

**Огісвич Роман Віталійович**

аспірант кафедри кібербезпеки та захисту інформації

Київський національний університет імені Тараса Шевченка, Київ, Україна

ORCID: 0009-0003-7948-1125

ohiievychr@fit.knu.ua

Пархоменко Іван Іванович

кандидат технічних наук, доцент,

завідувач кафедри кібербезпеки та захисту інформації

Київський національний університет імені Тараса Шевченка, Київ, Україна

ORCID: 0000-0001-6889-9284

ivan.parkhomenko@knu.ua

**ДОПУСТИМА ОБЛАСТЬ ПАРАМЕТРІВ RTCT-ПЕРЕВІРКИ В ДЕЦЕНТРАЛІЗОВАНИХ
ОВЕРЛЕЙНИХ МЕРЕЖАХ**

Анотація. У статті побудовано допустиму область параметрів перевірки на основі випадкових часових челендж-токенів (Random Time Challenge Tokens, RTCT) у децентралізованих оверлейних мережах як перетин обмеження зверху на частку хибних пропусків чесних вузлів і обмеження знизу на вартість підтримання множини фіктивних ідентичностей. Закон хибного пропуску відповіді виведено з розподілу часу розв'язання головоломки, тому він залежить від складності виклику; мінімальне вікно відповіді слід обчислювати за найповільнішим допустимим вузлом, інакше частка хибних пропусків у гетерогенній популяції недооцінюється у 5,8 раз. Місткість супротивника для обслуговування k ідентичностей визначено як розв'язок задачі про систему з відмовами за формулою Ерланга, нечутливою до розподілу часу розв'язання, і вона має два режими за k . Доведено, що за обмеження на частку процесорного часу чесного вузла та лінійних цін ресурсів питомі витрати супротивника на обчислення мають асимптотичну стелю, що не залежить ні від складності, ні від інтенсивності перевірок; за публічними цінами енергії та оренди обчислень вона становить близько $6 \cdot 10^{-4}$ EUR на ідентичність за добу, що на порядок нижче за вартість мережевої присутності. Стимульований ефект RTCT забезпечує примусова повторюваність витрат входу, а не обчислювальна вартість: кількість ідентичностей, які можна утримувати без обслуговування, визначають час виселення і час відновлення дефіцитного ресурсу входу. За строго зростаючого показника безпеки з додатним граничним ефектом на межі завантаження оптимум параметрів є кутовим розв'язком на обмеженнях чесною стороною, а множник Лагранжа обмеження завантаження є тіньовою ціною безпеки. Результати перевірено методом Монте-Карло.

Ключові слова: атака Сивілли; контроль участі; децентралізована оверлейна мережа; челендж-токен; допустима область; частка хибних пропусків; формула Ерланга; криптоекономічна вартість атаки; умови Каруша – Куна – Таккера.

ВСТУП

Децентралізовані оверлейні мережі (розподілені хеш-таблиці, пірингові сховища, мережі поширення блоків) не мають центру, який засвідчував би унікальність учасника. Тому один суб'єкт може створити довільну кількість ідентичностей і, захопивши ними частку таблиць маршрутизації чи реплік, порушити роботу мережі. Таку атаку Сивілли описано в [1], а її похідні (атаку затемнення, отруєння таблиць маршрутизації, утримання позиції на маршруті) продемонстровано на практиці: в IPFS кілька десятків фіктивних ідентичностей поблизу цільового ключа цензурують вміст за незначних витрат [2]. Відомі методи протидії роблять ідентичність дорогою: вимагають розв'язати головоломку під час входу [3], [4] або прив'язують ідентичність до дефіцитного ресурсу [5].

Випадкові часові челендж-токени (Random Time Challenge Tokens, RTCT) переносять витрати супротивника з моменту створення фіктивних ідентичностей на весь час їх утримання. У непередбачувані моменти ідентичність отримує криптографічний виклик і має надати перевірюваний токен-відповідь у



межах жорсткого вікна, інакше її довіра знижується аж до виселення [6], [7]. Токен є перевірюваним об'єктом-відповіддю, не фінансовим активом: «спалення» токена в [6] означає неможливість повторного використання, а незворотність витрат забезпечує обчислення, яке займає обчислювальну одиницю на час розв'язання. У [6] побудовано криптоекономічну модель вартості атаки з RTCT, у [7] описано протокол і оцінено його стійкість імітаційним моделюванням, у [8] поставлено задачу адаптивної оптимізації трійки параметрів перевірки: складності m , інтенсивності λ і вікна відповіді Δ .

Постановка проблеми. Зі збільшенням складності та інтенсивності перевірок зростають витрати супротивника; разом із ними зростають навантаження на чесні вузли й частка тих, що не встигають відповісти у вікні Δ і безпідставно зазнають санкцій. У [6], [7] першу сторону розглянуто докладно, а другу розглянуто без кількісних оцінок; у [8] бюджет хибних відхилень задано на один виклик без зв'язку з горизонтом і правилом виселення, а закон пропуску вікна постульовано як показникове спадання з Δ зі сталою Δ_c , не пов'язаною зі складністю m . Друга проблема стосується вартості атаки. У [6], [7] її обчислено як сумарний обсяг роботи, пропорційний кількості фіктивних ідентичностей k , і ця пропорційність виконується тотожно за побудовою. У [8] за нормування потужності чесного вузла одиницею зроблено висновок про k -кратну потужність супротивника, хоча чесний вузол зайнятий викликами тільки частку $\lambda t_{\text{solve}} \ll 1$ часу.

Аналіз останніх досліджень і публікацій. У [1] показано, що без логічно централізованого засвідчення атака Сивілли можлива завжди, а перевірка ресурсів обмежує кількість ідентичностей супротивника відношенням його ресурсів до ресурсів найслабшого учасника; за оглядом [5], сильну стійкість у бездозвільних мережах забезпечують механізми, що прив'язують ідентичність до дефіцитного ресурсу. Обчислювальні головоломки як ціну за дію введено в [3], а постійне поширення свіжих викликів проти повторного використання розв'язків запропоновано в [4]. Періодичну перевірку реалізовано в SybilControl [9]: сусідів, які не розв'язали чергову головоломку, замінюють ціною близько 1 % успішності пошуку в моделюванні Chord.

Розподіл часу розв'язання головоломки залежить від її типу: для пошуку часткового прообразу хешу кількість спроб має геометричний розподіл, а межі прискорення спеціалізованим обладнанням немає; для функцій із перевірюваною затримкою (VDF) [10] час розв'язання послідовний і детермінований, а для функцій, жадібних до пам'яті [11], обмежений пропускну здатністю пам'яті. Економічне підґрунтя дає модель [12]: повторювані («потоківі») витрати на підтримання довіри мають бути великими порівняно з одноразовою вигодою від атаки; модель постійних витрат на участь запропоновано в [6], а умову безпеки з поточковим членом на рівні контролю участі сформульовано в [8]. За вимірюваннями в IPFS пробивання NAT вдається приблизно у 70 % випадків [13]; решта чесних вузлів досяжна через ретранслятор, що збільшує затримку.

