КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1287
УДК 004.738.5:004.056.5:621.39

Жебка Вікторія Вікторівна
д.т.н. професор,
завідувач кафедри технологій цифрового розвитку
Державний університет інформаційно комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-4051-1190
v.zhebka@duikt.edu.ua

БЛОКЧЕЙН-ОРІЄНТОВАНА АРХІТЕКТУРА МОНІТОРИНГУ ТА АДАПТИВНОГО УПРАВЛІННЯ ФУНКЦІОНАЛЬНО СТІЙКОЮ ГЕТЕРОГЕННОЮ ТЕЛЕКОМУНІКАЦІЙНОЮ МЕРЕЖЕЮ

Анотація. У статті розглянуто проблему забезпечення функціональної стійкості гетерогенних телекомунікаційних мереж в умовах зростання складності мережевої інфраструктури, збільшення обсягів трафіку, поширення технологій хмарних і периферійних обчислень, програмно-конфігурованих мереж та Інтернету речей. Визначено, що традиційні централізовані системи моніторингу характеризуються наявністю єдиної точки відмови та не забезпечують належного рівня довіри до телеметричних даних, що може призводити до прийняття помилкових управлінських рішень в умовах кібернетичних атак, відмов обладнання або навмисної фальсифікації інформації. Обґрунтовано доцільність використання технології блокчейн для забезпечення достовірності моніторингових даних та підтримки процесів адаптивного управління мережею. Запропоновано блокчейн-орієнтовану архітектуру моніторингу та адаптивного управління функціонально стійкою гетерогенною телекомунікаційною мережею, яка поєднує засоби телеметрії, механізми розподіленої верифікації даних, модулі оцінювання функціонального стану мережі, прогнозування розвитку дестабілізуючих впливів і формування керуючих рішень. Особливістю запропонованого підходу є використання permissioned blockchain для збереження агрегованих телеметричних подій, результатів оцінювання довіри та інформації про прийняті керуючі впливи, що забезпечує незмінність записів, простежуваність рішень та підвищення рівня довіри до процесів управління. Розроблено методологію моніторингу та адаптивного управління мережею, яка реалізує замкнений цикл «моніторинг – верифікація – оцінювання – прогнозування – управління». Методологія передбачає збір і нормалізацію телеметричних даних, оцінювання їх достовірності на основі показників децентралізації, надійності консенсусу, цілісності транзакцій, аудитованості та репутації джерел даних, а також розрахунок інтегрального показника функціональної стійкості мережі. Для переходу від реактивного до проактивного управління запропоновано використовувати прогнозування ризику деградації функціонального стану та вибір оптимальних керуючих впливів з урахуванням очікуваного ефекту, вартості реалізації та залишкового ризику. Результати експериментального дослідження підтвердили ефективність запропонованого підходу порівняно з централізованими системами моніторингу та традиційними SDN/NFV-рішеннями. Встановлено підвищення інтегрального показника функціональної стійкості мережі, збільшення достовірності телеметричних даних, скорочення часу виявлення дестабілізуючих впливів і реагування на них, а також зменшення кількості помилкових управлінських рішень. Отримані результати свідчать про перспективність використання блокчейн-технологій для побудови довірених систем моніторингу та адаптивного управління телекомунікаційними мережами нового покоління.

Ключові слова: блокчейн, гетерогенна телекомунікаційна мережа, функціональна стійкість, моніторинг мережі, адаптивне управління, телеметричні дані, permissioned blockchain, кіберстійкість.

ВСТУП

Постановка проблеми. Сучасні гетерогенні телекомунікаційні мережі, які поєднують мобільні, хмарні, периферійні та програмно-конфігуровані середовища, функціонують в умовах постійного зростання обсягів трафіку, кількості підключених пристроїв та вимог до якості обслуговування. Це зумовлює необхідність забезпечення їх функціональної стійкості, оскільки відмови обладнання, перевантаження ресурсів, помилки конфігурації та кібернетичні атаки можуть призводити до деградації мережевих сервісів і порушення безперервності надання послуг.

Ефективність підтримання функціональної стійкості значною мірою залежить від достовірності телеметричних даних, на основі яких здійснюється моніторинг стану мережі та формуються керуючі впливи. Водночас більшість існуючих систем моніторингу використовує централізовані підходи до збору й оброблення інформації, що створює ризики компрометації даних, виникнення єдиної точки відмови та прийняття неефективних управлінських рішень.

Перспективним напрямом розв'язання зазначених проблем є використання технології блокчейн, яка забезпечує незмінність записів, розподілену верифікацію інформації та прозорість процесів прийняття рішень. Проте існуючі дослідження переважно зосереджені на питаннях безпеки та захисту даних, тоді як задачі забезпечення функціональної стійкості телекомунікаційних мереж на основі блокчейн-технологій залишаються недостатньо дослідженими.

У зв'язку з цим актуальним є розроблення блокчейн-орієнтованої архітектури моніторингу та адаптивного управління функціонально стійкою гетерогенною телекомунікаційною мережею, яка забезпечує підвищення достовірності моніторингових даних, своєчасне виявлення дестабілізуючих впливів та формування ефективних керуючих рішень для підтримання працездатності мережевої інфраструктури.

Аналіз останніх досліджень і публікацій. Аналіз сучасних досліджень свідчить, що підвищення складності гетерогенних телекомунікаційних мереж сприяло активному розвитку засобів моніторингу та управління на основі програмно-конфігурованих мереж і віртуалізації мережевих функцій. Значна увага приділяється використанню телеметрії для отримання детальної інформації про стан мережі в реальному часі, що дозволяє підвищити ефективність керування ресурсами та забезпечити необхідний рівень якості обслуговування. Зокрема, у роботі Isolani та співавторів запропоновано SDN-орієнтований підхід до оркестрації мережевих зрізів із використанням In-Band Network Telemetry (INT), який забезпечує збір детальної статистики та її використання для динамічного керування мережевими ресурсами [1]. Разом із тим зазначені підходи орієнтовані переважно на підвищення ефективності управління мережею та не враховують питання довіри до отриманих телеметричних даних.

