

DOI: <https://doi.org/10.15276/ict.03.2026.43>

УДК 004.451:502/504

Безпеково-орієнтована динамічна кластеризація вузлів розподіленої мережі з урахуванням їхнього криптографічного стану

Соловйова Діана Вячеславівна¹⁾

ORCID: <https://orcid.org/0009-0007-5253-8848>; soloviova.d.v@op.edu.ua. Scopus Author ID: 59185442400

Болтънков Віктор Олексійович¹⁾

ORCID: <https://orcid.org/0000-0003-2777-3137>; vabolttenkov@gmail.com. Scopus Author ID: 57203623617

Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

У роботі розглянуто проблему безпеково-орієнтованої динамічної кластеризації вузлів розподілених мереж з урахуванням їхнього криптографічного стану. Обґрунтовано необхідність урахування не лише ресурсних і мережевих характеристик вузлів, а й відповідності їхніх криптографічних конфігурацій установлений політиці, особливо в умовах оновлення криптографічних механізмів. Метою дослідження є розроблення та експериментальна оцінка методу кластеризації, спрямованого на зменшення локальної концентрації вузлів, що не відповідають поточним криптографічним вимогам. Запропоновано модель криптографічного стану, яка передбачає три категорії вузлів: ті, що відповідають установлений політиці, перебувають у перехідному стані або не відповідають її вимогам. Розроблено нормалізований критерій формування кластерів, який поєднує ресурсні характеристики з криптографічним станом вузлів. Для адаптації кластерної структури передбачено моніторинг та реконфігурацію в разі перевищення заданого порогу концентрації невідповідних вузлів. Проведено імітаційне моделювання та порівняння запропонованого методу з базовою кластеризацією за різних співвідношень криптографічних станів. У чотирьох експериментальних сценаріях отримано зниження середньої максимальної концентрації криптографічно невідповідних вузлів у межах від сорока трьох цілих сімдесяти восьми сотих до п'ятдесяти восьми цілих п'ятдесяти семи сотих відсотка. Дослідження масштабності для мереж із кількістю вузлів від п'ятдесяти до однієї тисячі показало зниження зазначеного показника в межах від тридцяти восьми цілих сімдесяти сотих до п'ятдесяти семи цілих сорока двох сотих відсотка. Статистична перевірка підтвердила значущість отриманих відмінностей. Динамічне моделювання продемонструвало можливість адаптації кластерної структури до зміни криптографічних станів, водночас виявивши значні витрати глобальної реконфігурації. Подальші дослідження доцільно спрямувати на розроблення локальної реконфігурації та зменшення кількості переміщень вузлів.

Ключові слова: розподілена мережа; динамічна кластеризація; криптографічний стан вузла; криптографічна політика; криптографічна гнучкість; безпеково-орієнтована кластеризація; реконфігурація кластерів; імітаційне моделювання

Для цитування: Соловйова Д. В., Болтънков В. О. “Безпеково-орієнтована динамічна кластеризація вузлів розподіленої мережі з урахуванням їхнього криптографічного стану”. *Інформатика. Культура. Техніка.* 2026; Том 3 № 2 (4): 577–587. DOI: <https://doi.org/10.15276/ict.03.2026.43>

Актуальність. Відомо, що розподілені мережі та блокчейн-мережі функціонують на основі взаємодії великої кількості вузлів, що відрізняються за обчислювальними ресурсами, мережевою зв'язністю та топологічним положенням. Зі збільшенням кількості учасників зростає складність обміну даними, синхронізації та підтримання ефективної взаємодії між вузлами. Та одним із підходів до розв'язання цієї проблеми є кластеризація, яка дозволяє організувати вузли у групи та локалізувати частину мережевих взаємодій.

У попередніх роботах авторів кластеризацію у цьому контексті було досліджено та запропоновано метод динамічної кластеризації вузлів блокчейн-мережі з консенсусом Proof-of-Work [1], [2]. Розроблена модель передбачала динамічний розподіл вузлів за ресурсними та мережевими характеристиками. За результатами моделювання було отримано зменшення середнього часу оброблення транзакцій на 1,67 с, затримки – на 1,667 с та модельного енергоспоживання – на 5122 умовні одиниці порівняно з базовим сценарієм.

Проте у попередньому дослідженні було відзначено, що збільшення кількості кластерів може супроводжуватися додатковими безпековими ризиками, базовий алгоритм кластеризації не враховував характеристики безпеки вузлів під час формування кластерів, тому подальший розвиток даного підходу потребує врахування не лише продуктивності, а й характеристик безпеки вузлів для вирішення виклику безпеки.

Отже, у початковій роботі кластеризація покращувала ефективність мережі, але не враховувала стан безпеки вузлів для формування кластерів. Тобто два вузли з однаковими power/connectivity/topology для алгоритму були практично рівнозначними, навіть якщо один відповідав актуальній криптографічній політиці, а інший, наприклад, використовував застарілу конфігурацію. Кластерна структура, зазначена у роботі, визначає склад локальних груп та функціональні взаємозв'язки між їх учасниками, тому характеристики вузлів, пов'язані з безпекою, можуть бути доцільними додатковими ознаками під час формування кластерів. Тому у запропонованому методі ми додаємо до ресурсних ознак ще одну ознаку – відповідність криптографічної конфігурації вузла політиці мережі.

У даній роботі як характеристику запропоновано використовувати криптографічний стан вузла (Cryptographic State) – модельний стан відповідності його поточної криптографічної конфігурації заданій політиці мережі CryptoPolicy. На відміну від використання криптографії безпосередньо для шифрування, автентифікації або захисту передачі даних, криптографічний стан у запропонованому підході виступає вхідною ознакою алгоритму формування та реконфігурації кластерів.