Метою статті є побудова допустимої області параметрів RTCT-перевірки як перетину обмеження зверху на частку хибних пропусків чесних вузлів і обмеження знизу на вартість утримання фіктивних ідентичностей, а також з'ясування її непорожності та положення оптимуму. Завдання: вивести закон хибного пропуску з параметрів головоломки та гетерогенності вузлів і нижню межу вікна Δ ; визначити місткість супротивника як розв'язок задачі про систему з відмовами; встановити стелю питомої вартості утримання ідентичності; з'ясувати джерело стримування; охарактеризувати оптимум трійки (m, λ, Δ) за умовами Каруша – Куна – Таккера; перевірити результати методом Монте-Карло.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Головоломка та час її розв'язання. Вважатимемо, що момент виклику непередбачуваний для супротивника, а потоки викликів до різних ідентичностей незалежні й пуассонівські (A1); повторний вхід виселеної ідентичності потребує ресурсу, що не відновлюється миттєво (A2); атака потребує безперервної присутності ідентичностей (A3); ціни енергії й оренди обчислень лінійні. Складність виклику m означимо як двійковий логарифм очікуваного обсягу елементарної роботи: головоломка потребує в середньому $W(m) = 2^m$ операцій (обчислень хешу або послідовних піднесень до квадрата). Для вузла з продуктивністю h операцій за секунду час розв'язання на одній обчислювальній одиниці дорівнює

$$t_1(m) = \frac{2^m}{h} \quad (1)$$

Для пошуку часткового прообразу кількість спроб має геометричний розподіл із параметром 2^{-m} , і вже для $m \geq 12$ час розв'язання близький до показникового із середнім $t_1(m)$; для послідовної головоломки типу VDF він детермінований і дорівнює $t_1(m)$ незалежно від кількості паралельних одиниць [10]. Композитну головоломку з часткою послідовної роботи $\sigma \in [0; 1]$ на P паралельних одиницях описує закон Амдала:



$$t_{\text{solve}}(m, P, \sigma) = t_1(m) \left[\sigma + (1 - \sigma) \frac{X}{P} \right], \quad X \sim \text{Exp}(1) \quad (2)$$

де X позначає випадковість пошукової частини ($X \equiv 1$ при $\sigma = 1$). З (2) випливає, що за будь-якого P паралелізм прискорює розв'язання не більше ніж у $1/\sigma$ разів; параметр послідовності σ з [8] задає цю межу, але «незалежності від обладнання» не гарантує. Для хешових головоломок ($\sigma = 0$) межі прискорення немає.

Закон хибного пропуску та нижня межа вікна. Чесний вузол відповідає на виклик протягом часу $R_h = \text{RTT} + t_{\text{solve}}(m, 1, \sigma)$, де RTT позначає мережеву затримку туди й назад (зсунутий гамма-розподіл із мінімумом d_0). Виклики він обслуговує послідовно, з чергою; за завантаження $a_h \leq \rho_{\text{max}}$ поправка на чергу для $\sigma = 0$ (система М/М/1) множить обчислювальну частину (5) не більше ніж на $1/(1 - \rho_{\text{max}}) \approx 1,05$, що враховано нижче як запас. Далі розрізняємо хибний пропуск (чесний вузол не вклався у вікно Δ , яке відлічує викликач), хибне відхилення (санкцію за пропуск) і хибне виселення (втрата участі після серії пропусків). Згідно з (2) умовна ймовірність хибного пропуску для чесного вузла з продуктивністю h за фіксованої затримки RTT дорівнює

$$p_{\text{fp}}(\Delta, m, \sigma) = \begin{cases} 1, & \Delta \leq \text{RTT} + \sigma t_1(m), \\ \exp\left(-\frac{\Delta - \text{RTT} - \sigma t_1(m)}{(1 - \sigma) t_1(m)}\right), & \Delta > \text{RTT} + \sigma t_1(m). \end{cases} \quad (3)$$

У граничному випадку $\sigma = 0$ і нехтовно малої затримки (3) набуває вигляду $p_{\text{fp}} = \exp(-\Delta/\Delta_c)$, що відтворює закон (9) з [8] і виражає його сталу через параметри головоломки: $\Delta_c = t_1(m) = 2^m/h$. Оскільки Δ_c зростає зі складністю показниково, оптимізацію за Δ не можна відокремити від оптимізації за m , і замкнені вирази в [8], побудовані на такому роз'єднанні, втрачають силу. Для $\sigma = 1$ закон (3) є сходиною в точці $\Delta = \text{RTT} + t_1(m)$.

Допустиме значення p_{fp} не можна задавати на один виклик: за λL викликів протягом горизонту L імовірність безпідставного виселення чесного вузла прямує до одиниці. Якщо виселення настає після j^* пропусків поспіль, а бюджет хибних виселень становить δ на вузол за горизонт L , то для малих ε імовірність появи серії з j^* пропусків серед λL викликів приблизно дорівнює $\lambda L \varepsilon^{j^*}$, звідки

$$\varepsilon_{\text{max}} = \left(\frac{\delta}{\lambda L}\right)^{1/j^*} \quad (4)$$

Вимога $p_{\text{fp}} \leq \varepsilon_{\text{max}}$ для кожного допустимого чесного вузла, зокрема для найповільнішого з продуктивністю h_{min} , з (3) дає нижню межу вікна

$$\Delta_{\text{min}}(m, \sigma) = d^{(q)} + \frac{2^m}{h_{\text{min}}} \left[\sigma + (1 - \sigma) \ln \frac{1}{\varepsilon_{\text{max}}} \right] \quad (5)$$

де $d^{(q)}$ позначає q -квантиль затримки ($q = 0,99$ для $\sigma = 0$; для $\sigma = 1$ потрібно $q \geq 1 - \varepsilon_{\text{max}}$).

Навантаження чесного вузла та система з відмовами супротивника. Виклики надходять до кожної ідентичності пуассонівським потоком інтенсивності λ (с^{-1}), а до супротивника з k ідентичностями сумарним потоком $k\lambda$ [8] (за вибору комітетів фіксованого розміру потоки від'ємно корельовані, і формула Ерланга дає верхню оцінку місткості). Навантаження від викликів на одну обчислювальну одиницю (в ерлангах) дорівнює добутку інтенсивності на середній час розв'язання; для чесного вузла з однією одиницею воно збігається з часткою процесорного часу:

$$a_h = \lambda t_1(m) = \frac{\lambda 2^m}{h} \quad (6)$$

Якщо вікно не залишає запасу понад час розв'язання, обслуговування викликів є системою з відмовами (виклик без вільної одиниці втрачається); якщо запас є, система з відмовами дає верхню оцінку потрібної місткості. Для c одиниць і навантаження a ймовірність втрати дає формула Ерланга

$$P_B(c, a) = \frac{a^c/c!}{\sum_{j=0}^c a^j/j!} \quad (7)$$

яка за теоремою Севастьянова [14] залежить від часу обслуговування лише через його середнє (і придатна для детермінованого часу VDF). Щоб не вирізнятися серед чесних вузлів часткою пропусків, супротивник має втрачати не більшу частку викликів, ніж допускається для чесного вузла, і має утримувати

$$c^*(k) = \min\{c \in \mathbb{N}: P_B(c, ka_A) \leq \varepsilon_{\text{max}}\}, \quad a_A = \frac{\lambda 2^m}{h_A} \quad (8)$$