Подальший розвиток засобів мережевого моніторингу пов'язаний із концепцією захищеної телеметрії. У роботах Zhao та співавторів запропоновано архітектуру SINT, у межах якої блокчейн використовується для захисту даних In-Band Network Telemetry від несанкціонованої модифікації та фальсифікації [2, 3]. Запропонований підхід дозволяє підвищити цілісність телеметричної інформації шляхом збереження мережевих знімків у розподіленому реєстрі. Водночас дослідження зосереджене переважно на захисті даних моніторингу та не розглядає питання оцінювання функціональної стійкості мережі та формування адаптивних керуючих впливів.

Важливий напрям досліджень пов'язаний із використанням блокчейн-технологій у мережах 5G та Beyond 5G. У роботах Onora та співавторів, а також інших дослідників показано можливості використання блокчейну для підвищення безпеки мережевої інфраструктури, керування мережевими зрізами, взаємодії між операторами та управління ресурсами розподілених мереж [4, 5]. Аналогічні результати наведено у роботах Das та співавторів, де запропоновано blockchain-enabled SDN-архітектуру для підвищення безпеки та ефективності функціонування мереж 5G [6]. Разом із тим більшість наявних рішень орієнтована на забезпечення безпеки, автентифікації та контролю доступу, тоді як задачі підтримання функціональної стійкості мережі розглядаються лише опосередковано.

Вагомий внесок у розвиток методів забезпечення стійкості телекомунікаційних мереж зробили українські науковці. Зокрема, у роботах І. А. Плюща, І. В. Стрєлковської, О. В. Лемешка та їхніх наукових шкіл досліджуються питання управління ресурсами мереж нового покоління, забезпечення якості обслуговування, маршрутизації трафіку та функціонування програмно-конфігурованих мережевих середовищ [7–9]. Значна увага приділяється розробленню моделей управління телекомунікаційними системами в умовах динамічної зміни навантаження та обмеженості мережевих ресурсів.

У роботах, присвячених проблемам кіберстійкості та функціонування критичної інформаційної інфраструктури, розглядаються питання виявлення аномалій, оцінювання ризиків, забезпечення живучості мереж та захисту інформаційно-комунікаційних систем від зовнішніх впливів [10, 11]. Запропоновані підходи дозволяють підвищити надійність функціонування мережевих середовищ, проте здебільшого ґрунтуються на централізованих механізмах збору та оброблення моніторингової інформації.

Водночас аналіз вітчизняних і зарубіжних досліджень показує, що питання інтеграції технології блокчейн у контур моніторингу та адаптивного управління функціонально стійкими гетерогенними телекомунікаційними мережами залишаються недостатньо дослідженими. Особливої уваги потребує розроблення архітектурних рішень, які поєднують механізми довіреного моніторингу, оцінювання функціональної стійкості, прогнозування розвитку дестабілізуючих впливів та автоматизованого формування керуючих дій на основі верифікованих телеметричних даних.

Мета і завдання дослідження. Метою роботи є розроблення блокчейн-орієнтованої архітектури моніторингу та адаптивного управління функціонально стійкою гетерогенною телекомунікаційною мережею, яка забезпечує підвищення достовірності телеметричних даних, своєчасне виявлення дестабілізуючих впливів та формування ефективних керуючих рішень для підтримання необхідного рівня функціональної стійкості мережевої інфраструктури.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1.Провести аналіз сучасних підходів до моніторингу, управління та забезпечення функціональної стійкості гетерогенних телекомунікаційних мереж, а також дослідити можливості використання технології блокчейн у телекомунікаційних системах.

2.Розробити блокчейн-орієнтовану архітектуру моніторингу та адаптивного управління гетерогенною телекомунікаційною мережею, яка забезпечує інтеграцію засобів телеметрії, розподіленої верифікації даних, оцінювання стану мережі та формування керуючих впливів.

3.Розробити методологію моніторингу та адаптивного управління функціонально стійкою гетерогенною телекомунікаційною мережею на основі блокчейн-верифікації телеметричних даних.

4.Провести експериментальне дослідження запропонованої архітектури та методології, а також виконати їх порівняння з існуючими підходами за показниками функціональної стійкості, достовірності моніторингових даних, часу реагування та ефективності управління мережею.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведений аналіз сучасних підходів до моніторингу та управління телекомунікаційними мережами показав, що переважна більшість існуючих рішень ґрунтується на централізованих системах збору телеметричної інформації, у межах яких достовірність даних визначається рівнем довіри до центрального вузла управління. Разом із тим розвиток гетерогенних телекомунікаційних мереж, що об'єднують різнорідні технології доступу, розподілені центри обробки даних, віртуалізовані мережеві функції та програмно-конфігуровані компоненти, призводить до суттєвого зростання кількості точок потенційної відмови та ускладнює процес отримання достовірної інформації про поточний стан мережевої інфраструктури.

У таких умовах функціональна стійкість мережі визначається не лише технічними характеристиками окремих вузлів, але й здатністю системи управління своєчасно виявляти дестабілізуючі впливи, оцінювати їх можливі наслідки та формувати коригувальні керуючі впливи до моменту виникнення критичних порушень функціонування.

Для формалізації зазначеної задачі будемо розглядати гетерогенну телекомунікаційну мережу як множину взаємопов'язаних вузлів

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

які об'єднані множиною каналів зв'язку

$$L = \{l_1, l_2, \dots, l_k\}. \quad (2)$$

Стан мережі в момент часу tописується вектором

$$S(t) = \{D(t), P(t), A(t), R(t), T(t), C(t)\}, \quad (3)$$

де $D(t)$– доступність мережевих ресурсів; $P(t)$– продуктивність; $A(t)$– рівень інформаційної безпеки; $R(t)$– надійність; $T(t)$– рівень довіри до мережевих вузлів; $C(t)$– ступінь зв'язності мережевої структури.

На відміну від існуючих підходів пропонується додатково враховувати рівень довіри до джерел телеметричних даних, оскільки в умовах кібернетичних впливів компрометація систем моніторингу може призвести до прийняття помилкових управлінських рішень навіть за умови фізичної працездатності мережі.

