DOI 10.31891/2307-5732-2023-319-1-344-350
УДК 004.93

ЛИСЕНКО СЕРГІЙ
Хмельницький національний університет
https://orcid.org/0000-0001-7243-8747
САХНЮК ВІТАЛІНА
Хмельницький національний університет
https://orcid.org/0009-0003-7888-2904
БОНДАРУК Олег
Хмельницький національний університет

МЕТОД СИНТЕЗУ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

В роботі представлено метод та програмно-технічний засіб забезпечення стійкості корпоративної комп'ютерної мережі під дією загроз різного виду. У даній статті буде представлено огляд аспектів стійкості та існуючі підходи до забезпечення стійкої маршрутизації. Ця стаття є результатом багатьох досліджень та експериментів, і, оцінюючи кінцевий результат, можна зауважити, що даний метод може успішно відображати можливу важливість вузла, коли йдеться про динаміку епідемії для різних мережевих моделей для забезпечення стійкості мережі.

Ключові слова: комп'ютерна мережа, стійкість корпоративної комп'ютерної мережі ,стійка маршрутизація

.LYSENKO SERGII, VITALINA SAKHNIUK, BONDARUK OLEG
Khmelnytskyi National University

A METHOD FOR SYNTHESIZING HARDWARE AND SOFTWARE TOOLS TO ENSURE THE STABILITY OF A CORPORATE COMPUTER NETWORK

The paper represents a method for ensuring the resilience of a corporate computer network under the influence of various types of threats. This article will provide an overview of the aspects of resilience and existing approaches to ensuring resilient routing. This article is the result of many studies and experiments, and evaluating the final result, it can be noted that this method can successfully reflect the possible importance of a node when it comes to epidemic dynamics for various network models to ensure network resilience. A possible way to solve the problem was to use the theory of linear stationary systems and the phenomenon of propagation in networks as the basis of the method. Complex interdependencies between their elements characterize various systems.

The method of synthesizing hardware and software means of ensuring the stability of a corporate computer network consists of such steps as representing networks as a linear stationary system, modelling the stability of a computer network in the context of epidemics by using virtual network expansion, studying the stability of a computer network in the context of uncertain data transmission and virtual network expansion, processing input data received from the modelled computer network, etc.

To solve the problem, the method involves the theory of linear stationary systems and the use of the NiR metric, which can successfully reflect the possible importance of a node when it comes to the dynamics of an epidemic for various network models to ensure network resilience.

The method is tested by simulations, the results of which show a high correlation with the actual propagation dynamics modeled by SI and SIR processes. NiR also shows a small variance, which means it is reliable for different computer network topologies. The method also involves finding the most critical nodes in a computer network, for which a cascading failure model was used, which models overloaded nodes as non-functional.

Keywords: computer network resilience, computer network, resilient routing

Вступ. Несправності елементів комунікаційної мережі є неуникненним. Причинами цих несправностей можуть бути різні фактори, такі як природні катаклізми, людські помилки або зловмисні атаки, і це лише кілька з них [1]. Незважаючи на різноманітність характеристик цих несправностей, вони мають одну спільну рису: їх неможливо повністю усунути [2]. Наше повсякденне життя все більше стає залежним від комунікаційних мереж, оскільки обмін інформацією росте експоненційно. В результаті, нові збої в мережевих каналах або вузлах призводять до серйозних втрат даних і прибутку [3-6]. Оскільки комунікаційні мережі все більше охоплюють різні сфери нашого суспільства, очікується, що негативні наслідки від несправностей будуть лише зростати [7-9].

Більшість випадків порушень маршрутизації в мережах зв'язку виникає внаслідок випадкових несправностей каналів або комутаційних пристроїв [10-12], таких як відключення кабелю під час робіт на вулицях, пошкодження підводних кабелів рибальськими суднами або відмови в електропостачанні. Згідно з [13], окремі випадки відмов в каналах відіграють важливу роль у глобальних мережах, становлячи більше 70% від усіх випадків збоїв. В мережах дальнього зв'язку на кожні 10 км оптоволоконного зв'язку припадає в середньому одна відмова кабелю за 12 років [14]. Випадки відмов можуть тривати декілька днів або навіть тижнів, призводячи до серйозного зниження продуктивності мережі. У бездротових мережах проблема ще складніша через те, що характеристики зв'язку залежать від різних факторів, включаючи погодні умови. Однак в локальних мережах з проводовими з'єднаннями відмови в вузлах зазвичай більше, оскільки коротші з'єднання можуть бути краще захищені фізично. Локалізація несправностей та подальший ремонт з'єднань або вузлів може займати від годин до декількох днів, що веде до серйозних збоїв в роботі мережевих служб.