одиниць із продуктивністю h_A кожна. Для великого навантаження $a = ka_A \rightarrow \infty$ з (7) впливає асимптотика системи з відмовами [15]:

$$c^*(k) = a + z_\varepsilon \sqrt{a} + o(\sqrt{a}), \quad \frac{\phi(z_\varepsilon)}{\Phi(z_\varepsilon)} = \varepsilon_{\text{max}} \sqrt{a}, \quad k_{\text{crit}} = \frac{1}{a_A} \quad (9)$$



де ϕ і Φ позначають щільність і функцію стандартного нормального розподілу. Величина k_{crit} розмежовує два режими: при $k \ll k_{\text{crit}}$ сумарне навантаження менше за одну одиницю, і $c^*(k)$ зростає приблизно логарифмічно, а при $k \gg k_{\text{crit}}$ зростає лінійно з нахилом a_A замість одиничного. Відношення обсягів роботи $k\lambda 2^m/(\lambda 2^m) = k$ виконується тотожно, а відношення кількостей одиниць $c^*(k)/1 \approx ka_A$ є змістовним передбаченням, яке можна перевірити, і при $a_A \ll 1$ воно значно менше за k . Цю місткість супротивник мусить утримувати безперервно, бо момент виклику непередбачуваний.

Вартість утримання ідентичностей. Чесний вузол володіє обладнанням, і його граничні витрати зводяться до енергії; супротивник, який масштабує атаку, орендує одиниці за ціною p_C (EUR за одиницю-секунду) і платить за енергію e_A джоулів на операцію за ціною p_E (EUR/Дж). Витрати супротивника за секунду становлять

$$\dot{C}_A(k) = c^*(k) p_C + k\lambda 2^m e_A p_E \quad (10)$$

Для порівняння використовуємо питомі витрати на одну ідентичність $\dot{C}_A/k$, оскільки від них залежить рішення супротивника щодо розміру k .

ДОПУСТИМА ОБЛАСТЬ ТА ХАРАКТЕРИЗАЦІЯ ОПТИМУМУ

Обмеження та множина допустимих параметрів. Нехай $\theta = (m, \lambda, \Delta)$, де $m \in \{m_{\min}, \dots, m_{\max}\} \subset \mathbb{N}$ є цілим за побудовою (кількість бітів), $\lambda, \Delta > 0$. Обмеження чесної сторони та сторони безпеки записуємо у формі $g_i(\theta) \leq 0$:

- $g_1 = \Delta_{\min}(m, \sigma) - \Delta$ – бюджет хибних пропусків (5);
- $g_2 = \lambda 2^m / (\rho_{\max} h_{\min}) - 1$ – частка процесорного часу найповільнішого допустимого вузла не перевищує $\rho_{\max}$;
- $g_3 = \lambda b_{\text{ev}} (1 + q_w(1 + f_g)) / \beta_{\max} - 1$ – пропускна здатність ($b_{\text{ev}} = 200$ Б на подію, $q_w = 2$ свідки, коефіцієнт розсилання $f_g = 4$, бюджет каналу $\beta_{\max} = 10^5$ Б/с);
- $g_4 = c_{\text{id}}^* - \lim_{k \rightarrow \infty} \dot{C}_A(k)/k$ – потрібна асимптотична питома вартість утримання ідентичності c_{id}^* (EUR на ідентичність за секунду), яку задає модель загрози;
- $g_5 = \Delta - \Delta_{\max}$ – викликач зберігає стан виклику не довше $\Delta_{\max}$;
- $g_6 = \lambda_{\min} - \lambda$, $\lambda_{\min} = j^*/(T_{\text{att}} - \Delta_{\max})$ – середня затримка виселення необслуговуваної ідентичності $j^*/\lambda + \Delta$ не перевищує масштабу часу атаки T_{att} (пунктир на рис. 3).

Допустимою областю є $\mathcal{F} = \{\theta: g_i(\theta) \leq 0, i = 1, \dots, 6\}$. Обмеження $g_1 - g_3$ і g_5 накладає чесна сторона, а обмеження g_4 і g_6 накладає сторона безпеки.

Твердження 1 (стеля обчислювальної вартості). Нехай виконується g_2 , а ціни енергії та оренди лінійні. Тоді асимптотичні питомі витрати супротивника (10) обмежені зверху стелею $\bar{c}_{\text{id}}$:

$$\lim_{k \rightarrow \infty} \frac{\dot{C}_A(k)}{k} = \lambda 2^m \left(\frac{p_C}{h_A} + e_A p_E \right) \leq \bar{c}_{\text{id}} \equiv \rho_{\max} \frac{h_{\min}}{h_A} (p_C + P_A p_E) \quad (11)$$

де $P_A = h_A e_A$ позначає споживану потужність однієї одиниці супротивника. Доведення: з (9) $c^*(k)/k \rightarrow a_A$, а енергетичний член (10) на ідентичність дорівнює $\lambda 2^m e_A p_E$; обидва пропорційні $\lambda 2^m \leq \rho_{\max} h_{\min}$ за g_2 , звідки й випливає (11). Для скінченних k питомі витрати перевищують стелю через надлишок $z_\epsilon \sqrt{a}$ і цілочисельність c^* (у вершині області у 2,1 раза при $k = 10^3$ і на 26 % при $k = 10^4$, табл. 2). Область $\mathcal{F}$ непорожня тоді й лише тоді, коли $c_{\text{id}}^* \leq \bar{c}_{\text{id}}$; вищої асимптотичної питомої вартості обчислювальна перевірка не забезпечує за жодних (m, λ, Δ) .

Твердження 2 (джерело стримування). Нехай ідентичність прив'язана до дефіцитного ресурсу входу (адреси, депозиту, засвідчення), якого супротивник має A одиниць, а після виселення одиниця ресурсу стає придатною для повторного входу через час τ_{cool} . Необслуговувану ідентичність виселяють у середньому через $T_{\text{evict}} = j^*/\lambda$. Тоді кількість одночасно живих необслуговуваних ідентичностей, яку можна підтримувати нескінченно довго, дорівнює

$$k_{\text{sust}} = A \frac{T_{\text{evict}}}{T_{\text{evict}} + \tau_{\text{cool}}}, \quad T_{\text{evict}} = \frac{j^*}{\lambda} \quad (12)$$

оскільки кожна одиниця ресурсу проводить частку $T_{\text{evict}}/(T_{\text{evict}} + \tau_{\text{cool}})$ циклу в стані «жива ідентичність». При $\tau_{\text{cool}} = 0$ маємо $k_{\text{sust}} = A$ за будь-якої λ , і миттєво відновлюваний ресурс входу стримування не створює. Якщо ж супротивник обслуговує ідентичності, він несе витрати (11) і регулярно платить за мережеву присутність кожної з них (адресу, обчислювальний вузол), тоді як за контролю на вході [3] ця плата була б одноразовою.