Актуальність дослідження також пов'язана з розвитком концепції crypto-agility. NIST визначає криптографічну гнучкість як сукупність можливостей, необхідних для заміни та адаптації криптографічних алгоритмів у протоколах, програмному та апаратному забезпеченні й інфраструктурі зі збереженням безпеки та безперервності функціонування, актуальність якої лише зростає [3]. У реальній системі під час криптографічного переходу різні компоненти можуть певний час перебувати у різних станах відповідності актуальній політиці, що обґрунтовує доцільність моделювання такого стану для вузлів розподіленої мережі.

Доречність урахування криптографічного стану пов'язана не з частотою зміни криптографічної політики, а зі складністю перехідних процесів у масштабних розподілених системах. Під час оновлення протоколів, криптографічних механізмів або вимог безпеки вузли можуть протягом певного періоду підтримувати різні версії та криптографічні можливості. Концепція crypto-agility передбачає необхідність керованої адаптації систем до таких змін без порушення їх функціонування. Тому у цих умовах стан відповідності вузла актуальній політиці може розглядатися як додаткова динамічна характеристика під час організації кластерної структури.

Метою роботи є розроблення та експериментальне дослідження методу безпеково-орієнтованої динамічної кластеризації вузлів розподіленої мережі, у якому під час формування та реконфігурації кластерів поряд із ресурсними характеристиками враховується поточний криптографічний стан вузлів. Для досягнення мети необхідно сформувати модель криптографічного стану вузла Cryptographic State, розробити нормалізований критерій безпеково-орієнтованої кластеризації, реалізувати механізм динамічного моніторингу та реконфігурації кластерів і провести порівняльне експериментальне дослідження запропонованого та базового методів.

Аналіз останніх досліджень. Проблема врахування характеристик безпеки під час кластеризації розглядається в бездротових сенсорних, транспортних та IoT-мережах. Значна частина таких досліджень ґрунтується на trust-based clustering, тобто використанні оцінок довіри до вузлів під час формування кластерної структури або вибору головного вузла.

Так, Oubabas та співавт. запропонували захищений алгоритм кластеризації VANET, у якому вибір головного вузла здійснюється з урахуванням як характеристик мобільності, так і показників довіри до комунікації та переданих даних [4]. У такій роботі безпекова характеристика безпосередньо впливає на кластеризацію, однак не пов'язана зі станом відповідності криптографічної конфігурації вузла певній політиці.

Для інтелектуальних транспортних систем на основі бездротових сенсорних мереж Gaber та співавт. також розглянули trust-based secure clustering як засіб зменшення комунікаційних витрат та підвищення надійності взаємодії [5]. У великомасштабних бездротових сенсорних мережах Khan та співавт. запропонували багаторівневий механізм оцінювання довіри, що

використовує кластерну структуру для виявлення несправних та зловмисних вузлів та зменшення ресурсних витрат [6]. Отже, напрям *trust/reputation* є добре представленою категорією безпекових характеристик вузла в існуючих кластерних моделях.

Поєднання кластеризації з блокчейн-механізмами також є актуальним напрямом та досліджується у сьогоденні. Ayed, Hbaieb та Chaari запропонували *blockchain-* і *trust-based* підхід для *Internet of Vehicles*, у якому формування кластерів та їх підтримання здійснюються з урахуванням рівня довіри, безпечної відстані та енергетичних характеристик вузлів [7]. У роботі оцінювалися, зокрема, *detection performance*, *communication overhead* та *runtime*, що демонструє можливість одночасного врахування безпекових і експлуатаційних характеристик кластерної мережі.

Інший напрям полягає у використанні криптографічних або блокчейн-механізмів після формування кластерів для захисту передачі даних. Наприклад, Nguyen та співавт. запропонували енергоефективний протокол кластеризації для *pervasive wireless sensor networks*, у якому кластеризація ґрунтується на енергії, щільності вузлів та відстанях, після чого блокчейн використовується для захищеної передачі даних між учасниками сформованих кластерів [8]. У такому випадку криптографічний механізм забезпечує захист взаємодії, але не виступає характеристикою, за якою визначається склад кластера.

Паралельно сучасні рекомендації NIST щодо *crypto-agility* розглядають необхідність керування переходом між криптографічними алгоритмами та конфігураціями зі збереженням поточних операцій системи [3]. Це формує передумови для розгляду криптографічної конфігурації як динамічного стану, який може змінюватися в процесі її функціонування, а не як незмінної властивості системи.

Порівняння зазначених напрямів показує, що наявні дослідження охоплюють, з одного боку, кластеризацію на основі довіри та репутації [4], [5], [6], [7], а з іншого – застосування блокчейн- і криптографічних механізмів для захисту передачі та зберігання даних у кластерних системах [7], [8]. Водночас у проаналізованій вибірці робіт не виявлено підходу, де поточна відповідність криптографічної конфігурації вузла заданій криптографічній політиці формалізується як окремий криптографічний стан і безпосередньо включається до критерію динамічного формування та подальшої реконфігурації кластерів.

Саме ця відмінність визначає напрям дослідження. Запропонований підхід не замінює *trust-management* та не розробляє нового криптографічного алгоритму. Натомість вводиться додатковий рівень інформації про стан вузла: криптографічна конфігурація – перевірка відповідності *CryptoPolicy* – *Cryptographic State* – критерій кластеризації – динамічна реконфігурація.

