеріального добору.

$$D_{new} = D_{old} \cdot \frac{T_{expected}}{T_{actual}}. \quad (7)$$

Добір параметрів $\theta = (m, \lambda, \Delta)$ підпорядкований трьома суперечливим критеріям: максимізації показника стійкості $Sec(\theta)$, мінімізації обчислювальних накладних витрат чесного вузла $Over_{comp}$ та мінімізації комунікаційних накладних витрат $Over_{comm}$. Скаляризація зваженою згортокою дає цільову функцію (8), де ваги $w_1, w_2, w_3 > 0$ відображають політику мережі й у багатокритеріальному сенсі параметризують границю Парето.

$$R(\theta) = w_1 Sec(\theta) - w_2 Over_{comp}(\theta) - w_3 Over_{comm}(\theta). \quad (8)$$

Допустима множина Θ задається обмеженнями на кожен параметр та двома експлуатаційними обмеженнями: бюджетом хибних відключень $p_{fp}(\Delta) \leq \varepsilon_{max}$, який через монотонне спадання частки прострочень із шириною вікна (9) встановлює нижню межу на Δ , та комунікаційним бюджетом на λ .

$$p_{fp}(\Delta) = e^{-\Delta/\Delta_c} \leq \varepsilon_{max}, \quad \Delta \geq -\Delta_c \ln \varepsilon_{max}. \quad (9)$$

Нехай показник стійкості Sec увігнутий і зростає за m та λ і спадає за Δ , а функції накладних витрат $Over_{comp}$ та $Over_{comm}$ опуклі та зростають; тоді цільова функція R увігнута на опуклій множині Θ . За цих припущень задача має єдиний глобальний максимум, що характеризується умовами Каруша–Куна–Таккера (10): стаціонарністю градієнта лагранжіана, доповнювальною нежорсткістю, прямою та двоїстою допустимістю [15].

$$\begin{aligned} \nabla R(\theta^*) &= \sum_i \mu_i \nabla g_i(\theta^*), \\ \mu_i g_i(\theta^*) &= 0, \quad g_i(\theta^*) \leq 0, \\ \mu_i &\geq 0, \quad i = 1, \dots, p. \end{aligned} \quad (10)$$

Економічна інтерпретація умов першого порядку: в оптимумі відношення граничного приросту стійкості до граничного приросту накладних витрат вирівнюється за всіма трьома параметрами з точністю до ваг. Якщо бюджет хибних відключень активний, його множник додатний, і оптимальне вікно фіксується на нижній допустимій межі $\Delta^* = -\Delta_c \cdot \ln \varepsilon_{max}$ – звідси випливає принцип: вікно звужують рівно настільки, наскільки дозволяє толерантність до колатеральних відключень чесних вузлів. Цей результат є строго доведеним і не залежить від конкретного алгоритму пошуку. Загальну архітектуру адаптивного контуру, що реалізує цей принцип, наведено на рис. 1.