Твердження 3 (кутовий оптимум). Розглянемо задачу вибору $\theta \in \mathcal{F}$ за скаляризованим критерієм

$$J(\theta) = w_1 \text{Sec}(\theta) - w_2 \frac{\lambda 2^m}{\rho_{\max} h_{\min}} - w_3 \frac{\lambda b_{\text{ev}} (1 + q_w (1 + f_g))}{\beta_{\max}}, \quad w_1 + w_2 + w_3 = 1 \quad (13)$$

де всі доданки нормовано на $[0; 1]$, а Sec є неспадною увігнутою функцією асимптотичної питомої вартості (11), отже, і добутку $u = \lambda 2^m$. За фіксованого u критерій (13) не спадає зі зменшенням λ , бо комунікаційний член залежить від λ окремо, і оптимальними є найбільше m , сумісне з g_1 , g_5 і g_6 , та $\Delta = \Delta_{\min}$. За фіксованого m умови Каруша – Куна – Таккера [16] у змінних (λ, Δ) мають вигляд $\nabla J(\theta^*) = \sum_i v_i \nabla g_i(\theta^*)$, $v_i \geq 0$, $v_i g_i(\theta^*) = 0$; градієнти активних обмежень лінійно незалежні, задача за λ одновимірною увігнута, а глобальний оптимум знаходять перебором цілих m . У вершині області, де активні g_1 і g_2 , зі стаціонарності за Δ випливає $v_1 = 0$, а множник обмеження завантаження дорівнює $v_2 = w_1 \rho_{\max} h_{\min} \text{Sec}'(u^*) - w_2 - w_3 \lambda^* b_{\text{ev}} (1 + q_w (1 + f_g)) / \beta_{\max}$. Якщо $v_2 > 0$, оптимум кутовий і лежить на межі області, заданій обмеженнями чесною стороною; в алгоритмах коригування складності за ковзним середнім натомість шукають внутрішню стаціонарну точку. Якщо Sec насичується в межах $\mathcal{F}$ так, що $v_2 < 0$, оптимум за u внутрішній (випадок модельного прикладу [8]); якщо ж $\text{Sec} \equiv 0$ на $\mathcal{F}$, критерій (13) вироджується до мінімізації навантаження з оптимумом на нижніх межах $\lambda_{\min}$, $m_{\min}$. Та сама вершина максимізує досяжну асимптотичну питому вартість атаки на $\mathcal{F}$, а множник Лагранжа при обмеженні $\lambda 2^m \leq \rho_{\max} h_{\min}$, віднесений до $\rho_{\max}$, дорівнює $\partial \bar{c}_{\text{id}} / \partial \rho_{\max} = (h_{\min} / h_A)(p_C + P_A p_E)$; цей множник і є тінювою ціною безпеки, бо показує, на скільки зростає досяжна питома вартість атаки з кожною одиницею допустимої частки процесорного часу чесного вузла.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Калібрування. Значення параметрів наведено в табл. 1. Ціни ресурсів узяті з публічних джерел: найнижча в ЄС ціна електроенергії для побутових споживачів у другому півріччі 2025 р. [17] (несприятливе для захисту припущення), найдешевший опублікований тариф оренди обчислювальної одиниці (5,49 EUR на місяць за два спільні vCPU без ПДВ) [18] та IPv4-адреси [19] того самого провайдера. Продуктивності та потужності задано з точністю до порядку; результати масштабуються за ними через (5), (6) і (11).

Таблиця 1

Параметри моделі та їх калібрування (базовий варіант: хешова головоломка, $\sigma = 0$)

Параметр	Позначення	Значення	Джерело / статус
Продуктивність типового / найповільнішого допустимого вузла	$h / h_{\min}$	$10^7 / 10^6$ оп/с	припущення (ядро x86 / одноплатний ARM)
Розкид продуктивності популяції (q_{90}/q_{10}); потужність одиниці	$- ; P_A$	8; 15 Вт	припущення (логнормальний розподіл; ядро під навантаженням)
Ціна енергії для супротивника (найнижча в ЄС)	p_E	0,0748 EUR/кВт·год	[17], 2-ге півріччя 2025 р. (середня в ЄС: 0,1837)
Оренда обчислювальної одиниці / IPv4-адреси	p_C / p_{IP}	0,0038 EUR/(vCPU·год) / 0,50 EUR/міс	[18], [19], станом на 13.10.2026
Затримка RTT: мінімум; гамма-розподіл (форма; масштаб)	$d_0; \Gamma$	0,05 с; (2; 0,1 с)	припущення; $d^{(0,99)} = 0,71$ с
Пропусків до виселення; бюджет хибних виселень на вузол за рік	$j^*; \delta$	3; 0,01	припущення (EWMA-довіра, $\alpha = 0,3$; поріг $x_{\text{ban}} = 0,35$)
Гранична частка процесорного часу; гранична тривалість вікна	$\rho_{\max}; \Delta_{\max}$	0,05; 60 с	політика; чутливість на рис. 3

Закон хибного пропуску та вікно відповіді. Для опорної інтенсивності $\lambda = 1/3600$ с⁻¹ (один виклик на годину) і $j^* = 3$ формула (4) дає $\varepsilon_{\max} = 1,05 \cdot 10^{-2}$; при $j^* = 1$, коли вузол виселяють після

першого пропуску, бюджет падає до $1,1 \cdot 10^{-6}$, і обчислювальна частина вікна потроюється (115 с для $m = 23$). EWMA-довіра з параметрами табл. 1 дає $j^* = \lceil \ln x_{\text{ban}} / \ln(1 - \alpha) \rceil = 3$. Найбільша складність, сумісна з $\Delta_{\text{max}} = 60$ с за (5), становить $m = 23$ ($t_1 = 8,4$ с на найповільнішому вузлі, $\Delta_{\text{min}} = 39,0$ с; для $m = 24$ уже $\Delta_{\text{min}} = 77,2$ с); за $j^* = 2$ і $j^* = 4$ вона становить відповідно 23 і 24 біти, тож якісні висновки від вибору j^* не залежать. На рис. 1 закон (3) порівняно з моделюванням методом Монте-Карло для популяції з $2 \cdot 10^5$ відповідей, у якій продуктивність розподілена логнормально з медіаною 10^7 оп/с і розкидом 8 між 10-м і 90-м перцентилями, а затримка має зсунутий гамма-розподіл.

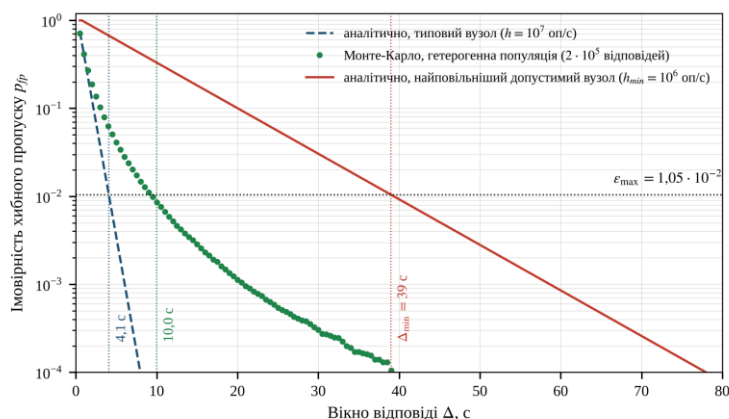


Рис. 1. Імовірність хибного пропуску відповіді для $m = 23$: аналітичний закон (3) для типового вузла (із середньою затримкою) і найповільнішого вузла (із квантилем $d^{(0,99)}$) та моделювання гетерогенної популяції; вертикальні лінії – вікна, за яких p_{fp} досягає ϵ_{max}

Якщо обчислювати вікно за законом (3) для типового вузла, бюджет ϵ_{max} досягається при $\Delta = 4,1$ с, проте частка пропусків у популяції за такого вікна становить 6,1 %, у 5,8 раза більше за допустиме, і її перевищує половина вузлів. Усереднена за популяцією частка задовольняє бюджет при $\Delta = 10,0$ с, але й тоді 12 % найповільніших вузлів перевищують річний бюджет δ . Вікно $\Delta_{\text{min}} = 39,0$ с за (5) гарантує дотримання бюджету кожним допустимим вузлом, бо його розраховано за найповільнішим вузлом; обчислювальна частина такого вікна в h/h_{min} разів довша, ніж для типового вузла.