Дослідницька гіпотеза полягає в тому, що включення такої характеристики до критерію кластеризації дозволить зменшити локальну концентрацію вузлів, які не відповідають встановленій криптографічній політиці, без необхідності їх повного вилучення з мережі. Перевірка цієї гіпотези виконується шляхом програмного моделювання, описаного в наступному розділі. Актуальність урахування криптографічного стану додатково зростає в умовах переходу до постквантових криптографічних алгоритмів, що потребує планування міграції криптографічних механізмів та врахування проблем їх упровадження [9].

Адаптація кластерної структури до змін характеристик вузлів також розглядається в дослідженні Ahmad та співавт., у якому запропоновано протокол вибору алгоритму кластеризації транспортної мережі залежно від поточної моделі мобільності. Такий підхід спрямований на зменшення накладних витрат на підтримання кластерів, однак, на відміну від запропонованого методу, не враховує відповідність криптографічної конфігурації вузлів мережі установленій політиці та взагалі не вирішує питання безпеки [10].

Модель безпеково-орієнтованої динамічної кластеризації. Запропонований метод розширює базову модель динамічної кластеризації введенням криптографічного стану вузла (*Cryptographic State*) як додаткової характеристики, що використовується під час формування та реконфігурації кластерів. У поточній програмній реалізації параметри криптографічної конфігурації вузлів моделюються. У практичній реалізації *Cryptographic State* може

визначатися на основі доступних і перевірюваних характеристик вузла, зокрема підтримуваної версії протоколу, можливостей захищеного транспортного рівня, версії політики безпеки, стану ключового матеріалу та інших спостережуваних або тестованих параметрів [11].

Отже, на відміну від базового підходу, в якому розподіл вузлів визначається їх мережевими та ресурсними параметрами, запропонований метод додатково враховує відповідність криптографічної конфігурації вузла встановленій політиці мережі.

Загальну структуру запропонованого методу наведено на Рис. 1. Модель охоплює три основні функціональні рівні: формування вхідних ознак, прийняття рішення щодо складу кластерів та адаптацію кластерної структури у часі. На першому рівні використовуються параметри вузла та вимоги CryptoPolicy. На другому рівні на основі цих даних виконується оцінювання Cryptographic State, після чого безпеково-орієнтований критерій використовується для формування кластерів. На третьому рівні здійснюється моніторинг сформованої структури та перевірка умови перевищення порогового значення максимальної концентрації NON_COMPLIANT вузлів. У разі виконання цієї умови ініціюється реконфігурація кластерів, інакше поточна структура зберігається до наступного циклу моніторингу.

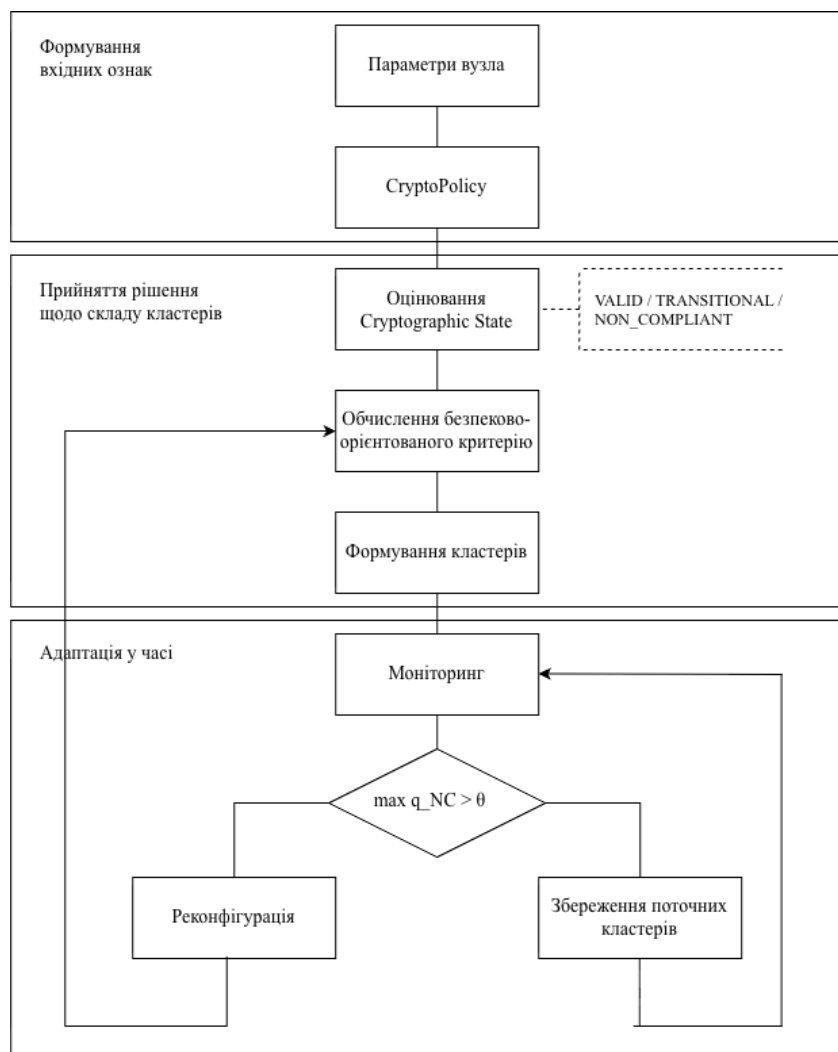


Рис. 1. Структурна схема моделі безпеково-орієнтованої динамічної кластеризації вузлів розподіленої мережі

Джерело: розроблено авторами

Модель вузла та криптографічного стану. Нехай розподілена мережа містить множину вузлів

$$N = \{n_1, n_2, \dots, n_m\} \quad (1)$$

Кожний вузол характеризується сукупністю мережових, ресурсних та криптографічних параметрів:

$$n_i = \{P_i, C_i, T_i, A_i, L_i, V_i, K_i\}, \quad (2)$$

де P_i – обчислювальна характеристика вузла; C_i – показник зв'язності; T_i – топологічні характеристики; A_i – параметр використовуваної криптографічної конфігурації; L_i – модельний рівень відповідності криптографічним вимогам; V_i – версія криптографічної політики; K_i – ознака чинності або допустимості ключового матеріалу.