Для кількісного оцінювання функціональної стійкості введемо інтегральний показник

$$FS(t) = \sum_{i=1}^{n} w_i \, x_i(t), \quad (4)$$

де

$$\sum_{i=1}^{n} w_i = 1, \quad (5)$$

а $x_i(t)$є нормованими показниками функціонування мережі, що характеризують доступність, продуктивність, живучість, безпеку, відновлюваність та рівень довіри до мережевих елементів.

Особливістю запропонованого підходу є те, що значення $x_i(t)$формуються виключно на основі телеметричних даних, достовірність яких підтверджується механізмами розподіленого консенсусу.

Для реалізації запропонованого підходу розроблено блокчейн-орієнтовану архітектуру моніторингу та управління функціонально стійкою гетерогенною телекомунікаційною мережею, структурну схему якої наведено на рис. 1. Архітектура побудована за багаторівневим принципом та поєднує компоненти збору телеметричних даних, розподіленої верифікації інформації, оцінювання функціонального стану мережі, прогнозування розвитку дестабілізуючих впливів і формування адаптивних керуючих впливів.

Основу архітектури становить гетерогенна мережева інфраструктура, яка об'єднує різні технології доступу та передачі даних, зокрема сегменти мобільного зв'язку 4G/5G/6G, програмно-конфігуровані мережі, хмарні та периферійні обчислювальні середовища, а також пристрої Інтернету речей. У процесі функціонування мережеві елементи формують значні обсяги телеметричної інформації, що характеризує їх поточний технічний стан, рівень навантаження, параметри якості обслуговування та безпеки.

Збір і первинна обробка телеметричних даних здійснюються на рівні моніторингу та телеметрії, до складу якого входять колектори телеметрії, модулі контролю показників QoS/QoE, підсистеми моніторингу продуктивності, виявлення відмов та засоби контролю інформаційної безпеки. На відміну від традиційних централізованих систем моніторингу, запропонована архітектура передбачає додатковий рівень довіри, реалізований на основі permissioned blockchain.

Блокчейн-рівень виконує функції розподіленої верифікації телеметричних подій, зберігання незмінного журналу станів мережі, підтримки механізмів репутації мережевих вузлів та виконання смарт-контрактів. При цьому до блокчейну передаються не повні потоки телеметричних даних, а агреговані події, хеш-значення записів моніторингу, результати оцінювання довіри та інформація про прийняті керуючі рішення. Такий підхід дозволяє суттєво знизити навантаження на блокчейн-мережу та одночасно забезпечити цілісність і простежуваність критично важливої інформації.

На основі верифікованих даних функціонує рівень аналітики та оцінювання, який містить модулі аналізу телеметричних потоків, оцінювання функціональної стійкості, виявлення аномалій, прогнозування розвитку дестабілізуючих впливів та визначення рівня довіри до мережевих вузлів. Результатом роботи цього рівня є формування інтегральних оцінок поточного та прогнозованого стану мережі, що використовуються для підтримки прийняття управлінських рішень.

Верхній рівень архітектури реалізує функції адаптивного управління мережею та включає SDN Controller, NFV Orchestrator, Resource Manager, Smart Contract Manager і модуль прийняття рішень. У разі виявлення ознак деградації функціонального стану мережі або прогнозування критичних сценаріїв функціонування система автоматично формує керуючі впливи, які можуть передбачати перебудову маршрутів передавання даних, перерозподіл ресурсів, активацію резервних каналів, міграцію мережевих сервісів або ізоляцію скомпрометованих елементів інфраструктури.

Рис. 1. Блокчейн-орієнтована архітектура моніторингу та управління функціонально стійкою гетерогенною телекомунікаційною мережею

Запропонована архітектура формує замкнений контур забезпечення функціональної стійкості, у межах якого результати моніторингу, оцінювання та прогнозування безпосередньо використовуються для

вироблення керуючих впливів, а інформація про виконані дії зберігається у розподіленому реєстрі та використовується під час наступних циклів прийняття рішень.