Два режими місткості супротивника. Для $m = 23$ розглянуто дві точки: опорну ($\lambda = 1/3600$ с⁻¹) і вершину області, тобто найбільшу інтенсивність, за якої частка процесорного часу найповільнішого вузла дорівнює ρ_{max} : $\lambda = 1/168$ с⁻¹, $\Delta_{\text{min}} = 47,5$ с, $T_{\text{evict}} = 503$ с. Опорна точка задовольняє g_6 тільки при $T_{\text{att}} > 3$ год. Супротивникові приписано $h_A = h$. Результати обчислення (7)–(10) зведено в табл. 2 і на рис. 2.

Таблиця 2

Потрібна місткість і витрати супротивника на обслуговування k ідентичностей ($m = 23$, $h_A = 10^7$ оп/с)

k	$a = ka_A$	$c^*(k)$ за (8)	$a + z_\epsilon \sqrt{a}$	c_q (з чергою)	Витрати за (10), EUR/доба	На ідентичність, EUR/доба
Опорна точка: $\lambda = 1/3600$ с ⁻¹ , $\epsilon_{\text{max}} = 1,05 \cdot 10^{-2}$, $k_{\text{crit}} = 4292$						
10^3	0,233	3	1,66	1	0,277	$2,8 \cdot 10^{-4}$
10^4	2,33	7	6,21	3	0,694	$6,9 \cdot 10^{-5}$
10^5	23,3	34	33,2	24	3,69	$3,7 \cdot 10^{-5}$
10^6	233	255	254,6	234	29,3	$2,9 \cdot 10^{-5}$
Вершина області: $\lambda = 1/168$ с ⁻¹ , $\epsilon_{\text{max}} = 3,76 \cdot 10^{-3}$, $k_{\text{crit}} = 200$						
10^3	5	12	11,2	6	1,22	$1,2 \cdot 10^{-3}$
10^4	50	67	66,5	51	7,39	$7,4 \cdot 10^{-4}$
10^5	500	540	539,9	501	62,2	$6,2 \cdot 10^{-4}$
10^6	5000	5075	5075,0	5001	592	$5,9 \cdot 10^{-4}$

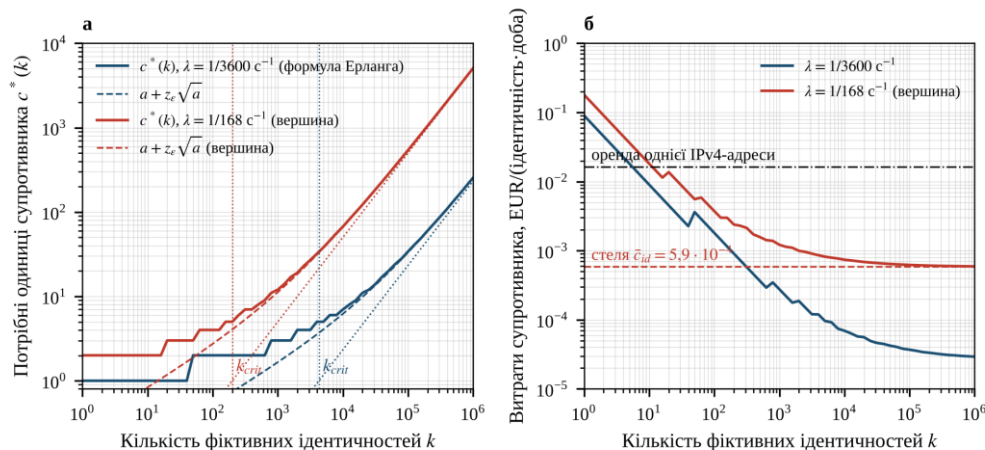


Рис. 2. Характеристики супротивника: а – місткість за формулою Ерланга (суцільні лінії), асимптотика (9) (штрихові) та навантаження ka_A (пунктир); б – питомі витрати на ідентичність, стеля (11) та, для порівняння, оренда однієї IPv4-адреси

Дані табл. 2 і рис. 2 підтверджують дворежимну залежність (9): нижче k_{crit} місткість майже не зростає, вище зростає лінійно з нахилом a_A , а асимптотика (9) відхиляється від (7) менш ніж на 2 % при $a \geq 50$. Відношення $c^*(k)/k$ прямує до a_A ($2,3 \cdot 10^{-4}$ в опорній точці і $5 \cdot 10^{-3}$ у вершині). Нормування потужності чесного вузла до одиницею в [8] приводить до одиничної границі і завищує асиметрію місткості в $1/a_A$ разів (у 4292 і 200 разів). Запас вікна $\Delta_{min} - d^{(q)}$ у 46–56 разів перевищує середній час розв'язання $t_A = 0,84$ с, і виклик у черзі встигають обслужити; формула Ерланга тут завищує місткість: оцінка для системи з очікуванням $c_q = \min\{c > a: C(c, a) e^{-(c-a)(\Delta_{min}-d^{(q)})/t_A} \leq \varepsilon_{max}\}$ (де $C(c, a)$ позначає формулу Ерланга для системи з очікуванням) дає $c_q \approx a + 1$ при $k \gg k_{crit}$. Стеля (11) і два режими від цього не залежать, а витрати за формулою Ерланга є верхніми оцінками. Нечутливість (7) до розподілу часу обслуговування підтверджено імітаційним моделюванням шести конфігурацій табл. 2 (M/D/c/c і M/M/c/c, 20 реплікацій по $5 \cdot 10^5$ надходжень): розбіжність із формулою Ерланга не перевищує 1,4 стандартної похибки середнього.

Стеля вартості та непорожність області. За твердженням 1 асимптотичні питомі витрати на утримання ідентичності обмежені стелею (11), яка для калібрування табл. 1 дорівнює $\bar{c}_{id} = 5,9 \cdot 10^{-4}$ EUR на ідентичність за добу (77 % оренда, 23 % енергія). До цієї величини сходиться крива вершини на рис. 2, б (крива опорної точки прямує до значення, у ≈ 21 раз меншого, бо g_2 там не активне). Утримання 10^6 ідентичностей коштує близько 590 EUR на добу, тоді як оренда 10^6 публічних IPv4-адрес за тарифом [19] коштувала б 16 400 EUR на добу, у 28 разів більше. Стеля лінійна за ρ_{max} і p_c та обернено пропорційна відношенню продуктивностей $\gamma_{hw} = h_A/h_{min}$: навіть за десятивідсоткового завантаження чесних вузлів і восьмикратно дорожчої оренди вона не перевищує 0,8 цента на ідентичність за добу. Для хешових головоломок на спеціалізованому обладнанні γ_{hw} сягає 10^4 – 10^5 , а для послідовних обмежене сталим множником апаратної переваги [10]. Цей висновок уточнює оцінки [6], [7]: вартість атаки зростає зі складністю показниково за означенням головоломки, проте обмеження g_2 задає верхню межу добутку $\lambda 2^m$, і на межі допустимої області питома вартість перестає зростати.