Для визначення відповідності криптографічної конфігурації у модель вводиться політика CryptoPolicy, яка задає набір вимог до допустимих криптографічних і протокольних параметрів вузла. У модельному експерименті такими параметрами є тип криптографічної конфігурації, внутрішній рівень відповідності, версія політики та ознака чинності ключового матеріалу.

На основі порівняння параметрів вузла з CryptoPolicy кожному вузлу призначається один із трьох станів:

- VALID – поточна конфігурація вузла відповідає встановленій CryptoPolicy;
- TRANSITIONAL – основні параметри конфігурації відповідають вимогам, але вузол ще не перейшов на актуальну версію політики;
- NON_COMPLIANT – одна або декілька контрольованих характеристик вузла не відповідають поточній CryptoPolicy.

Таким чином, Cryptographic State є результатом перевірки конкретних параметрів вузла відносно заданої політики.

Критерій безпеково-орієнтованого формування кластерів. Для формування критерію пояснимо складові частини. Для мережі з N вузлів кількість кластерів визначається як:

$$K = \lfloor \sqrt{N} \rfloor, \quad (3)$$

де K – кількість кластерів; $\sqrt{N}$ – загальна кількість вузлів мережі (що обґрунтовано у попередніх дослідженнях).

Перед розподілом вузли впорядковуються за пріоритетом криптографічного стану у послідовності VALID – TRANSITIONAL – NON_COMPLIANT. У межах кожної групи додаткове впорядкування здійснюється за зростанням значень обчислювальної характеристики, зв'язності та топологічного показника.

Частки вузлів із криптографічними станами NON_COMPLIANT та TRANSITIONAL після умовного додавання вузла до кластера визначаються як:

$$Q_{NC,j} = \frac{N_{NC,j}}{N_j}, \quad Q_{TR,j} = \frac{N_{TR,j}}{N_j}, \quad (4)$$

де $N_{NC,j}$ та $N_{TR,j}$ – кількість вузлів відповідних станів у прогнозованому складі j -го кластера, а N_j – його прогнозована кількість вузлів.

Базова кластеризація враховує ресурсне навантаження вузлів. У запропонованому методі цей критерій доповнюється характеристикою криптографічного складу кожного кластера.

Для забезпечення порівнянності складових використовується нормалізований критерій вибору кластера:

$$J_j = w_R R_j + w_{NC} Q_{NC,j} + w_{TR} Q_{TR,j}, \quad (5)$$

де R_j – нормалізована ресурсна складова j -го кластера; $Q_{NC,j}$ – частка вузлів NON_COMPLIANT; $Q_{TR,j}$ – частка вузлів TRANSITIONAL; w_R, w_{NC}, w_{TR} – вагові коефіцієнти відповідних складових.

Новий вузол призначається до кластера, для якого значення критерію J_j є мінімальним.

Використання відносних часток замість абсолютної кількості вузлів дає змогу уникнути прямої залежності безпекової складової критерію від поточного розміру кластера. При цьому збільшення w_{NC} підвищує штраф для кластерів із більшою часткою NON_COMPLIANT вузлів, а w_{TR} визначає вплив перехідних криптографічних конфігурацій.

За результатами проведеного аналізу чутливості для подальших експериментів використано $w_R = 1$, $w_{NC} = 2$ та $w_{TR} = 1$. Ці значення розглядаються як параметри експериментальної моделі, а не як універсально оптимальні коефіцієнти.

Запропонований механізм впливає на розподіл вузлів NON_COMPLIANT між кластерами, не видаляючи їх з мережі, що важливо, бо метою запропонованого методу наразі є обмеження локальної концентрації криптографічно невідповідних вузлів.

При цьому метод не гарантує жорсткого дотримання заданої максимальної частки NON_COMPLIANT у кожному кластері, оскільки результат залежить від глобального складу мережі та доступного розподілу вузлів.

Динамічна реконфігурація кластерів. Оскільки криптографічний стан вузла може змінюватися під час функціонування мережі, модель передбачає періодичне повторне оцінювання відповідності вузлів політиці CryptoPolicy.

У формулі (4) вище зазначено, що для кожного кластера визначається частка NON_COMPLIANT вузлів $Q_{NC,j}$. Отже, реконфігурація ініціюється, якщо хоча б для одного кластера виконується умова

$$Q_{NC,j} > \theta, \quad (6)$$

де θ – експериментально задане порогове значення, перевищення якого використовується як умова ініціювання реконфігурації.

У проведених експериментах використовувалося значення $\theta = 0,20$. Воно є параметром модельного сценарію і не розглядається як універсальна межа криптографічної безпеки.

Після виявлення перевищення порогу виконується повторне формування кластерів за критерієм (5).

Таким чином, загальна послідовність роботи методу має наступний вигляд:

- 1) формування мережі;
- 2) оцінювання Cryptographic State;
- 3) Security-Aware кластеризація;
- 4) моніторинг станів;
- 5) перевірка порогу;
- 5) реконфігурація за необхідності.