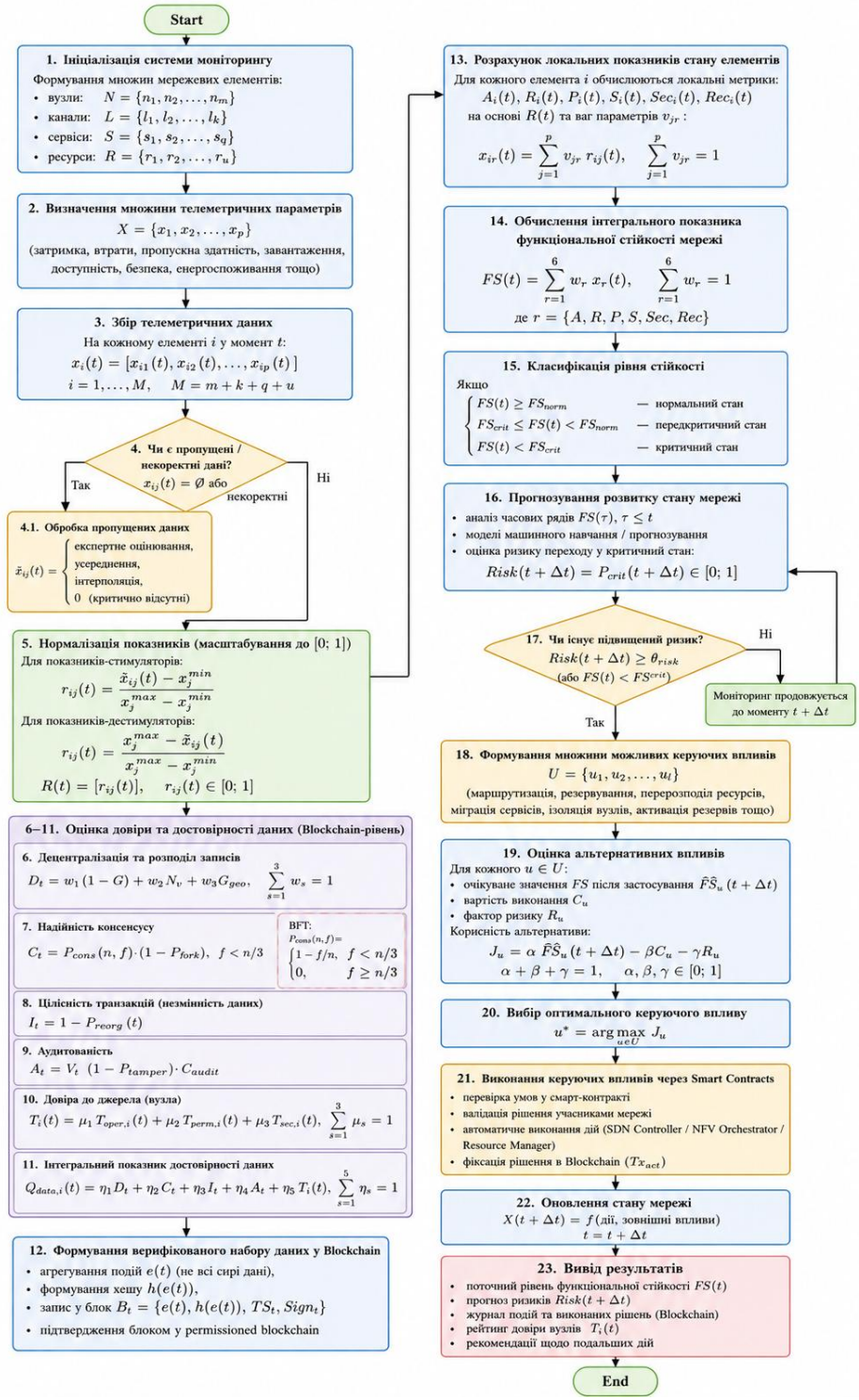

Рис.2. Методологія моніторингу та управління функціонально стійкою мережею

Запропонована методологія моніторингу та управління функціонально стійкою гетерогенною телекомунікаційною мережею ґрунтується на тому, що стан мережі розглядається не як сукупність ізольованих технічних параметрів, а як динамічна багатовимірна система, у якій працездатність окремих вузлів, каналів, сервісів і ресурсів безпосередньо впливає на здатність мережі зберігати виконання

основних функцій за умов дії дестабілізуючих чинників. Саме тому методологія поєднує класичний телекомунікаційний моніторинг, блокчейн-верифікацію достовірності даних, розрахунок інтегрального показника функціональної стійкості, прогнозування ризику деградації та формування керуючих впливів через смарт-контракти.

На першому етапі здійснюється ініціалізація системи моніторингу, у межах якої формується опис гетерогенної телекомунікаційної мережі як сукупності взаємопов'язаних елементів:

$$N = \{n_1, n_2, \dots, n_m\}, \tag{6}$$

де N – множина мережевих вузлів, n_i – окремий вузол мережі, а m – загальна кількість вузлів. До таких вузлів можуть належати маршрутизатори, комутатори, базові станції, сервери, вузли доступу, SDN-контролери, edge-вузли та віртуалізовані мережеві функції. Оскільки гетерогенна мережа не обмежується лише вузлами, додатково задається множина каналів зв'язку

$$L = \{l_1, l_2, \dots, l_k\}, \tag{7}$$

де l_j – окремий канал передавання даних, а k – кількість каналів. Для врахування сервісної складової вводиться множина сервісів

$$S = \{s_1, s_2, \dots, s_q\}, \tag{8}$$

де s_z описує окремий мережевий або прикладний сервіс, а q є кількістю сервісів, доступність яких повинна підтримуватися навіть за умов часткової деградації інфраструктури. Крім того, у методології враховується множина ресурсів

$$R = \{r_1, r_2, \dots, r_u\}, \tag{9}$$

де r_h – окремий ресурс мережі, наприклад пропускна здатність, обчислювальна потужність, буферна пам'ять, резервний канал або енергетичний ресурс, а u – кількість таких ресурсів.

Наступним кроком є визначення множини телеметричних параметрів, які характеризують поточний функціональний стан мережі:

$$X = \{x_1, x_2, \dots, x_p\}. \tag{10}$$

До складу множини X входять показники затримки, втрат пакетів, пропускної здатності, завантаженості каналів, доступності вузлів, рівня безпеки, енергоспоживання, кількості аномальних подій та інших характеристик, які можуть змінюватися під впливом дестабілізуючих чинників. У цьому випадку x_j є окремим телеметричним параметром, а p– загальною кількістю параметрів, що використовуються для подальшого оцінювання.

Для кожного елемента мережі у момент часу tформується вектор телеметричних даних:

$$x_i(t) = \left[x_{i1}(t), x_{i2}(t), \dots, x_{ip}(t)\right], \tag{11}$$

де $x_{ij}(t)$ – значення j-го телеметричного параметра для i-го елемента мережі у момент часу t. При цьому кількість контрольованих елементів визначається як

$$M = m + k + q + u, \tag{12}$$

де m – кількість вузлів, k – кількість каналів, q – кількість сервісів, а u – кількість ресурсів. Такий підхід дозволяє розглядати мережу не лише на рівні фізичної топології, але й на рівні сервісної та ресурсної взаємодії.

Оскільки у реальних умовах телеметричні дані можуть бути неповними або некоректними через збої датчиків, втрату повідомлень, перевантаження каналів моніторингу чи навмисну модифікацію даних, методологія передбачає перевірку наявності пропущених або некоректних значень:

$$x_{ij}(t) = \emptyset \text{або некоректні.} \tag{13}$$

Якщо такі значення виявляються, виконується процедура їх обробки:

$$\tilde{x}_{ij}(t) = \begin{cases} \text{експертне оцінювання}, \\ \text{усереднення}, \\ \text{інтерполяція}, \\ 0, \text{якщо значення критично відсутнє}. \end{cases} \tag{14}$$

Тут $\tilde{x}_{ij}(t)$позначає відновлене або скориговане значення телеметричного параметра. Використання нульового значення у випадку критичної відсутності даних є доцільним тоді, коли відсутність інформації сама по собі розглядається як ознака потенційного порушення функціонування мережі, оскільки для систем критичної інфраструктури неможливість підтвердити стан елемента повинна інтерпретуватися як ризик.