Допустиму область у площині (λ, m) при $\Delta = \Delta_{min}(m)$ зображено на рис. 3. Обмеження g_2 є в цій площині прямою $m = \log_2(\rho_{max} h_{min}/\lambda)$, обмеження вікна g_1 разом із g_5 задає горизонтальну пряму $m = m_{max}(\Delta_{max})$, а ізолінії питомої вартості паралельні g_2 , бо обидві величини залежать від добутку $\lambda 2^m$. Ізолінія, що відповідає стелі (11), збігається з межею g_2 , а будь-яка вимога $c_{id}^* > \bar{c}_{id}$, зокрема 10^{-2} або 1 EUR на ідентичність за добу, лежить цілком у недопустимій зоні; за суто обчислювальної вартості атаки області чесної сторони та сторони безпеки не перетинаються.

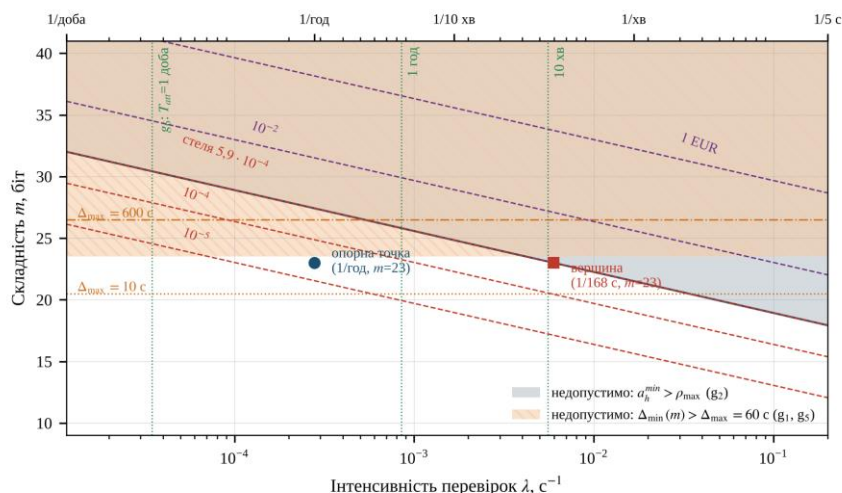


Рис. 3. Допустима область у площині (λ, m) при $\Delta = \Delta_{\min}(m)$: заштриховано зони порушення g_2 та g_1, g_5 ; штрихові лінії – ізолінії питомої вартості, EUR на ідентичність за добу; пунктир – нижні межі λ за g_6 для масштабів часу атаки T_{att}

Кутовий розв'язок. Для критерію, строго зростаючого за вартістю, з $v_2 > 0$ максимум досягається у вершині, де активні g_2 і g_1 , а $m = 23$ є найбільшим цілим, за якого $\Delta_{\min}(m) \leq \Delta_{\max}$: $\lambda = 1/168 \text{ c}^{-1}$, $\Delta = 47,5 \text{ c}$. Для Sec у вигляді частки стриманих супротивників за паретівського розподілу їхніх бюджетів (показник 1,5; масштаб 10^{-6} EUR/c) і $w_1 = w_2 = 0,5$ стеля (11) у ≈ 150 разів нижча за масштаб бюджетів, тому $\text{Sec} \equiv 0$ на всій області і критерій вироджується до мінімізації навантаження. Формальна стаціонарна точка продовженої функції при $\lambda = 1/3600 \text{ c}^{-1}$ лежить при $m \approx 32,0$ (завантаження найповільнішого вузла у ≈ 24 рази більше за $\rho_{\max}$, вікно (5) близько 5 год). За реалістичного калібрування внутрішнього оптимуму в $\mathcal{F}$ немає; вершина є оптимумом, якщо вимога безпеки лежить нижче стелі, а граничний ефект безпеки в ній перевищує граничні накладні витрати. Тінюва ціна безпеки $\partial \bar{c}_{id} / \partial \rho_{\max}$ становить $1,2 \cdot 10^{-4} \text{ EUR}$ на ідентичність за добу на кожен відсоток дозволеного завантаження найповільнішого вузла.

Стимування через ресурс входу. Частка k_{sust}/A за (12) при $j^* = 3$ сильно залежить від часу відновлення ресурсу: в опорній точці ($T_{\text{evict}} = 3 \text{ год}$) з добовим відновленням ресурсу без обслуговування можна утримувати 11 % одиниць, з місячним відновленням 0,4 %; у вершині ($T_{\text{evict}} = 8,4 \text{ хв}$) годинне відновлення зменшує частку до 12 %, а добове зменшує її до 0,6 %. Обслуговування ідентичності протягом T_{evict} коштує супротивникові $\bar{c}_{id} T_{\text{evict}} = j^* 2^m \kappa$, де $\kappa = p_c/h_A + e_A p_E$ позначає вартість операції; для $m = 23$ добуток $j^* 2^m \kappa$ дорівнює $3,4 \cdot 10^{-6} \text{ EUR}$. Відмова від обслуговування коштує повторного входу C_{entry} , втрати позиції L_{pos} і утримання ресурсу під час відновлення $p_{\text{res}} \tau_{\text{cool}}$, тому раціональний супротивник обслуговує ідентичності, щойно $C_{\text{entry}} + L_{\text{pos}} + p_{\text{res}} \tau_{\text{cool}} > j^* 2^m \kappa$. За калібрування табл. 1 ця умова виконується для будь-якого ненульового ресурсу входу (для орендованої IPv4-адреси вже при $\tau_{\text{cool}} \approx 18 \text{ c}$), і витрати на ресурс присутності стають повторюваними. Підтримувати безперервну присутність супротивника змушують непередбачуваність моменту виклику і жорстке вікно відповіді; складність головоломки на цей ефект майже не впливає.

Межі застосовності. Результати справедливі за припущень (A1)–(A3); якщо змінити калібрувальні продуктивності на порядок, на той самий порядок зміняться стеля (11) і вікно (5). Кореляція затримок і недосяжність вузлів за NAT [13] збільшують p_{fp} , тож (5) є нижньою межею вікна. Варіант $\sigma = 0$ з $h_A = h$ є найсприятливішим для захисту, бо для хешових головоломок спеціалізоване обладнання на кілька порядків ефективніше за процесор; тому рекомендуємо $\sigma \rightarrow 1$ [10] або функції, жадібні до пам'яті [11], для яких відношення продуктивностей обмежене.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті побудовано допустиму область параметрів RTCT-перевірки як перетин обмежень чесної сторони й сторони безпеки та охарактеризовано її оптимум. Основні результати такі.

- Закон хибного пропуску відповіді виведено з розподілу часу розв'язання головоломки та затримки: його стала дорівнює $2^m/h$, що зв'яже вікно відповіді зі складністю, а нижню межу вікна (5) слід обчислювати за найповільнішим допустимим вузлом; обчислення за типовим вузлом недооцінює



частку хибних пропусків у гетерогенній популяції в 5,8 раза.