Для оцінювання роботи методу використовуються максимальна концентрація NON_COMPLIANT вузлів, нерівномірність розмірів кластерів, кількість реконфігурацій та кількість вузлів, переміщених між кластерами.

Експериментальне дослідження запропонованого методу. Експериментальне дослідження проведено з метою оцінювання здатності запропонованого методу безпеково-орієнтованої динамічної кластеризації зменшувати локальну концентрацію вузлів, криптографічна конфігурація яких не відповідає встановленій політиці CryptoPolicy. Як базовий варіант (Baseline) використовувався базовий метод кластеризації, що враховує ресурсні та мережеві характеристики вузлів без використання їхнього криптографічного стану. У оновленому варіанті (Security-Aware) до критерію формування кластерів додатково включено стани VALID, TRANSITIONAL та NON_COMPLIANT.

У поточній програмній реалізації параметри криптографічної конфігурації вузлів формуються в межах імітаційної моделі. Стан NON_COMPLIANT означає невідповідність контрольованих параметрів вузла заданій CryptoPolicy (відповідно до принципів crypto-agility) і не однозначно є ознакою того, що вузол є зловмисним або скомпрометованим.

Основною метрикою безпекової збалансованості обрано максимальну частку вузлів зі станом NON_COMPLIANT серед усіх сформованих кластерів. Такий показник дає змогу оцінити ступінь локальної концентрації невідповідних вузлів в окремому кластері.

Отже, у створеній моделі на першому етапі проведено порівняння середнього значення максимальної частки NON_COMPLIANT вузлів серед сформованих кластерів для Baseline та Security-Aware для чотирьох сценаріїв із різним співвідношенням криптографічних станів вузлів. Результати 50 запусків наведено в Таблиці 1. Співвідношення VALID/TRANSITIONAL/NON_COMPLIANT, використані в експериментах, є параметрами модельних сценаріїв і не розглядаються як оцінка фактичного розподілу таких станів у конкретній PoW-мережі.

Таблиця 1. Результати порівняння методів кластеризації

Сценарій VALID/TRANSITIONAL/ NON_COMPLIANT	Середня максимальна концентрація NON_COMPLIANT, Baseline	Середня максимальна концентрація NON_COMPLIANT, Security-Aware	Відносне зниження, %
90/0/10	0,2684	0,1122	58,19
80/10/10	0,2703	0,1120	58,57
70/20/10	0,2615	0,1134	56,63
60/20/20	0,4177	0,2348	43,78

Джерело: розроблено авторами

Отримані після моделювання та проведення експериментів результати показали, що в усіх досліджених сценаріях середнє значення максимальної концентрації NON_COMPLIANT вузлів для запропонованого методу було нижчим, ніж для базової кластеризації. Відносне зниження показника становило від 43,78 % до 58,57 %. Найбільше зниження отримано для сценарію 80/10/10, а найменше – для сценарію 60/20/20, у якому загальна частка NON_COMPLIANT вузлів була вдвічі більшою. Отже, у межах проведеного моделювання врахування Cryptographic State під час формування кластерів забезпечило більш рівномірний розподіл вузлів, конфігурація яких не відповідає поточній CryptoPolicy.

Крім зменшення середнього значення показника, для мережі Security-Aware спостерігалася нижча варіативність максимальної концентрації невідповідних вузлів між незалежними реалізаціями: стандартне відхилення становило 0,0038-0,0154 проти 0,0583-0,0714 для Baseline.

Для перевірки впливу параметрів критерію кластеризації проведено аналіз чутливості вагових коефіцієнтів w_{NC} та w_{TR} . Дослідження 25 комбінацій параметрів показало залежність результатів від їх співвідношення. Для подальших експериментів використано $w_R = 1$, $w_{NC} = 2$ та $w_{TR} = 1$, що в дослідженому просторі параметрів забезпечувало поєднання низької максимальної концентрації NON_COMPLIANT вузлів та прийнятної збалансованості розмірів кластерів. Зазначені значення є параметрами експериментальної моделі та не розглядаються як універсально оптимальні для довільних розподілених мереж.

Працездатність механізму динамічної реконфігурації перевірено протягом 100 часових кроків, під час яких моделювалися зміни криптографічних конфігурацій вузлів. Частка вузлів, конфігурація яких змінювалася на кожному кроці, становила 0,10, а ймовірність погіршення стану – 0,75. Як умову ініціювання реконфігурації використовувалося експериментально задане порогове значення максимальної концентрації NON_COMPLIANT $\theta = 0,20$. Зазначене значення є параметром модельного сценарію та не є нормативною межею безпеки або гарантованим обмеженням після реконфігурації. Для даної моделі за 100 часових кроків було зафіксовано 526 фактичних змін криптографічного стану вузлів. Перевищення порогового значення спостерігалось на всіх 100 кроках, що спричинило 100 реконфігурацій кластерної структури. Середня максимальна концентрація NON_COMPLIANT-вузлів у кластері до реконфігурації становила 0,7042, а після реконфігурації – 0,6299. Абсолютне зменшення агрегованих середніх значень становило 0,0743, що відповідає приблизно 10,55 % відносного зниження.

Водночас було зафіксовано 8241 переміщення вузлів між кластерами – в середньому 82,41 переміщення на одну реконфігурацію. Отримані результати підтвердили працездатність механізму реагування на зміну Cryptographic State, але також показали високу

вартість глобального переформування кластерів у стресовому сценарії. Крім того, реконфігурація не гарантувала зниження максимальної концентрації нижче $\theta = 0,20$, оскільки за накопичення значної кількості NON_COMPLIANT вузлів такий розподіл може бути структурно недосяжним. Це обґрунтовує подальший розвиток локальної реконфігурації, гістерезису або обмеження частоти глобального переформування.