Після цього здійснюється нормалізація показників до єдиної шкали $[0; 1]$, оскільки телеметричні параметри мають різну фізичну природу та різні одиниці вимірювання. Для показників-стимуляторів, зростання яких позитивно впливає на функціональну стійкість мережі, використовується залежність

$$r_{ij}(t) = \frac{\tilde{x}_{ij}(t) - x_j^{min}}{x_j^{max} - x_j^{min}}, \tag{15}$$

а для показників-дестимуляторів, збільшення яких свідчить про погіршення стану мережі, застосовується формула

$$r_{ij}(t) = \frac{x_j^{max} - \tilde{x}_{ij}(t)}{x_j^{max} - x_j^{min}}. \quad (16)$$

У цих формулах $r_{ij}(t)$– нормоване значення j-го параметра для i-го елемента мережі, x_j^{min}та x_j^{max}– мінімально та максимально допустимі або спостережувані значення відповідного параметра. У результаті формується нормована матриця телеметрії

$$R(t) = [r_{ij}(t)], \quad (17)$$

де

$$r_{ij}(t) \in [0; 1]. \quad (18)$$

Саме матриця $R(t)$є базою для подальшої оцінки стану мережевих елементів, оскільки вона переводить різнорідні показники до єдиного вимірювального простору.

Окремим блоком методології є оцінювання довіри до достовірності даних на блокчейн-рівні, оскільки в умовах кібернетичних впливів проблема полягає не лише в погіршенні мережевих параметрів, а й у можливості фальсифікації або прихованої модифікації телеметрії. Для цього спочатку визначається показник децентралізації та розподілу записів:

$$D_t = w_1(1 - G) + w_2 N_v + w_3 G_{geo}, \quad (19)$$

де D_t– рівень децентралізації блокчейн-рівня у момент часу t, G– коефіцієнт концентрації записів або керування, N_v– нормована кількість валідаторів, G_{geo}– показник географічного або доменного розподілу вузлів верифікації, а w_1, w_2, w_3– вагові коефіцієнти, для яких виконується умова

$$\sum_{s=1}^{3} w_s = 1. \quad (20)$$

Чим вищим є значення D_t, тим меншою є залежність системи моніторингу від одного центру довіри, що принципово важливо для функціонально стійкої гетерогенної мережі.

Надійність консенсусу визначається як

$$C_t = P_{cons}(n, f) \cdot (1 - P_{fork}), \quad (20)$$

де C_t – надійність досягнення консенсусу, $P_{cons}(n, f)$ – імовірність успішного консенсусу за наявності nвузлів-учасників і fпотенційно несправних або скомпрометованих вузлів, а P_{fork}– імовірність виникнення розгалуження або конфлікту записів. Для BFT-подібної моделі консенсусу використовується умова

$$P_{cons}(n, f) = \begin{cases} 1 - \frac{f}{n}, & f < \frac{n}{3}, \\ 0, & f \geq \frac{n}{3}. \end{cases} \quad (21)$$

Це означає, що система зберігає здатність до коректної верифікації даних лише тоді, коли кількість несправних або недовірених вузлів не перевищує критичної межі, що є типовою умовою для візантійсько-стійких механізмів консенсусу.

Показник цілісності транзакцій, тобто незмінності записаних даних, задається як

$$I_t = 1 - P_{reorg}(t), \quad (22)$$

де I_t – рівень цілісності записів у момент часу t, а $P_{reorg}(t)$ – імовірність реорганізації, відкочування або суперечливої зміни записів. Чим нижчою є ймовірність реорганізації, тим вищою є довіра до журналу подій, що зберігається у permissioned blockchain.

Аудитованість системи описується формулою

$$A_t = V_t \cdot (1 - P_{tamper}) \cdot C_{audit}, \quad (23)$$

де A_t – рівень аудитованості, V_t – повнота верифікованих записів у момент часу t, P_{tamper} – імовірність несанкціонованої модифікації або підміни даних, а C_{audit} – коефіцієнт доступності аудиту для перевірки дій системи управління. У контексті запропонованої методології цей показник важливий тому, що кожне управлінське рішення повинно бути не лише виконаним, а й простежуваним.

Рівень довіри до джерела, тобто до окремого вузла або елемента мережі, визначається як

$$T_i(t) = \mu_1 T_{oper,i}(t) + \mu_2 T_{perm,i}(t) + \mu_3 T_{sec,i}(t), \quad (24)$$

де $T_i(t)$ – рівень довіри до i-го джерела телеметричних даних у момент часу t, $T_{oper,i}(t)$ – операційна довіра, що враховує стабільність роботи вузла, $T_{perm,i}(t)$ – довіра, пов'язана з його правами та дозволами у системі, $T_{sec,i}(t)$ – безпекова довіра, яка відображає наявність або відсутність інцидентів, а μ_1, μ_2, μ_3 – вагові коефіцієнти, для яких виконується умова

$$\sum_{s=1}^{3} \mu_s = 1. \quad (24)$$

На основі цих компонентів формується інтегральний показник достовірності даних:

$$Q_{data,i}(t) = \eta_1 D_t + \eta_2 C_t + \eta_3 I_t + \eta_4 A_t + \eta_5 T_i(t), \quad (25)$$

де $Q_{data,i}(t)$ – інтегральний рівень достовірності даних, отриманих від i-го елемента мережі, а $\eta_1, \eta_2, \eta_3, \eta_4, \eta_5$ – вагові коефіцієнти, які задовольняють умову

$$\sum_{s=1}^{5} \eta_s = 1. \quad (26)$$

Таким чином, достовірність телеметрії визначається не одним параметром, а сукупністю характеристик блокчейн-рівня, що дозволяє врахувати децентралізацію, надійність консенсусу, незмінність транзакцій, аудитованість і репутацію джерела даних.