- Місткість супротивника визначено як розв'язок задачі про систему з відмовами за формулою Ерланга; її залежність від кількості ідентичностей має два режими з межею $k_{crit} = 1/a_A$, а опубліковане раніше твердження про k -кратну асиметрію є тотожністю для обсягів роботи й завищує асиметрію місткості в $1/a_A$ разів (у 200–4300 разів для розглянутих точок).
- Доведено, що за обмеження частки процесорного часу чесного вузла та лінійних цін ресурсів питомі витрати супротивника на обчислення асимптотично обмежені стелею (11), що не залежить ні від складності, ні від інтенсивності перевірок; за публічними цінами ресурсів вона становить близько $6 \cdot 10^{-4}$ EUR на ідентичність за добу, і для будь-якої вищої вимоги область допустимих параметрів порожня.
- Стимувальний ефект RTCT породжує примусова повторюваність витрат входу: кількість ідентичностей, утримуваних без обслуговування, визначає відношення (12), а за миттєвого відновлення ресурсу стримування відсутнє.
- За строго зростаючого показника безпеки з додатним граничним ефектом на межі завантаження оптимум трійки (m, λ, Δ) є кутовим розв'язком на обмеженнях чесної сторони; за реалістичного калібрування внутрішньої стаціонарної точки в допустимій області немає, а множник Лагранжа обмеження завантаження є тінювою ціною безпеки.

Практичне значення результатів полягає в процедурі вибору параметрів: задати бюджет хибних виселень і допустиме завантаження найслабшого вузла, обчислити вікно (5) і вершину області, оцінити стелю (11) і порівняти її з ціною ресурсу входу. Подальші дослідження передбачають перевірку дворежимної залежності на імітаційній моделі мережі з раціональним супротивником, вимірювання p_{fr} за корельованого відтоку й недосяжності вузлів за NAT, модель довіри з накопиченням віку присутності та призначенням перевірок за фактом використання ідентичності, а також оцінювання стелі (11) для послідовних і жадібних до пам'яті головоломок на реальному обладнанні.

ДЕКЛАРАЦІЯ ПРО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Під час підготовки статті автори використовували великі мовні моделі Claude (Anthropic, 2026) для збору та перевірки бібліографічної інформації й для редагування тексту. Наукові положення, розрахунки, рисунки та висновки належать авторам і перевірені ними; автори несуть повну відповідальність за зміст статті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Douceur, J. R. (2002). The Sybil attack. In Peer-to-Peer Systems (IPTPS 2002), LNCS 2429 (pp. 251–260). Springer. https://doi.org/10.1007/3-540-45748-8_24
2. Sridhar, S., Ascigil, O., Keizer, N., Genon, F., Pierre, S., Psaras, Y., Rivière, E., & Król, M. (2024). Content censorship in the InterPlanetary File System. In Proceedings of the 2024 Network and Distributed System Security Symposium (NDSS 2024). Internet Society. <https://doi.org/10.14722/ndss.2024.23153>
3. Dwork, C., & Naor, M. (1993). Pricing via processing or combatting junk mail. In Advances in Cryptology – CRYPTO '92, LNCS 740 (pp. 139–147). Springer. https://doi.org/10.1007/3-540-48071-4_10
4. Borisov, N. (2006). Computational puzzles as Sybil defenses. In Sixth IEEE International Conference on Peer-to-Peer Computing (P2P'06) (pp. 171–176). IEEE. <https://doi.org/10.1109/P2P.2006.10>
5. Platt, M., & McBurney, P. (2023). Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance. Algorithms, 16(1), Article 34. <https://doi.org/10.3390/a16010034>
6. Пархоменко, І., & Огієвич, Р. (2025). Криптоекономічна стійкість децентралізованої мережі з використанням випадкових часових члендж-токенів (RTCT). Кібербезпека: освіта, наука, техніка, 4(28), 465–477. <https://doi.org/10.28925/2663-4023.2025.28.817>
7. Parkhomenko, I., Myrutenko, L., Ohiievych, R., & Laptiev, O. (2026). Improving resistance to Sybil attacks in decentralized networks using the RTCT protocol. In Proceedings of the Workshop on Cyber Security and Data Protection (CSDP 2026), Lviv, Ukraine, May 7, 2026 (CEUR Workshop Proceedings, Vol. 4223, pp. 55–72). CEUR-WS.org. <https://ceur-ws.org/Vol-4223/paper5.pdf>
8. Огієвич, Р., & Пархоменко, І. (2026). Адаптивна багатокритеріальна оптимізація RTCT-перевірки в децентралізованих оверлейних мережах. Наукоємні технології, 71(3), 373–381. <https://doi.org/10.18372/2310-5461.71.21453>
9. Li, F., Mittal, P., Caesar, M., & Borisov, N. (2012). SybilControl: Practical Sybil defense with



- computational puzzles. In Proceedings of the Seventh ACM Workshop on Scalable Trusted Computing (STC '12) (pp. 67–78). ACM. <https://doi.org/10.1145/2382536.2382548>
10. Boneh, D., Bonneau, J., Bünz, B., & Fisch, B. (2018). Verifiable delay functions. In Advances in Cryptology – CRYPTO 2018, LNCS 10991 (pp. 757–788). Springer. https://doi.org/10.1007/978-3-319-96884-1_25
 11. Biryukov, A., Dinu, D., & Khovratovich, D. (2016). Argon2: New generation of memory-hard functions for password hashing and other applications. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 292–302). IEEE. <https://doi.org/10.1109/EuroSP.2016.31>
 12. Budish, E. (2025). Trust at scale: The economic limits of cryptocurrencies and blockchains. *The Quarterly Journal of Economics*, 140(1), 1–62. <https://doi.org/10.1093/qje/qjae033>
 13. Trautwein, D., Ihle, C., Schubotz, M., Breiting, C., & Gipp, B. (2026). Large-scale measurement of NAT traversal for the decentralized web: A case study of DCUtr in IPFS. In Proceedings of the 2026 ACM Internet Measurement Conference (IMC '26) (pp. 779–794). ACM. <https://doi.org/10.1145/3777912.3809138>
 14. Sevast'yanov, B. A. (1957). An ergodic theorem for Markov processes and its application to telephone systems with refusals. *Theory of Probability & Its Applications*, 2(1), 104–112. <https://doi.org/10.1137/1102005>
 15. Jagerman, D. L. (1974). Some properties of the Erlang loss function. *Bell System Technical Journal*, 53(3), 525–551. <https://doi.org/10.1002/j.1538-7305.1974.tb02756.x>
 16. Boyd, S., & Vandenberghe, L. (2004). *Convex optimization*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511804441>
 17. Eurostat. (2026, May 8). Non-household electricity prices in 2nd half of 2025: –3.5% [News article]. <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260508-2>
 18. Hetzner Online GmbH. (2026). Hetzner price adjustment 15 June 2026. Hetzner Docs. Retrieved October 13, 2026, from <https://docs.hetzner.com/general/infrastructure-and-availability/price-adjustment/>
 19. Hetzner Online GmbH. (2022). Overview [Cloud servers: Primary IPs]. Hetzner Docs. Retrieved October 13, 2026, from <https://docs.hetzner.com/cloud/servers/overview/>

**Roman Ohiiievych**

Postgraduate Student at the Department of Cybersecurity and Information Protection