Час виконання програмної реалізації вимірювався додатково, однак через малу абсолютну тривалість операцій та чутливість таких вимірювань до накладних витрат середовища виконання цей показник не використовувався як основний критерій ефективності методу.

Для перевірки масштабованості методу проведено серію експериментів для мереж із 50, 100, 250, 500 та 1000 вузлів. Для кожного розміру виконано 30 незалежних реалізацій. Мережі Baseline та Security-Aware порівнювалися на однакових реалізаціях мережі, що забезпечило парний характер експериментальних спостережень. Отримані після запуску програмного експерименту результати наведено на Рис. 2 та в Таблиці 2.

Для всіх досліджених розмірів мережі запропонований метод забезпечив менше середнє значення максимальної концентрації NON_COMPLIANT вузлів порівняно з Baseline. Відносне зниження становило 38,70-57,42 %, та перевага методу спостерігалася для всіх досліджених розмірів мережі від 50 до 1000 вузлів.

Для статистичної перевірки відмінностей застосовано парний критерій знакових рангів Вілкоксона p . Для всіх досліджених розмірів мережі отримано $p < 0,001$, що свідчить про статистично значущу різницю між результатами у базовій мережі Baseline та оновленій Security-Aware у сформованих експериментальних вибірках.

Сукупність отриманих результатів підтверджує, що в межах розробленої імітаційної моделі включення криптографічного стану вузлів до критерію кластеризації дає змогу зменшити їх локальну концентрацію у випадку невідповідності встановленій криптографічній політиці. Ефект спостерігався для різних початкових співвідношень криптографічних станів та зберігався для модельних мереж розміром від 50 до 1000 вузлів. Варто зауважити, що отримані результати характеризують саме криптографічну відповідність вузлів, а не безпосередню стійкість до конкретних кібератак. Стан NON_COMPLIANT у запропонованій моделі означає невідповідність параметрів вузла політиці CryptoPolicy і не є тотожним поняттю зловмисного або скомпрометованого вузла.

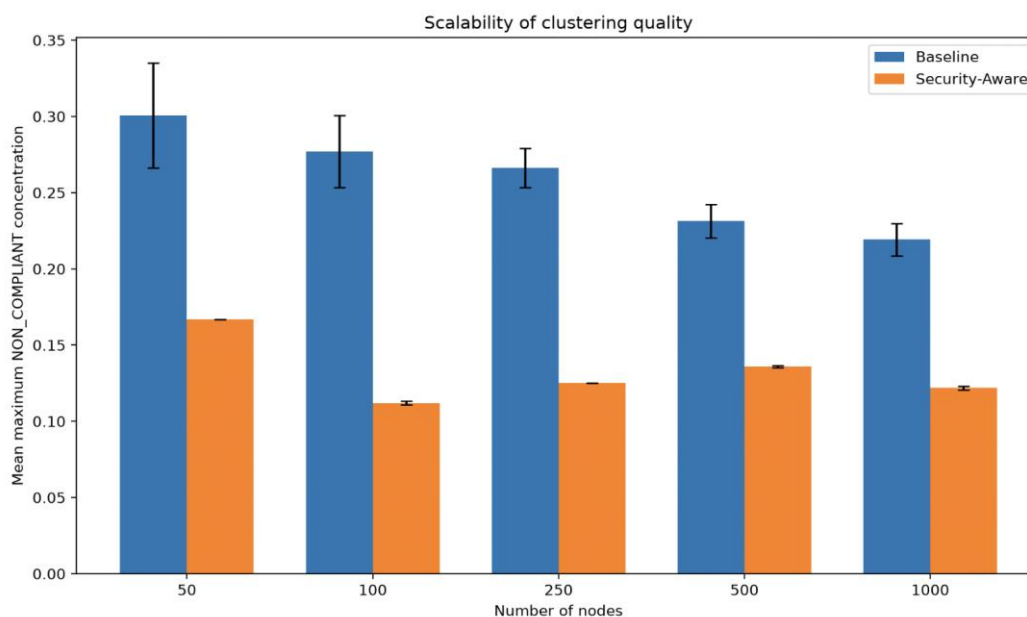


Рис. 2. Залежність середньої максимальної концентрації NON_COMPLIANT вузлів від кількості вузлів мережі для методів Baseline та Security-Aware

Джерело: розроблено авторами

Таблиця 2. Результати дослідження масштабованості методу

Кількість вузлів у мережі	Середня максимальна концентрація NON_COMPLIANT, Baseline	Середня максимальна концентрація NON_COMPLIANT, Security-Aware	Відносне зниження, %	p-value
50	0,3007	0,1667	38,70	$2,15 \cdot 10^{-6}$
100	0,2770	0,1120	57,42	$7,96 \cdot 10^{-7}$
250	0,2662	0,1250	52,12	$7,96 \cdot 10^{-7}$
500	0,2313	0,1358	40,32	$8,23 \cdot 10^{-7}$
1000	0,2192	0,1219	43,44	$8,64 \cdot 10^{-7}$

Джерело: розроблено авторами

Висновки. Отже, у даній роботі запропоновано метод безпеково-орієнтованої динамічної кластеризації вузлів розподіленої мережі, особливістю якого є врахування криптографічного стану вузла поряд із його мережевими та ресурсними характеристиками, що є актуальним в контексті розвитку концепції crypto-agility. Для цього введено модель Cryptographic State, відповідно до якої вузли класифікуються за станом як VALID, TRANSITIONAL або NON_COMPLIANT залежно від відповідності їх криптографічної конфігурації встановленій політиці CryptoPolicy.