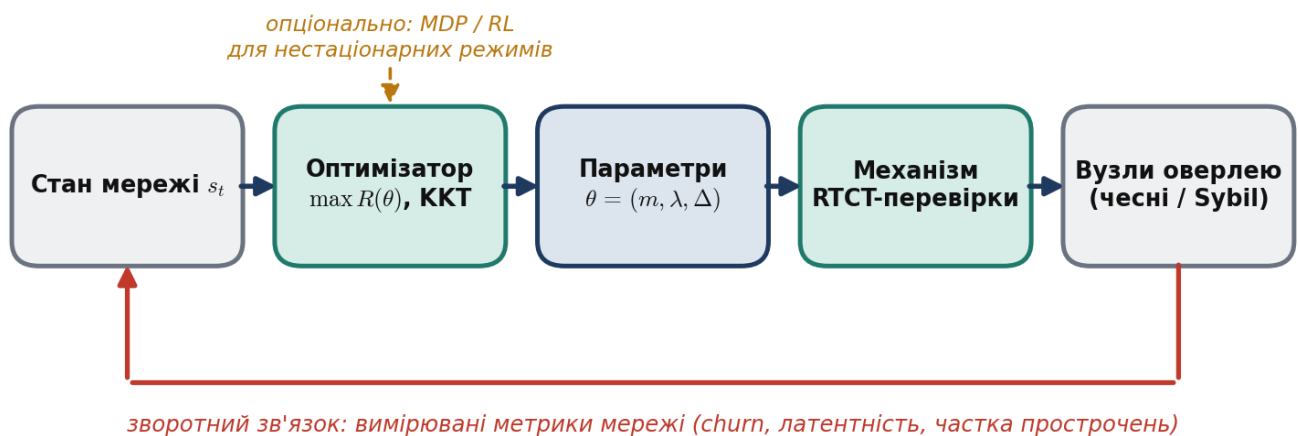


Рис. 1. Схема адаптивного контуру налаштування параметрів RTCT-перевірки

Для наочності розглянемо нормований модельний приклад (емпіричної валідації він не передбачає, параметри задано ілюстративно; табл. 2). Показник стійкості задано у вигляді $Sec(\theta) = a_m \cdot \ln(1 + m) + a_\lambda \cdot \ln(1 + \lambda) + a_\Delta \cdot (1 - \Delta/\Delta_{max})$, обчислювальні витрати $Over_{comp} = b_m \cdot 2^{(m-m_0)}$, комунікаційні $Over_{comm} = b_\lambda \cdot \lambda$. За значень, наведених у табл. 2, цільова функція сепарабельна й увігнута за кожним параметром.

Розв'язок умов першого порядку дає інтер'єрний оптимум складності $m^* \approx 17,9$ біт (трансцендентне рівняння (12)) та інтенсивності $\lambda^* = \frac{w_1 a_\lambda}{w_3 b_\lambda} - 1 = 9$ викликів/год (11); за бюджету

хвибних відключень $\varepsilon_{max} = 0,05$ і масштабу гетерогенності $\Delta_c = 10$ с активне обмеження фіксує вікно $\Delta^* \approx 30$ с.

$$\lambda^* = \frac{w_1 a_\lambda}{w_3 b_\lambda} - 1, \quad \Delta^* = -\Delta_c \ln \varepsilon_{max}. \quad (11)$$

$$\frac{w_1 a_m}{1 + m^*} = w_2 b_m (\ln 2) 2^{m^* - m_0}. \quad (12)$$

Рис. 2 ілюструє компроміс за складністю: увігнутий приріст стійкості та опуклі обчислювальні витрати дають унімодальну згортку з єдиним максимумом m^* . Рис. 3 показує оптимум за інтенсивністю та роль бюджету хвибних відключень у фіксації вікна.

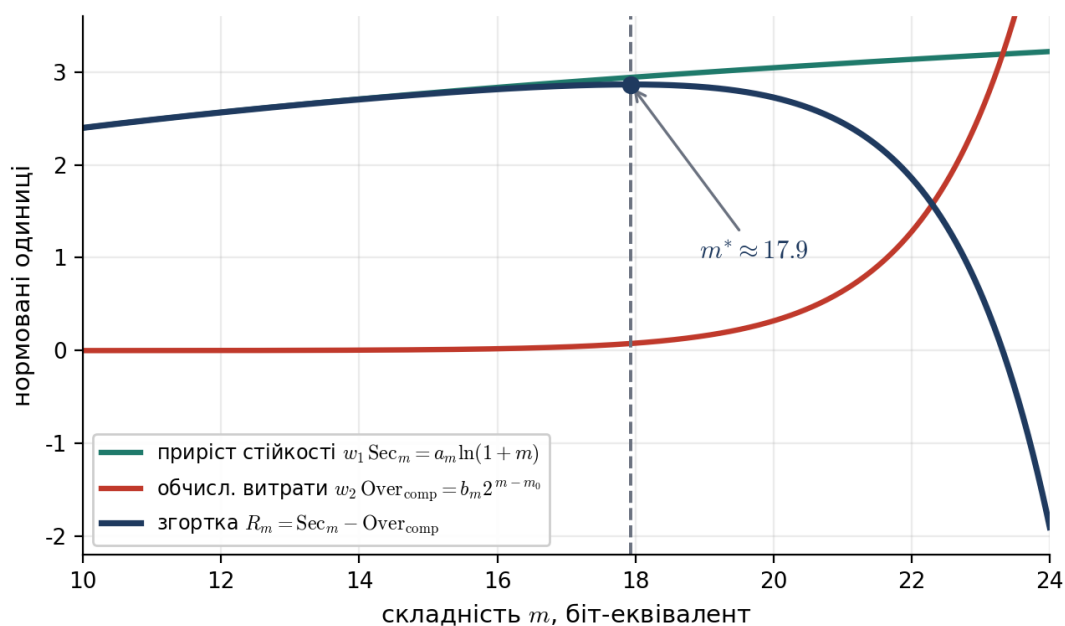


Рис. 2. Компроміс «стійкість – обчислювальні витрати» за складністю m та оптимум m^*