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ORCID: 0009-0003-7948-1125

ohiiievychr@fit.knu.ua

Ivan Parkhomenko

Candidate of Technical Sciences, Associate Professor,

Head of CSIP Department

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ORCID: 0000-0001-6889-9284

ivan.parkhomenko@knu.ua

FEASIBLE REGION OF RTCT VERIFICATION PARAMETERS IN DECENTRALIZED OVERLAY NETWORKS

Abstract. This paper constructs the feasible region of verification parameters based on Random Time Challenge Tokens (RTCT) in decentralized overlay networks as the intersection of an upper bound on the false-miss rate of honest nodes and a lower bound on the cost of sustaining a set of fake identities. The false-miss law is derived from the distribution of the puzzle-solving time and therefore depends on the challenge difficulty; the minimum response window must be computed for the slowest tolerated node, otherwise the false-miss rate in a heterogeneous population is underestimated by a factor of 5.8. The capacity an adversary needs to service k identities is found from an Erlang loss-system staffing problem, insensitive to the distribution of the solving time, and has two regimes in k . It is proved that, when the CPU duty cycle of an honest node is bounded and resource prices are linear, the adversary's per-identity computing cost has an asymptotic ceiling independent of both the difficulty and the challenge intensity; with public energy and compute-rental prices it is about $6 \cdot 10^{-4}$ EUR per identity per day, far below the cost of network presence. The deterrent effect of RTCT therefore rests on the enforced recurrence of entry costs rather than on computing cost: the number of identities that can be held without servicing is set by the eviction time and the recovery time of the scarce entry resource. For a strictly increasing security index with a positive marginal effect at the load bound, the optimum is a corner solution on the honest-side constraints, and the Lagrange multiplier of the load constraint is the shadow price of security. The results were verified by Monte Carlo simulation.

Keywords: Sybil attack; participation control; decentralized overlay network; challenge token; feasible region; false-miss rate; Erlang formula; crypto-economic attack cost; Karush–Kuhn–Tucker conditions.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Douceur, J. R. (2002). The Sybil attack. In Peer-to-Peer Systems (IPTPS 2002), LNCS 2429 (pp. 251–260). Springer. https://doi.org/10.1007/3-540-45748-8_24
2. Sridhar, S., Ascigil, O., Keizer, N., Genon, F., Pierre, S., Psaras, Y., Rivière, E., & Król, M. (2024). Content censorship in the InterPlanetary File System. In Proceedings of the 2024 Network and Distributed System Security Symposium (NDSS 2024). Internet Society. <https://doi.org/10.14722/ndss.2024.23153>
3. Dwork, C., & Naor, M. (1993). Pricing via processing or combatting junk mail. In Advances in Cryptology – CRYPTO '92, LNCS 740 (pp. 139–147). Springer. https://doi.org/10.1007/3-540-48071-4_10
4. Borisov, N. (2006). Computational puzzles as Sybil defenses. In Sixth IEEE International Conference on Peer-to-Peer Computing (P2P'06) (pp. 171–176). IEEE. <https://doi.org/10.1109/P2P.2006.10>
5. Platt, M., & McBurney, P. (2023). Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance. Algorithms, 16(1), Article 34. <https://doi.org/10.3390/a16010034>
6. Parkhomenko, I., & Ohiiievych, R. (2025). Kryptoekonomichna stiiikist detsentralizovanoi merezhi z vykorystanniam vypadkovykh chasovykh chelendzh-tokeniv (RTCT) [Crypto-economic resilience of a decentralized network using Random Time Challenge Tokens (RTCT)]. Kiberbezpeka: osvita, nauka, tekhnika, 4(28), 465–477. <https://doi.org/10.28925/2663-4023.2025.28.817>
7. Parkhomenko, I., Myrutenko, L., Ohiiievych, R., & Laptiev, O. (2026). Improving resistance to Sybil attacks



- in decentralized networks using the RTCT protocol. In Proceedings of the Workshop on Cyber Security and Data Protection (CSDP 2026), Lviv, Ukraine, May 7, 2026 (CEUR Workshop Proceedings, Vol. 4223, pp. 55–72). CEUR-WS.org. <https://ceur-ws.org/Vol-4223/paper5.pdf>
8. Ohiievych, R., & Parkhomenko, I. (2026). Adaptivna bahatokryterialna optymizatsiia RTCT-perevirky v detsentralizovanykh overleinykh merezhakh [Adaptive multi-criteria optimization of RTCT verification in decentralized overlay networks]. *Naukoiemni tekhnolohii*, 71(3), 373–381. <https://doi.org/10.18372/2310-5461.71.21453>
 9. Li, F., Mittal, P., Caesar, M., & Borisov, N. (2012). SybilControl: Practical Sybil defense with computational puzzles. In Proceedings of the Seventh ACM Workshop on Scalable Trusted Computing (STC '12) (pp. 67–78). ACM. <https://doi.org/10.1145/2382536.2382548>
 10. Boneh, D., Bonneau, J., Bünz, B., & Fisch, B. (2018). Verifiable delay functions. In *Advances in Cryptology – CRYPTO 2018*, LNCS 10991 (pp. 757–788). Springer. https://doi.org/10.1007/978-3-319-96884-1_25
 11. Biryukov, A., Dinu, D., & Khovratovich, D. (2016). Argon2: New generation of memory-hard functions for password hashing and other applications. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 292–302). IEEE. <https://doi.org/10.1109/EuroSP.2016.31>
 12. Budish, E. (2025). Trust at scale: The economic limits of cryptocurrencies and blockchains. *The Quarterly Journal of Economics*, 140(1), 1–62. <https://doi.org/10.1093/qje/qjae033>
 13. Trautwein, D., Ihle, C., Schubotz, M., Breiting, C., & Gipp, B. (2026). Large-scale measurement of NAT traversal for the decentralized web: A case study of DCUtr in IPFS. In Proceedings of the 2026 ACM Internet Measurement Conference (IMC '26) (pp. 779–794). ACM. <https://doi.org/10.1145/3777912.3809138>
 14. Sevast'yanov, B. A. (1957). An ergodic theorem for Markov processes and its application to telephone systems with refusals. *Theory of Probability & Its Applications*, 2(1), 104–112. <https://doi.org/10.1137/1102005>
 15. Jagerman, D. L. (1974). Some properties of the Erlang loss function. *Bell System Technical Journal*, 53(3), 525–551. <https://doi.org/10.1002/j.1538-7305.1974.tb02756.x>
 16. Boyd, S., & Vandenberghe, L. (2004). *Convex optimization*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511804441>
 17. Eurostat. (2026, May 8). Non-household electricity prices in 2nd half of 2025: –3.5% [News article]. <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260508-2>
 18. Hetzner Online GmbH. (2026). Hetzner price adjustment 15 June 2026. Hetzner Docs. Retrieved October 13, 2026, from <https://docs.hetzner.com/general/infrastructure-and-availability/price-adjustment/>
 19. Hetzner Online GmbH. (2022). Overview [Cloud servers: Primary IPs]. Hetzner Docs. Retrieved October 13, 2026, from <https://docs.hetzner.com/cloud/servers/overview/>

Отримано редакцією журналу / Received: 01.09.26

Прорецензовано / Revised: 16.09.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.