Для формування кластерів розроблено нормалізований критерій, що поєднує ресурсну складову з частками NON_COMPLIANT та TRANSITIONAL вузлів у кластері. Запропонований підхід спрямований на обмеження локальної концентрації невідповідних вузлів в окремих кластерах. Динамічність методу забезпечується періодичним оцінюванням криптографічного стану та реконфігурацією кластерної структури у разі перевищення заданого порогу концентрації NON_COMPLIANT вузлів.

У чотирьох досліджених сценаріях із різним співвідношенням криптографічних станів запропонований метод забезпечив зниження середньої максимальної концентрації NON_COMPLIANT вузлів на 43,78-58,57 % порівняно з базовою кластеризацією. Аналіз чутливості підтвердив залежність результатів від вагових коефіцієнтів критерію та дав змогу визначити їх робочу конфігурацію для подальших експериментів. При цьому для оновленої мережі Security-Aware також спостерігалася нижча варіативність результатів між незалежними реалізаціями.

Дослідження масштабованості для мереж із 50, 100, 250, 500 та 1000 вузлів показало перевагу запропонованого методу для всіх досліджених розмірів мережі. Середнє відносне зниження максимальної концентрації NON_COMPLIANT становило 38,70-57,42 %, а парне статистичне порівняння за критерієм Вілкоксона для всіх досліджених розмірів мережі дало $p < 0,001$, що підтверджує статистично значущу відмінність отриманих результатів у межах сформованих експериментальних вибірок.

Динамічне моделювання підтвердило можливість реагування на зміну криптографічних станів вузлів: у стресовому сценарії середня максимальна концентрація зменшилася з 0,7042 до 0,6299 після реконфігурації. Водночас 100 реконфігурацій спричинили 8241 переміщення вузлів, що виявило високу вартість глобального переформування кластерної структури за інтенсивної зміни станів, що виявило обмеження поточної реалізації та визначило напрям подальшого вдосконалення методу.

Таким чином, отримані результати моделювання підтверджують доцільність використання криптографічного стану як стану відповідності криптографічній політиці у якості додаткової ознаки динамічної кластеризації та демонструють можливість зменшення локальної концентрації вузлів, що не відповідають встановленій криптографічній політиці. Стан NON_COMPLIANT не є тотожним поняттю зловмисного або скомпрометованого вузла, а отримані результати не є безпосереднім доказом стійкості до конкретних атак, зокрема атаки 51 %, проте потенційно впливають на загальний рівень безпеки у системі. Подальші дослідження доцільно спрямувати на локальну реконфігурацію кластерів, зменшення

кількості переміщень вузлів та дослідження взаємозв'язку Cryptographic State, розподілу обчислювальної потужності та структури й механізмів консенсусу.

Конфлікт інтересів: Автори декларують, що не мають конфлікту інтересів, зокрема фінансового, особистого, авторського чи будь-якого іншого характеру, який міг би вплинути на дослідження, а також на результати, опубліковані в цій статті

Фінансування: Дослідження проводилося без фінансової підтримки

Доступність даних: Код моделювання, використаний для одержання наведених результатів, подано у відкритому репозиторії https://github.com/disvik/algorithm_security_aware

Використання засобів штучного інтелекту: Під час підготовки рукопису використовувався інструмент інструмент ChatGPT (OpenAI, модель GPT-5.6 Sol) штучного інтелекту (ШІ) для граматичної та стилістичної перевірки тексту. Усі фрагменти, опрацьовані за його допомогою, були перевірені й відредаговані автором. ШІ не використовувався для генерації тексту, формул і таблиць, формування наукових положень, отримання результатів або формулювання висновків. Наукові положення, результати та висновки є власним інтелектуальним внеском авторів

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Soloviova, D., Antoshchuk, S. & Boltenkov, V. "Development and Research of the Methodology for Improving the Proof-of-Work Blockchain Technology by Implementing Dynamic Clustering of Network Nodes". *IET Blockchain*. 2025; 5 (1): e70006. DOI: <https://doi.org/10.1049/blc2.70006>.
2. Soloviova, D., Antoshchuk, S. & Boltenkov, V. "Research into the possibilities of improving Proof-of-Work blockchain technology". *Herald of Advanced Information Technology*. 2024; 7 (2): 131–146. DOI: <https://doi.org/10.15276/hait.07.2024.9>.
3. Barker, E., Chen, L., Cooper, D., Moody, D., Regenscheid, A., Souppaya, M., Newhouse, W., Housley, R., Turner, S., Barker, W. & Kent, K. "Considerations for Achieving Crypto Agility: Strategies and Practices". *NIST Cybersecurity White Paper CSWP 39upd1*. Gaithersburg, MD, USA: National Institute of Standards and Technology. 2026. DOI: <https://doi.org/10.6028/NIST.CSWP.39-upd1>.
4. Oubabas, S., Aoudjit, R., Rodrigues, J. J. P. C. & Talbi, S. "Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme". *Vehicular Communications*. 2018; 13: 128–138. DOI: <https://doi.org/10.1016/j.vehcom.2018.08.001>.
5. Gaber, T., Abdelwahab, S., Elhoseny, M. & Hassanien, A. E. "Trust-based secure clustering in WSN-based intelligent transportation systems". *Computer Networks*. 2018; 146: 151–158, <https://www.scopus.com/record/display.uri?eid=2-s2.0-85054025971>. DOI: <https://doi.org/10.1016/j.comnet.2018.09.015>.
6. Khan, T., Singh, K., Son, L. H., Abdel-Basset, M., Long, H. V., Singh, S. P. & Manjul, M. "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks". *IEEE Access*. 2019; 7: 58221–58240. DOI: <https://doi.org/10.1109/ACCESS.2019.2914769>.
7. Ayed, S., Hbaieb, A. & Chaari, L. "Blockchain and trust-based clustering scheme for the IoT". *Ad Hoc Networks*. 2023; 142: 103093. DOI: <https://doi.org/10.1016/j.adhoc.2023.103093>.
8. Nguyen, G. N., Le Viet, N. H., Devaraj, A. F. S., Gobi, R. & Shankar, K. "Blockchain enabled energy efficient red deer algorithm based clustering protocol for pervasive wireless sensor networks". *Sustainable Computing: Informatics and Systems*. 2020; 28: 100464. DOI: <https://doi.org/10.1016/j.suscom.2020.100464>.
9. Barker, W., Polk, W. & Souppaya, M. "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms". *NIST Cybersecurity White Paper CSWP 15*. Gaithersburg, MD, USA: National Institute of Standards and Technology. 2021. DOI: <https://doi.org/10.6028/NIST.CSWP.15>.
10. Ahmad, M., Hameed, A., Ullah, F., Wahid, I., Khan, A., Uddin, M. I., Ahmad, S. & El-Sherbeeney, A. M. "Adaptation of Vehicular Ad hoc Network Clustering Protocol for Smart Transportation". *Computers, Materials & Continua*. 2021; 67 (2): 1353–1368, <https://www.scopus.com/record/display.uri?eid=2-s2.0-85102518452>. DOI: <https://doi.org/10.32604/cmc.2021.014237>.