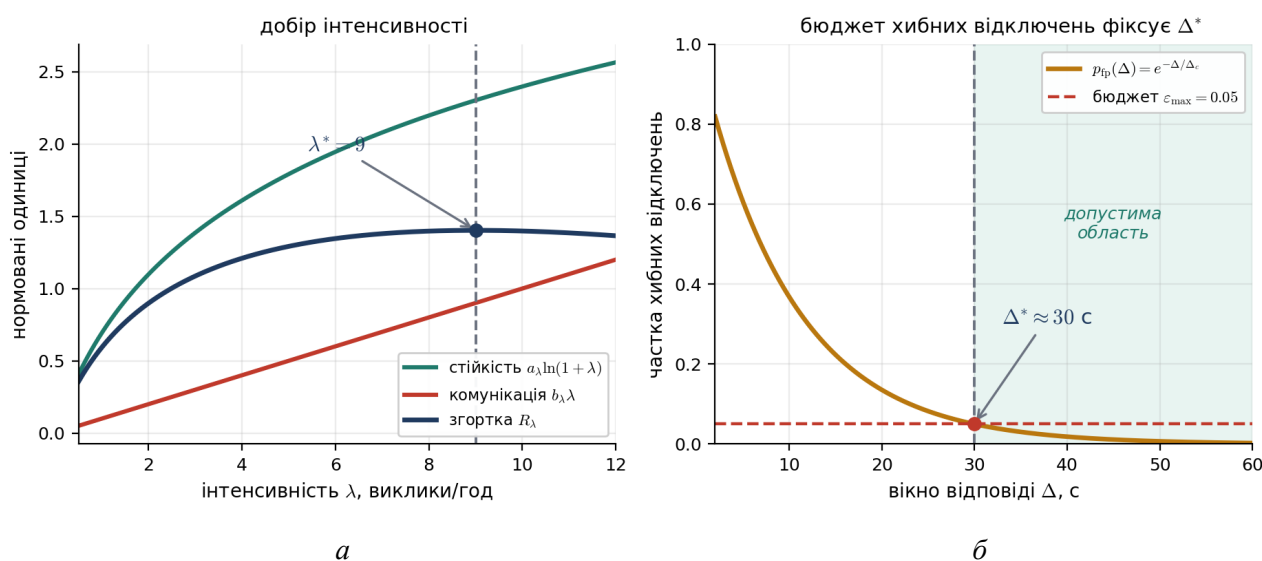


Рис. 3. Добір інтенсивності λ (а) та фіксація вікна Δ^* бюджетом хвибних відключень (б)

Таблиця 2

Параметри модельного ілюстративного прикладу та результат

Величина	Позначення	Значення
Коефіцієнти показника стійкості	a_m, a_λ, a_Δ	1; 1; 0,5
Обчислювальні витрати	b_m, m_0	0,02; 16
Комунікаційні витрати	b_λ	0,1
Ваги критеріїв	w_1, w_2, w_3	1; 1; 1
Бюджет хибних відключень	ε_{max}	0,05
Масштаб гетерогенності вузлів	Δ_c	10 с
Результат – оптимум	m^*, λ^*, Δ^*	$\approx 17,9$ біт; 9 викл./год; ≈ 30 с

Порівняльна статика узгоджується з інтуїцією й вимогами адаптивності: оптимальна інтенсивність λ^* лінійно зростає з вагою стійкості w_1 і спадає зі зростанням вартості комунікації; оптимальна складність m^* зростає з $w_1 a_m$ і спадає з $w_2 b_m$; оптимальне вікно Δ^* розширюється зі зменшенням допустимого рівня хибних відключень ε_{max} . Підвищення оцінюваного рівня загрози (зростання підозрюваної кількості фіктивних ідентичностей k , що збільшує цінність атаки) еквівалентне зростанню ваги стійкості й веде до автоматичного посилення перевірки – підвищення λ та m – у межах, заданих експлуатаційними бюджетами. Так односкладове коригування складності узагальнюється до узгодженого добору всієї трійки параметрів (табл. 3).