Отже, необхідність розробки мережевих механізмів автоматичної реконфігурації, зокрема для відновлення мережевих послуг до моменту фізичного усунення несправностей елементів мережі, має обгрунтовану потребу. Відсутність вбудованого механізму відновлення пошкодженого трафіку може призвести до значних негативних наслідків для клієнтів, які втратять доступ до мережевих послуг. Щоб впоратися з несправностями елементів мережі, необхідно спочатку аналізувати причини, що призводять до їх виникнення. Таким чином, основною метою дослідження є синтез апаратно-програмних засобів, спрямованих на забезпечення стійкості корпоративної комп'ютерної мережі.

Аспекти стійкості та існуючі підходи до забезпечення стійкої маршрутизації

Згідно з джерелами [15-19], поняття стійкості можна розділити на дві основні категорії: толерантність до викликів, що зосереджена на підходах до проектування мережі з метою забезпечення неперервності обслуговування навіть у випадку виникнення проблем, та достовірність, яка відображає вимірювані характеристики аналізованих систем зв'язку. Взаємодія між цими двома категоріями, відома як надійність, вказує на продуктивність мережі в умовах викликів. Виявлення несправностей також повинно включати локалізацію та ізоляцію несправностей, тобто визначення несправного вузла або зв'язку, необхідних для припинення подальшої передачі інформації через пошкоджений елемент, який потребує відновлення, згідно з джерелами [20-26].

В основі поширення збоїв у мережах лежать дві динаміки - каскади та епідемії, які мають спільні характеристики, такі як обмежена кількість вузлів, в яких вони виникають, та здатність поширюватися по мережі, спричиняючи глобальні перебої. Однак механізм та наслідки цих збоїв відрізняються. Каскадні збої виникають через дефіцит пропускної здатності, тоді як епідемії пояснюються властивістю вірусів поширюватися. Кожен збій також має свій власний тригер. Каскадні збої виникають через вийдення з ладу вузлів або зв'язків, що може бути викликане випадковими збоями, географічно пов'язаними збоями або навмисними атаками. Епідемії спричиняються шкідливим вірусним зараженням, яке поширюється на ретельно вибрані вузли мережі за допомогою шкідливого програмного забезпечення, що поширюється на фізично та логічно підключених сусідніх вузлах. Згідно з [27, 28], можна виділити певні фази порушення роботи системи, такі як підготовка, реагування та фаза відновлення, і вибір стратегії для підвищення стійкості мережі залежить від фази, на якій буде застосована дана стратегія.

Дослідження методів моделювання збоїв корпоративної комп'ютерної мережі

Існують два основних підходи до моделювання - аналітичні та чисельні методи. Аналітичний підхід дозволяє отримати рішення про стан системи без використання симуляцій та великих обчислювальних потужностей. Методи теорії систем застосовуються для аналізу мереж, розглядаючи їх як LTI-системи та оцінюючи реакції системи на вхідні впливи. Отримані результати використовуються для оцінки потужності поширення вузлів та визначення найбільш критичних елементів [29].

Чисельні методи моделювання широко використовуються для спостереження за динамікою всередині мережі. Моделювання мереж є поширеним методом дослідження мереж. Воно дозволяє отримати уявлення про динаміку процесу та надати багато інформації, яку не можна передбачити заздалегідь. Для цього використовується MATLAB - математичне програмне забезпечення, яке охоплює багато аспектів математики та може бути використане для моделювання та обчислень мереж.

Основним підходом до аналізу є використання міри кореляції, зокрема тау-коефіцієнта рангової кореляції Кендалла, який застосовується для перевірки припущень при оцінці вузлів. Ця непараметрична міра зв'язку між ранжованими даними є потужним інструментом для порівняння результатів, отриманих різними методами моделювання [30].

Існує велика кількість методів моделювання збоїв корпоративної комп'ютерної мережі, які далі будуть використані для розробки методу синтезу апаратно-програмних засобів для забезпечення резилієнтності (стійкості) корпоративної комп'ютерної мережі [31].

Метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

З метою вирішення задачі забезпечення стійкості комп'ютерних мереж необхідним є розроблення методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі. Одним з можливих шляхів розв'язку задачі є залучення теорії лінійних стаціонарних систем та явища розповсюдження в мережах як основи методу синтезу апаратно-програмних засобів забезпечення стійкості. Різноманітні системи характеризуються складними взаємозалежностями між їхніми елементами.

Для вирішення задачі метод передбачає залучення теорії лінійних стаціонарних систем, та використання метрики NiR, яка може успішно відображати можливу важливість вузла, коли йдеться про динаміку епідемії для різних мережевих моделей для забезпечення стійкості мережі.