11. Birkholz, H., Thaler, D., Richardson, M., Smith, N. & Pan, W. “Remote ATtestation procedureS (RATS) Architecture”. RFC 9334. Internet Engineering Task Force. 2023. – Available from: <https://www.rfc-editor.org/rfc/rfc9334.html>. – [Accessed: 17.04.2026]. DOI: <https://doi.org/10.17487/RFC9334>.

Отримано 04.09.2026

Отримано після перегляду 09.10.2026

Прийнято 12.10.2026

DOI: <https://doi.org/10.15276/ict.03.2026.43>

UDC 004.451:502/504

Security-aware dynamic clustering of distributed network nodes considering their cryptographic state

Diana V. Soloviova¹⁾

ORCID: <https://orcid.org/0009-0007-5253-8848>; soloviova.d.v@op.edu.ua. Scopus Author ID: 59185442400

Viktor O. Boltenkov¹⁾

ORCID: <https://orcid.org/0000-0003-2777-3137>; vaboltenkov@gmail.com. Scopus Author ID: 57203623617

¹⁾ Odesa Polytechnic National University, 1, Shevchenko Av. Odesa, 65044, Ukraine

ABSTRACT

This paper addresses the problem of security-aware dynamic clustering of nodes in distributed networks, taking into account their cryptographic state. The need to consider not only the resource and network characteristics of nodes but also the compliance of their cryptographic configurations with an established policy is substantiated, particularly during the updating of cryptographic mechanisms. The aim of this study is to develop and experimentally evaluate a clustering method designed to reduce the local concentration of nodes that do not comply with current cryptographic requirements. A cryptographic state model is proposed that classifies nodes into three categories: those that comply with the established policy, those in a transitional state, and those that do not meet its requirements. A normalized cluster formation criterion is developed that combines resource characteristics with the cryptographic states of nodes. To adapt the cluster structure, monitoring and reconfiguration are performed when a specified threshold for the concentration of non-compliant nodes is exceeded. Simulation experiments were conducted to compare the proposed method with baseline clustering under different distributions of cryptographic states. Across four experimental scenarios, the proposed method reduced the mean maximum concentration of cryptographically non-compliant nodes by between forty-three point seventy-eight and fifty-eight point fifty-seven percent. A scalability study involving networks ranging from fifty to one thousand nodes demonstrated a reduction in this metric of between thirty-eight point seventy and fifty-seven point forty-two percent. Statistical testing confirmed that the observed differences were significant. Dynamic simulations demonstrated the ability to adapt the cluster structure to changes in cryptographic states while revealing substantial overhead associated with global reconfiguration. Future research will focus on developing local reconfiguration mechanisms and reducing the number of node relocations.

Keywords: Distributed network; dynamic clustering; cryptographic state of a node; cryptographic policy; cryptographic agility; security-aware clustering; cluster reconfiguration; simulation modelling

ІНФОРМАЦІЯ ПРО АВТОРІВ



Соловійова Діана Вячеславівна - асистент кафедри Інформаційних систем. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

Галузь досліджень: розподілені та децентралізовані системи, блокчейн-технології, криптографія

Diana V. Soloviova - Assistant, Information Systems Department. Odesa Polytechnic National University, 1, Shevchenko Av. Odesa, 65044, Ukraine

ORCID: <https://orcid.org/0009-0007-5253-8848>; soloviova.d.v@op.edu.ua. Scopus Author ID: 59185442400

Research field: distributed and decentralized systems, blockchain technologies, cryptography



Болтьонков Віктор Олександрович - кандидат технічних наук, доцент кафедри Інформаційних систем, Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

Галузь досліджень: блокчейн-технології, обробка сигналів

Viktor O. Boltenkov - PhD, Associate Professor of the Information System Department, Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine

ORCID: <https://orcid.org/0000-0003-2777-3137>; vaboltenkov@gmail.com. Scopus Author ID: 57203623617

Research field: Blockchain technologies; signal processing