Аналітичний оптимум обчислюється за відомих функцій *Sec* і *Over* та стаціонарного режиму.

Для нестационарних режимів і невідомої динаміки мережі добір параметрів формують як марковський процес прийняття рішень: стан s_t описує спостережуваний стан мережі (оцінки churn, латентності, частки прострочень, аномалій реєстрації), дія a_t коригує параметри (13), а винагорода збігається зі скаляризованою згортою R . Задачу розв'язує агент навчання з підкріпленням [13; 14], причому така реалізація надбудовується над аналітично визначеним оптимумом, а не замінює його, що зберігає доказовість гарантій для стаціонарного випадку. Цей поділ узгоджується з концепцією рухомої цілі [11; 12]. Стійкість RL-агента до спрямованих маніпуляцій спостереженнями залишається предметом подальших досліджень.

$$\theta_{t+1} = \theta_t + a_t, \quad a_t = (\Delta m_t, \Delta \lambda_t, \Delta \Delta_t). \quad (13)$$

Таблиця 3

Порівняння базового коригування складності та запропонованого методу

Аспект	Базове коригування складності (DAA)	Запропонований метод
Об'єкт керування	лише складність m	трійка параметрів (m, λ, Δ)
Критерії	єдиний – відхилення часу події від цільового	багатокритеріально: стійкість, обчислювальні та комунікаційні витрати
Гарантія оптимальності	відсутня (евристичне правило)	глобальний оптимум за умовами ККТ (увігнута задача)
Гетерогенність вузлів	не враховується	враховується через бюджет хибних відключень і ваги критеріїв
Передбачуваність	детермінована, піддається грі	випадковість моментів перевірки та адаптивні ваги
Реалізація	статичне правило коригування	аналітичний оптимум; опційно – MDP/RL

Висновки

Удосконалено метод адаптивного налаштування параметрів захисних механізмів контролю участі в децентралізованих оверлейних мережах. На відміну від базового детермінованого коригування лише складності, метод здійснює узгоджений добір трійки параметрів RTCT-перевірки – складності, інтенсивності та вікна відповіді – за трьома суперечливими критеріями: стійкістю до атак, обчислювальними та комунікаційними накладними витратами. Задачу скаляризовано зваженою згорткою, ваги якої параметризують границю Парето й політику мережі.

Головний теоретичний результат – характеристика оптимуму умовами Каруша–Куна–Таккера за припущень увігнутості показника стійкості й опуклості функцій накладних витрат, що забезпечує єдиність глобального розв’язку незалежно від алгоритму пошуку. Аналіз умов першого порядку дає змістовний принцип налаштування: вікно відповіді звужують доти, доки це дозволяє бюджет хибних відключень чесних вузлів, а інтенсивність і складність добирають за вирівнюванням граничного приросту стійкості на одиницю накладних витрат. Модельний ілюстративний приклад демонструє інтер’єрний оптимум та порівняльну статику, узгоджену з вимогами адаптивності: посилення загрози автоматично підвищує інтенсивність і складність перевірки в межах експлуатаційних бюджетів.

Практична цінність методу полягає в тому, що умови першого порядку прямо задають політиці мережі важелі балансування: за зростання частки прострочених відповідей у спостережуваному режимі слід насамперед розширювати вікно Δ у межах допустимого бюджету хибних відключень, а вже потім переглядати інтенсивність λ ; за стійкого зростання підозрюваної кількості фіктивних ідентичностей k інтенсивність λ та складність m узгоджено підвищують, а пропорції приросту визначає вирівнювання граничного приросту стійкості на одиницю відповідних накладних витрат. Такий принцип усуває типову ваду односкладового коригування лише складності, за якого підвищення m в умовах обмеженого комунікаційного бюджету спричиняє зростання прострочень у частини чесних вузлів та їх помилкове виключення з оверлею. Запропонована багатокритеріальна постановка робить такий компроміс явним і керованим: ваги w_1 , w_2 , w_3 параметризують політику мережі й узгоджуються з класом застосувань – від чутливого до затримок mesh-оверлею до інфраструктурного P2P-репозиторію.