Апробація методу здійснюється шляхом моделювання, результати якого показують високу кореляцію з фактичною динамікою поширення, змодельованою за допомогою процесів SI та SIR.

NiR також показує невелику дисперсію, що означає його надійність для різних топологій комп'ютерних мереж. Також метод передбачає знаходження найбільш критичних вузлів в комп'ютерній мережі, для чого було використано модель каскадних відмов, яка моделює перевантажені вузли як нефункціональні.

Одним з найважливіших кроків є дослідження стійкості. Для цього етапу слід врахувати можливі варіант інфікувань. Інфікування загрозою може моделюватись, починаючи з одного і того ж початкового

вузла для вихідної та розширеної мереж. В ході роботи було здійснено спостереження за кумулятивною кількістю заражених вузлів з плином часу. На рисунку 1 показано майже ідеальний збіг результатів моделювання для вихідної та розширеної мереж, що доводить можливість застосування методу розширення мережі для забезпечення стійкості корпоративної комп'ютерної мережі в умовах епідемій.

Для дослідження стійкості важливе також порівняння динаміки інфікування вихідної мережі $G(V, E)$ та реакції системи, отриманої з розширеної мережі $G_E(V_E, E_E)$. Подібно до прикладу, показаного на рисунку 1, спочатку моделюється динаміка поширення за допомогою моделі SI. На кожному часовому кроці t заражений вузол намагається заразити сприйнятливого сусіда. Інфекція передається з ймовірністю $p = 0.4$. Таким чином, сприйнятливий вузол заражається з ймовірністю $P = 1 - (1 - p)k$, де k - кількість інфікованих сусідів. Дані, зібрані за допомогою симуляції, включають кумулятивну кількість інфікованих вузлів $\underline{vu}(n)$ та кількість інфікованих вузлів на кожному часовому кроці $\underline{vu}(n)$, яка є похідною від $\underline{vu}(n)$.

Потім система створюється з розширеної мережі $GE(VE, EE)$ з ймовірністю інфікування $p = 0.4$. На рисунку 2 зображено динаміку епідемії як vu(n), змодельовану на вихідній мережі з ймовірністю інфікування $p = 0{,}4$. Значення $\underline{vu}(n)$ порівнюються зі ступінчастою реакцією $\underline{y_H}(n)$ системи, створеної на основі розширеної вихідної мережі. Результати, отримані в результаті моделювання та реакція системи сильно корелюють.

Рис. 1. Лінійна стаціонарна система з розрахунком крокової та імпульсної реакції

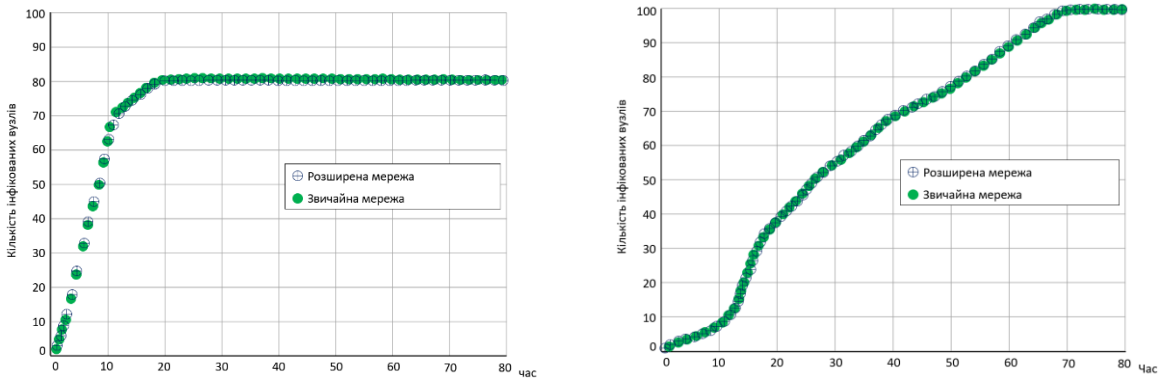

Рис. 2. Динаміка поширення загрози в звичайній мережі та розширеній

Наступним кроком методу забезпечення стійкості корпоративної комп'ютерної мережі є оброблення вхідних даних, отриманих з комп'ютерної мережі. Три типи мереж, що використовуються в моделюванні, генеруються випадковим чином за трьома різними мережевими моделями.

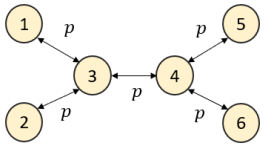

Рис. 3. Неорієнтована мережа з M = 6 вузлами та N = 5 зв'язками та ймовірністю передачі p

Щоб продемонструвати можливість застосування ЛСС підходу до аналізу динаміки поширення було взяти неорієнтовану мережу $G(V, E)$ з $|V| = 6$ вузлів і $|E| = 5$ ребер (рис. 3) і застосовано підхід ЛСС.