Після оцінювання достовірності події агрегуються та записуються у блокчейн. Для цього формується подія

$$e(t), \quad (27)$$

а також її хеш

$$h(e(t)). \quad (28)$$

Запис у блок можна подати як

$$B_t = \{e(t), h(e(t)), TS_t, Sign_t\}, \quad (29)$$

де B_t– блок або запис подій у момент часу t, $e(t)$– агрегована подія, $h(e(t))$– криптографічний хеш події, TS_t– часова мітка, а $Sign_t$– цифровий підпис джерела або валідатора. Завдяки такому поданню забезпечується можливість перевірити, чи не були змінені телеметричні дані після їх фіксації.

На наступному етапі розраховуються локальні показники стану елементів мережі. Для кожного елемента iобчислюються доступність $A_i(t)$, надійність $R_i(t)$, продуктивність $P_i(t)$, живучість $S_i(t)$, безпека $Sec_i(t)$та відновлюваність $Rec_i(t)$. Узагальнено локальний показник можна записати як

$$x_{ir}(t) = \sum_{j=1}^{p} v_{jr}\, r_{ij}(t), \quad (30)$$

де $x_{ir}(t)$ – значення r-ї локальної характеристики для i-го елемента мережі, v_{jr} – вага j-го телеметричного параметра під час формування r-ї характеристики, а $r_{ij}(t)$ – нормоване значення телеметричного параметра. Для вагових коефіцієнтів виконується умова

$$\sum_{j=1}^{p} v_{jr} = 1. \quad (31)$$

Після цього обчислюється інтегральний показник функціональної стійкості мережі:

$$FS(t) = \sum_{r=1}^{6} w_r\, x_r(t), \quad (32)$$

де

$$\sum_{r=1}^{6} w_r = 1, \quad (33)$$

а множина характеристик має вигляд

$$r = \{A, R, P, S, Sec, Rec\}. \quad (34)$$

У цій формулі $FS(t)$ – інтегральний показник функціональної стійкості мережі у момент часу t, $x_r(t)$ – узагальнене значення відповідної характеристики всієї мережі, w_r – ваговий коефіцієнт важливості цієї характеристики, A– доступність, R – надійність, P – продуктивність, S – живучість, Sec – безпека, а Rec – відновлюваність.

Для інтерпретації отриманого значення вводиться класифікація рівня стійкості:

$$\begin{cases} FS(t) \geq FS^{norm}, & \text{нормальний стан,} \\ FS^{crit} \leq FS(t) < FS^{norm}, & \text{передкритичний стан,} \\ FS(t) < FS^{crit}, & \text{критичний стан.} \end{cases} \quad (35)$$

Тут FS^{norm}– порогове значення нормального функціонування, а FS^{crit}– критичний поріг, нижче якого мережа втрачає здатність гарантовано підтримувати виконання основних функцій. Така класифікація дозволяє не лише оцінити поточний стан мережі, але й визначити необхідність переходу до керуючих дій.

Для переходу від реактивного до проактивного управління методологія передбачає прогнозування розвитку стану мережі. На основі історії значень

$$FS(\tau), \tau \leq t, \quad (36)$$

а також моделей машинного навчання або статистичного прогнозування оцінюється ризик переходу мережі у критичний стан:

$$Risk(t + \Delta t) = P_{crit}(t + \Delta t) \in [0; 1], \quad (37)$$

де $Risk(t + \Delta t)$ – прогнозований ризик на інтервалі часу Δt, а $P_{crit}(t + \Delta t)$ – імовірність досягнення критичного стану в майбутній момент часу. Якщо виконується умова

$$Risk(t + \Delta t) \geq \theta_{risk} \quad (38)$$

або

$$FS(t) < FS^{crit}, \quad (39)$$

де θ_{risk} – допустимий поріг ризику, система переходить до формування керуючих впливів.

Множина можливих керуючих впливів задається як

$$U = \{u_1, u_2, \dots, u_l\}, \quad (40)$$

де u_l – окрема дія управління, наприклад зміна маршруту, резервування каналу, перерозподіл ресурсів, міграція сервісу, ізоляція вузла або активація резервного сегмента. Для кожного керуючого впливу оцінюється очікуване значення функціональної стійкості після його застосування:

$$\widehat{FS}_u(t + \Delta t), \quad (41)$$

вартість виконання дії

$$C_u, \quad (42)$$

та фактор ризику

$$R_u. \quad (43)$$

Корисність альтернативного керуючого впливу визначається як

$$J_u = \alpha \widehat{FS}_u(t + \Delta t) - \beta C_u - \gamma R_u, \quad (44)$$

де J_u – корисність альтернативи u, $\widehat{FS}_u(t + \Delta t)$ – прогнозований рівень функціональної стійкості після виконання дії u, C_u – вартість або ресурсна складність реалізації дії, R_u– залишковий ризик, а α, β, γ – вагові коефіцієнти, для яких виконується умова

$$\alpha + \beta + \gamma = 1, \alpha, \beta, \gamma \in [0; 1]. \quad (45)$$

Оптимальний керуючий вплив визначається за правилом

$$u^* = \arg\max_{u \in U} J_u. \quad (46)$$

Отже, система обирає ту дію, яка забезпечує найкращий компроміс між підвищенням функціональної стійкості, витратами на реалізацію та залишковим ризиком.

Виконання керуючих впливів здійснюється через смарт-контракти, які перевіряють умови активації політики управління [12], валідують рішення учасниками мережі, ініціюють автоматичне виконання дії через SDN Controller, NFV Orchestrator або Resource Manager, а також фіксують факт прийняття рішення у блокчейні у вигляді транзакції

$$Tx_{act}. \quad (47)$$

Після виконання керуючих дій стан мережі оновлюється:

$$X(t + \Delta t) = f(\text{дії,зовнішні впливи}), \quad (48)$$

де $X(t + \Delta t)$ – новий вектор стану мережі, а функція f описує залежність майбутнього стану від виконаних керуючих дій та дії зовнішніх дестабілізуючих чинників. Після цього процес моніторингу повторюється, що формує замкнений контур адаптивного управління функціональною стійкістю мережі.