Серед обмежень методу слід відзначити припущення про увігнутість показника стійкості

$Sec(\theta)$ та опуклість функцій накладних витрат $Over(\theta)$, де $\theta = (m, \lambda, \Delta)$, за яких умови ККТ є не лише необхідними, а й достатніми для глобального оптимуму. На практиці локальні відхилення від цих припущень можливі, зокрема за наявності кореляції між атакувальними подіями або немонотонних ефектів масштабу в накладних витратах; у такому разі рекомендується розбити допустиму множину параметрів на кусково-увігнуті області та застосувати запропонований оптимум у межах кожної з них. Окреме питання – калібрування коефіцієнтів a_m , a_λ , a_Δ , b_m , b_λ за вимірними даними реальних мереж: запропонована форма допускає онлайн-оцінювання цих коефіцієнтів за методом найменших квадратів зі змінним вікном.

З погляду обчислювальної реалізації аналітичний оптимум розв’язується методом внутрішньої точки за час, лінійний за кількістю активних обмежень, що для трипараметричної задачі еквівалентно одиничному виклику градієнтного методу й допускає періодичний перерахунок із кроком, узгодженим з характерним часом дрейфу режиму мережі. Моменти перевірки залишаються Пуассонівськими з інтенсивністю λ^* ; властивість відсутності пам’яті (2) забезпечує непередбачуваність перевірки для адверсарія незалежно від поточних значень параметрів. У MDP-надбудові параметри (m, λ, Δ) обмежують довірчою областю навколо аналітичного оптимуму, що пришвидшує збіжність RL-агента та запобігає експлуатаційно небезпечним викидам у простір дій під час навчання.

Для нестаціонарних режимів окреслено опціональну реалізацію добору параметрів як марковського процесу прийняття рішень із розв’язанням засобами навчання з підкріпленням; ця реалізація надбудовується над аналітичним оптимумом і не послаблює доказовості гарантій стаціонарного випадку. Перспективи подальших досліджень – імітаційне моделювання методу проти раціонального адверсарія в гетерогенних P2P- та оверлейних середовищах із параметрами, відкаліброваними за вимірними даними, а також аналіз стійкості RL-агента до спрямованих маніпуляцій спостереженнями.

Подальші дослідження доцільно зосередити на трьох взаємодоповнюваних напрямках. По-перше, на побудові емпіричної бази для калібрування коефіцієнтів a_m , a_λ , a_Δ , b_m , b_λ та функціональної форми $Sec(\theta)$ за телеметрією реальних оверлейних розгортань – зокрема, mesh-мереж та інфраструктурних P2P-репозиторіїв – з оцінкою довірчих інтервалів параметрів і чутливості оптимуму до похибок калібрування. По-друге, на врахуванні

апаратної гетерогенності вузлів через індивідуальні бюджети хибних відключень $\varepsilon_{\max}$ і ваги критеріїв w_1, w_2, w_3 , що узгоджується з обмеженнями базового підходу, зазначеними в постановці завдання. Нарешті, перспективним є розширення моделі раціонального адверсарія – включенням крипто-економічних стимулів у функцію цінності атаки V_A й аналізом стійкості оптимуму до спрямованих маніпуляцій спостереженнями RL-агента.

ЛІТЕРАТУРА

- [1] Douceur J. R. The Sybil Attack. Peer-to-Peer Systems : IPTPS 2002 / eds. P. Druschel, F. Kaashoek, A. Rowstron. Berlin ; Heidelberg : Springer, 2002. P. 251–260. (Lecture Notes in Computer Science ; vol. 2429). DOI: 10.1007/3-540-45748-8_24.
- [2] Пархоменко І. І., Огієвич Р. В. Криптоекономічна стійкість децентралізованої мережі з використанням випадкових часових члендждж-токенів (RTCT). Кібербезпека: освіта, наука, техніка. 2025. № 4 (28). С. 465–477. DOI: 10.28925/2663-4023.2025.28.817.
- [3] Dwork C., Naor M. Pricing via Processing or Combatting Junk Mail. Advances in Cryptology – CRYPTO '92 / ed. E. F. Brickell. Berlin ; Heidelberg : Springer, 1993. P. 139–147. (Lecture Notes in Computer Science ; vol. 740). DOI: 10.1007/3-540-48071-4_10.
- [4] Li F., Mittal P., Caesar M., Borisov N. SybilControl: Practical Sybil Defense with Computational Puzzles. Proceedings of the 7th ACM Workshop on Scalable Trusted Computing (STC '12). New York : ACM, 2012. P. 67–78. DOI: 10.1145/2382536.2382548.
- [5] Budish E. Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains. The Quarterly Journal of Economics. 2025. Vol. 140, No. 1. P. 1–62. DOI: 10.1093/qje/qjae033.
- [6] Boneh D., Bonneau J., Bünz B., Fisch B. Verifiable Delay Functions. Advances in Cryptology – CRYPTO 2018 / eds. H. Shacham, A. Boldyreva. Cham : Springer, 2018. P. 757–788. (Lecture Notes in Computer Science; vol. 10991). DOI: 10.1007/978-3-319-96884-1_25.
- [7] Percival C. Stronger Key Derivation via Sequential Memory-Hard Functions : BSDCan 2009. Ottawa, 2009. 16 p.
- [8] Biryukov A., Dinu D., Khovratovich D. Argon2: New Generation of Memory-Hard Functions for Password Hashing and Other Applications. 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Saarbrücken : IEEE, 2016. P. 292–302. DOI: 10.1109/EuroSP.2016.31.
- [9] Lamport L. Time, Clocks, and the Ordering of Events in a Distributed System. Communications of the ACM. 1978. Vol. 21, No. 7. P. 558–565. DOI: 10.1145/359545.359563.
- [10] Lee S., Bak Y. Looking for Attention: Randomized Attention Test Design for Validator Monitoring in Optimistic Rollups : preprint. 2025. arXiv:2505.24393.
- [11] Cho J.-H., Sharma D. P., Alavizadeh H. et al. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. IEEE Communications Surveys & Tutorials. 2020. Vol. 22, No. 1. P. 709–745. DOI: 10.1109/COMST.2019.2963791.
- [12] Sengupta S., Chowdhary A., Sabur A. et al. A Survey of Moving Target Defenses for Network Security. IEEE Communications Surveys & Tutorials. 2020. Vol. 22, No. 3. P. 1909–1941. DOI: 10.1109/COMST.2020.2982955.
- [13] Sutton R. S., Barto A. G. Reinforcement Learning: An Introduction. 2nd ed. Cambridge, MA : MIT Press, 2018. 552 p.
- [14] Nguyen T. T., Reddi V. J. Deep Reinforcement Learning for Cyber Security. IEEE Transactions on Neural Networks and Learning Systems. 2023. Vol. 34, No. 8. P. 3779–3795. DOI: 10.1109/TNNLS.2021.3121870.
- [15] Mukherjee A., Kumar V., Jorswieck E. A. et al. On the Optimality of the Stationary Solution of Secrecy Rate Maximization for MIMO Wiretap Channel. IEEE Wireless Communications Letters. 2022. Vol. 11, No. 2. P. 357–361. DOI: 10.1109/LWC.2021.3128331.
- [16] Noda S., Okumura K., Hashimoto Y. An Economic Analysis of Difficulty Adjustment Algorithms in Proof-of-Work Blockchain Systems. International Economic Review. 2026. Vol. 67, No. 1. P. 259–285. DOI: 10.1111/iere.70028.
- [17] Halfin S., Whitt W. Heavy-Traffic Limits for Queues with Many Exponential Servers. Operations Research. 1981. Vol. 29, No. 3. P. 567–588. DOI: 10.1287/opre.29.3.567.

Огієвич Р. В., Пархоменко І. І.