Таким чином, запропонована методологія забезпечує перехід від звичайного спостереження за параметрами мережі до комплексного управління її функціональною стійкістю, оскільки кожне рішення приймається не лише на основі поточної телеметрії, а й з урахуванням достовірності джерел даних, незмінності журналу подій, прогнозованого ризику деградації та очікуваної ефективності керуючих впливів. Її принципова відмінність полягає в тому, що блокчейн-рівень не замінює систему моніторингу, а створює довірену основу для прийняття управлінських рішень, завдяки чому функціональна стійкість гетерогенної телекомунікаційної мережі розглядається як керований динамічний стан, підтримання якого відбувається у безперервному циклі «моніторинг – верифікація – оцінювання – прогнозування – управління – повторний моніторинг».

Експериментальне дослідження

Як видно з рис. 3, запропонована архітектура забезпечує найвище значення інтегрального показника функціональної стійкості. Порівняно з централізованим моніторингом значення $FS(t)$зросло з 0,47 до 0,79, що свідчить про підвищення здатності мережі підтримувати виконання своїх функцій в умовах дії дестабілізуючих чинників. Отриманий результат пояснюється використанням механізмів блокчейн-верифікації телеметричних даних та адаптивного управління мережевими ресурсами.

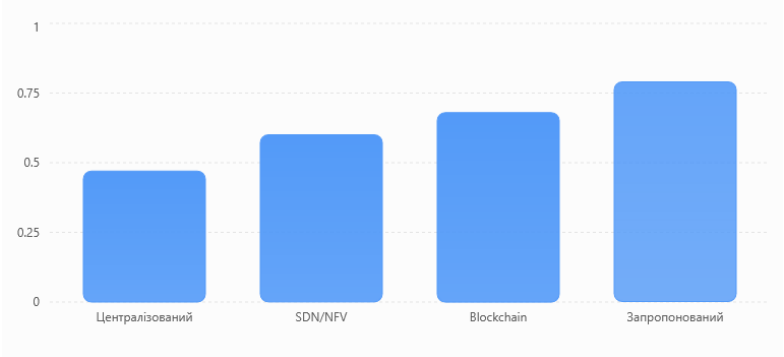

Рис.3. Порівняння середнього значення FS(t) для різних підходів до моніторингу та управління мережею

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження розглянуто проблему забезпечення функціональної стійкості гетерогенних телекомунікаційних мереж в умовах впливу дестабілізуючих чинників, зумовлених відмовами обладнання, перевантаженням мережевих ресурсів, помилками конфігурації та кібернетичними загрозами. Аналіз сучасних наукових підходів показав, що більшість існуючих рішень орієнтована або на моніторинг мережевого середовища, або на забезпечення безпеки даних, тоді як питання довіри до телеметричної інформації та її використання для підтримання функціональної стійкості мережі залишаються недостатньо дослідженими.

У роботі розроблено блокчейн-орієнтовану архітектуру моніторингу та адаптивного управління функціонально стійкою гетерогенною телекомунікаційною мережею, яка інтегрує засоби збору телеметричних даних, механізми блокчейн-верифікації інформації, підсистеми оцінювання функціонального стану мережі та модулі формування керуючих впливів. Запропоноване рішення забезпечує підвищення достовірності моніторингових даних за рахунок використання розподіленого реєстру та дозволяє зменшити ризик прийняття помилкових управлінських рішень у разі компрометації окремих джерел інформації.

Запропоновано методологію моніторингу та адаптивного управління мережею, яка реалізує замкнений цикл «моніторинг – верифікація – оцінювання – прогнозування – управління» та забезпечує своєчасне виявлення ознак деградації функціонального стану мережі. Крім того, розроблено модель оцінювання функціональної стійкості, що враховує показники доступності, надійності, продуктивності, живучості, безпеки та відновлюваності мережевої інфраструктури, що дозволяє комплексно оцінювати її поточний стан та прогнозувати подальший розвиток ситуації.

Результати експериментального дослідження показали переваги запропонованого підходу порівняно з централізованими системами моніторингу та традиційними SDN/NFV-рішеннями. Встановлено підвищення інтегрального показника функціональної стійкості мережі, зростання достовірності телеметричних даних, скорочення часу виявлення дестабілізуючих впливів та часу реагування на них, а також зменшення кількості помилкових керуючих рішень. Найбільша ефективність запропонованої архітектури спостерігається у сценаріях компрометації телеметричних даних та комбінованого впливу технічних і кібернетичних загроз.

Перспективи подальших досліджень полягають у розробленні методів прогнозування функціонального стану телекомунікаційних мереж на основі технологій машинного навчання, удосконаленні механізмів оцінювання довіри до мережевих вузлів, адаптації запропонованої архітектури до середовищ 6G та мережевих зрізів, а також проведенні її практичної апробації в реальних програмно-конфігурованих телекомунікаційних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Isolani, P. H., Haxhibeqiri, J., Moerman, I., Hoebeke, J., Marquez-Barja, J. M., Granville, L. Z., & Latré, S. (2020). An SDN-based framework for slice orchestration using in-band network telemetry in IEEE 802.11. Proceedings of the IEEE Conference on Network Softwarization (NetSoft 2020). https://doi.org/10.1109/NetSoft48620.2020.9165358

2. Zhao, Y., Liu, Y., Wang, J., et al. (2023). SINT: Toward a blockchain-based secure in-band network telemetry architecture. IEEE Transactions on Information Forensics and Security. https://doi.org/10.1109/TIFS.2023.3269891
3. Onopa, S., Pliushch, I., & Strelkovskaya, I. (2024). State-of-the-art and new challenges in 5G networks with blockchain technology. Electronics, 13(5), Article 974. https://doi.org/10.3390/electronics13050974
4. Dorofeev, A., & Kotenko, I. (2020). Blockchain technology in 5G networks. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 20(4), 473–482.
5. Das, D., Chatterjee, M., & Roy, S. (2023). Blockchain enabled SDN framework for security enhancement of 5G applications. Proceedings of the ACM International Conference.
6. Плющ, І. А., & Стрєлковська, І. В. (2020). Управління ресурсами телекомунікаційних мереж нового покоління. Одеса: ОНАЗ ім. О. С. Попова.
7. Лемешко, О. В., & Євсєєва, О. Ю. (2019). Моделі та методи забезпечення якості обслуговування в телекомунікаційних мережах. Харків: ХНУРЕ.
8. Стрєлковська, І. В., Плющ, І. А., & Стрєлковський, Д. В. (2021). Програмно-конфігуровані мережі та управління телекомунікаційною інфраструктурою. Зв'язок, 4, 12–18.
9. Барабаш, О. В., Мусієнко, А. П., & Дахно, Н. Б. (2022). Методи забезпечення кіберстійкості інформаційно-телекомунікаційних систем критичної інфраструктури. Сучасний захист інформації, 2, 5–15.
10. Лєнков, Є. С., Перегудов, Д. А., & Хорошко, В. О. (2021). Забезпечення функціональної стійкості інформаційно-телекомунікаційних систем в умовах дестабілізуючих впливів. Київ: ДУТ.
11. Zhebka, V., Zhebka, S., Bazhan, T., Skladannyi, P., & Sokolov, V. (2024). Methodology for choosing a consensus algorithm for blockchain technology. CEUR Workshop Proceedings, 3665, 106–113.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Victoriia Zhebka
Doctor of Technical Sciences, Professor,
Head of the Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-4051-1190
v.zhebka@duikt.edu.ua