АДАПТИВНА БАГАТОКРИТЕРІАЛЬНА ОПТИМІЗАЦІЯ RTCT-ПЕРЕВІРКИ В ДЕЦЕНТРАЛІЗОВАНИХ ОВЕРЛЕЙНИХ МЕРЕЖАХ

Децентралізовані оверлейні мережі – однорангові системи, інфраструктури Інтернету речей, mesh- та MANET-середовища, а також реєр-рівень Web3-екосистем – функціонують без єдиного центру координації та довіреного органу сертифікації, що унеможливорює гарантовану перевірку унікальності учасників і відкриває простір для атаки Сивілли та її похідних: отруєння таблиць розподіленого зберігання, затемнення вузла, штучного підсилення репутації й утримання вигідної маршрутної позиції. Механізм випадкових часових членддж-токенів (RTCT) зміщує захист із разового контролю входу на контроль підтримання участі, проте його практична придатність визначається вибором параметрів перевірки – складності завдання, інтенсивності викликів і ширини вікна відповіді. Базові детерміновані схеми коригування складності керують єдиним параметром, реагують лише на агреговане відхилення часу й нечутливі до апаратної гетерогенності вузлів. У статті удосконалено метод адаптивного налаштування параметрів контролю участі: здійснено перехід від коригування лише складності до аналітичної багатокритеріальної оптимізації трійки параметрів RTCT-перевірки за критеріями стійкості до атак та обчислювальних і комунікаційних накладних витрат чесних вузлів. Задачу скаляризовано зваженою зорткою, ваги якої параметризують границю Парето. Оптимум характеризується умовами Каруша–Куна–Таккера за припущень увігнутості показника стійкості й опуклості функцій накладних витрат, що забезпечує єдиність глобального розв’язку незалежно від алгоритму пошуку. Аналіз умов першого порядку дає змістовний принцип налаштування: вікно відповіді звужують доти, доки це дозволяє бюджет хибних відключень чесних вузлів, а інтенсивність і складність добирають за вирівнюванням граничного приросту стійкості на одиницю накладних витрат. Лінійне масштабування ресурсу зловмисника з кількістю фіктивних ідентичностей обґрунтовано засобами теорії масового обслуговування. На модельному ілюстративному прикладі продемонстровано інтер’єрний оптимум та його порівняльну статистику, узгоджену з вимогами адаптивності. Для нестационарних режимів окреслено опціональну реалізацію добору параметрів як марковського процесу прийняття рішень із розв’язанням засобами навчання з підкріпленням, що надбудовується над аналітичним оптимумом і не послаблює доказовості гарантій.

Ключові слова: кібербезпека; Сивілла; RTCT; оверлей; P2P; оптимізація; KKT; адаптивність; криптоекономіка.

Ohiiievych R., Parkhomenko I.

ADAPTIVE MULTI-CRITERIA OPTIMIZATION OF RTCT VERIFICATION IN DECENTRALIZED OVERLAY NETWORKS

Decentralized overlay networks – peer-to-peer systems, Internet-of-Things infrastructures, mesh and MANET environments, and the peer layer of Web3 ecosystems – operate without a single coordination center or trusted certification authority, which makes guaranteed verification of participant uniqueness impossible and opens the way to the Sybil attack and its derivatives: distributed-storage table poisoning, node eclipsing, artificial reputation inflation, and retention of an advantageous routing position. The mechanism of random time challenge tokens (RTCT) shifts protection from one-off admission control to participation-retention control; however, its practical suitability is determined by the choice of verification parameters – puzzle difficulty, challenge intensity, and response-window width. Baseline deterministic difficulty-adjustment schemes control a single parameter, react only to aggregate timing deviation, and are insensitive to the hardware heterogeneity of nodes. This article improves the method of adaptive tuning of participation-control parameters: the approach moves from adjusting difficulty alone to analytical multi-criteria optimization of the RTCT verification triple under the criteria of attack resistance and the computational and communication overhead of honest nodes. The problem is scalarized by a weighted sum whose weights parameterize the Pareto frontier. The optimum is characterized by the Karush–Kuhn–Tucker conditions under the assumptions of concavity of the security index and convexity of the overhead functions, which guarantees a unique global solution independent of the search algorithm. Analysis of the first-order conditions yields a meaningful tuning principle: the response window is tightened only as far as the honest-node false-positive budget permits, while intensity and difficulty are set by equalizing the marginal gain in resistance per unit of overhead. The linear scaling of the adversary’s resources with the number of fake identities is justified by queueing theory. A model illustrative example demonstrates the interior optimum and its comparative statics, consistent with the requirements of adaptivity. For non-stationary regimes, an optional realization of parameter selection as a Markov decision process solved by reinforcement learning is outlined, which is built on top of the analytical optimum and does not weaken the provability of the guarantees.

Keywords: cybersecurity; Sybil; RTCT; overlay; P2P; optimization; KKT; adaptivity; crypto-economics.

Дата першого надходження: 05.06.2026 р.

Дата прийняття до друку: 14.08.2026 р.

Дата публікації: 10.09.2026 р.