BLOCKCHAIN-ORIENTED ARCHITECTURE FOR MONITORING AND ADAPTIVE MANAGEMENT OF A FUNCTIONALLY RESILIENT HETEROGENEOUS TELECOMMUNICATION NETWORK

Abstract. This paper addresses the problem of ensuring the functional resilience of heterogeneous telecommunication networks under conditions of increasing network infrastructure complexity, growing traffic volumes, and the widespread adoption of cloud computing, edge computing, software-defined networking, and the Internet of Things. It is determined that traditional centralized monitoring systems are characterized by the presence of a single point of failure and do not provide a sufficient level of trust in telemetry data, which may lead to incorrect management decisions in the presence of cyberattacks, equipment failures, or deliberate information falsification. The feasibility of using blockchain technology to ensure the reliability of monitoring data and support adaptive network management processes is substantiated. A blockchain-oriented architecture for monitoring and adaptive management of a functionally resilient heterogeneous telecommunication network is proposed. The architecture integrates telemetry tools, distributed data verification mechanisms, network state assessment modules, forecasting of destabilizing impacts, and decision-making components. A distinctive feature of the proposed approach is the use of a permissioned blockchain for storing aggregated telemetry events, trust assessment results, and information on applied control actions. This ensures record immutability, decision traceability, and an increased level of trust in management processes. A methodology for network monitoring and adaptive management has been developed, implementing a closed-loop cycle of "monitoring – verification – assessment – forecasting – control." The methodology includes the collection and normalization of telemetry data, assessment of their reliability based on decentralization indicators, consensus reliability, transaction integrity, auditability, and data source reputation, as well as the calculation of an integral indicator of network functional resilience. To enable a transition from reactive to proactive management, it is proposed to use forecasting of functional state degradation risks and the selection of optimal control actions considering expected effectiveness, implementation cost, and residual risk. The results of the experimental study confirmed the effectiveness of the proposed approach compared to centralized monitoring systems and conventional SDN/NFV solutions. An increase in the integral indicator of network functional resilience, improved reliability of telemetry data, reduced detection and response times to destabilizing impacts, and a decrease in the number of incorrect management decisions were observed. The obtained results demonstrate the potential of blockchain technologies for building trusted monitoring and adaptive management systems for next-generation telecommunication networks.

Keywords: blockchain, heterogeneous telecommunication network, functional resilience, network monitoring, adaptive management, telemetry data, permissioned blockchain, cyber resilience.

REFERENCES

1. Isolani, P. H., Haxhibeqiri, J., Moerman, I., Hoebeke, J., Marquez-Barja, J. M., Granville, L. Z., & Latré, S. (2020). An SDN-based framework for slice orchestration using in-band network telemetry in IEEE 802.11. Proceedings of the IEEE Conference on Network Softwarization (NetSoft 2020). https://doi.org/10.1109/NetSoft48620.2020.9165358
2. Zhao, Y., Liu, Y., Wang, J., et al. (2023). SINT: Toward a blockchain-based secure in-band network telemetry architecture. IEEE Transactions on Information Forensics and Security. https://doi.org/10.1109/TIFS.2023.3269891
3. Onopa, S., Pliushch, I., & Strelkovskaya, I. (2024). State-of-the-art and new challenges in 5G networks with blockchain technology. Electronics, 13(5), Article 974. https://doi.org/10.3390/electronics13050974
4. Dorofeev, A., & Kotenko, I. (2020). Blockchain technology in 5G networks. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 20(4), 473–482.

5. Das, D., Chatterjee, M., & Roy, S. (2023). Blockchain-enabled SDN framework for security enhancement of 5G applications. Proceedings of the ACM International Conference.
6. Pliushch, I. A., & Strelkovskaya, I. V. (2020). Resource management of next-generation telecommunication networks. Odessa: ONAT named after O. S. Popov.
7. Lemeshko, O. V., & Yevsieieva, O. Yu. (2019). Models and methods for ensuring quality of service in telecommunication networks. Kharkiv: KhNURE.
8. Strelkovskaya, I. V., Pliushch, I. A., & Strelkovskyi, D. V. (2021). Software-defined networks and management of telecommunication infrastructure. Zviazok, 4, 12–18.
9. Barabash, O. V., Musiienko, A. P., & Dakhno, N. B. (2022). Methods for ensuring cyber resilience of information and telecommunication systems of critical infrastructure. Modern Information Security, 2, 5–15.
10. Lienkov, Ye. S., Peregudov, D. A., & Khoroshko, V. O. (2021). Ensuring functional resilience of information and telecommunication systems under destabilizing influences. Kyiv: State University of Telecommunications.
11. Zhebka, V., Zhebka, S., Bazhan, T., Skladannyi, P., & Sokolov, V. (2024). Methodology for selecting a consensus algorithm for blockchain technology. CEUR Workshop Proceedings, 3665, 106–113.

Отримано редакцією журналу / Received: 07.03.26
Прорецензовано / Revised: 20.03.26
Схвалено до друку / Accepted: 25.06.26