Ймовірність передачі змінюється з $p1 = 0.6$ до $p2 = 0.2$. Ймовірність передачі однакова для всіх пар сусідніх вузлів, і вважається, що інфекція походить з вузла. На основі інформації про топологію $G(V, E)$ ми будуємо дві системи ЛСС: першу з $p_1 = 0.6$ і другу з $p_2 = 0.2$. Потім було обчислено ступінчасті відгуки для отриманих систем. Було виявлено різницю між нахилами двох отриманих кривих (рис. 4). Крива з більшим

нахилом представляє ступінчасту характеристику системи, отриману від мережі з більшою швидкістю передачі. Таким чином, аналізуючи реакцію даної системи, можна оцінити динаміку епідемії у відповідній мережі. Нахил кривої відповідає швидкості поширення епідемії в кожний момент часу. Ця ж величина відповідає і імпульсному відгуку.

0,6 та p = 0,2

Наступним кроком запропонованого методу є вирішення проблеми модифікації комп'ютерної мережі. Це вимагає додаткової модифікації топології шляхом віртуального розширення мережі. Пропонований метод використовує міру Node Imposed Response (NiR), яка фіксує потенціал поширення вузла. Алгоритми видалення циклів можуть змінити топологію мережі так, що деякі шляхи стають недоступними, особливо в неорієнтованих мережах, де потрібно вибирати напрямок ребра. Щоб зберегти найважливіші шляхи з вихідного вузла і мінімізувати кількість видалених ребер, слід були знайти правильний метод видалення циклів. Після маніпуляцій з вихідним графом ми створюємо матрицю системи A таким чином, що $A = A_{adj}^{T}$. Всі ненульові елементи замінились значенням d, так що $\forall a_{ij} = 0 : a_{ij} = d$, і $0 < d < 1$. Додаткове дослідження показує, що дисперсія між значеннями NiR для всіх вузлів стає вищою при меншому d.

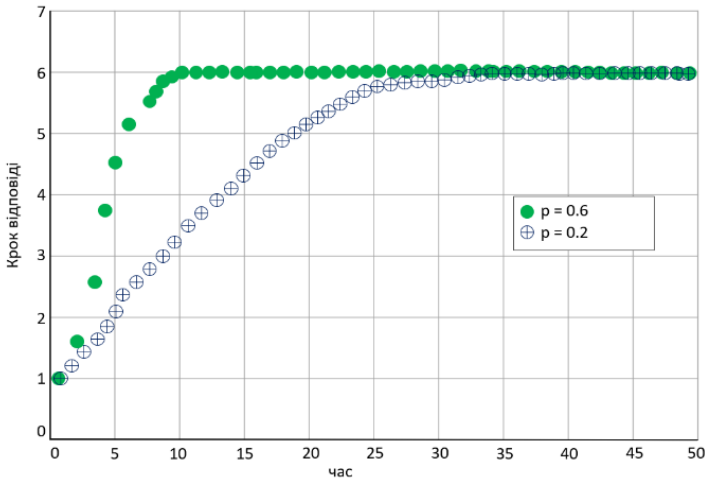

Рис. 4. Покрокові реакції системи, отримані з мережі з використанням двох ймовірностей зараження p =

Наступним кроком методу забезпечення стійкості корпоративної комп'ютерної мережі є знаходження найбільш критичних вузлів в комп'ютерній мережі. Для вирішення даної підзадачі було використано модель каскадних відмов, яка моделює перевантажені вузли як нефункціональні. Модель дозволяє встановити факт, що атака на один важливий вузол (з високим початковим навантаженням) може викликати каскадний ефект, який може призвести до збою всієї мережі та, як наслідок, серйозного збою служби.

Таким чином, вважатимемо найбільш критичним вузлом той, видалення якого спричинить найбільшу шкоду мережі. Пошкодження визначається як зворотна величина найбільшого підключеного компонента, що залишився після моделювання каскаду. Після видалення вузла і відносний розмір найбільшого з'єднаного компонента, що залишився, дорівнює G_i і так само після видалення j відносний розмір найбільшого з'єднаного компонента дорівнює G_j . Якщо $G_i < G_j$, ми робимо висновок, що вузол і є більш критичним.

Для вирішення підзадачі знаходження множини k найбільш критичних вузлів мережі було використано генетичний алгоритм. Набір з 100 найбільш критичних вузлів включається в додаткову оцінку. Початковий простір розв'язків різко зменшується, але все ще має значний розмір (F_n=10 = 1,73 × 1013). Генетичний алгоритм уможливлює знайти розв'язок через поступове покращення пристосованості всього покоління. Оптимізація, що проводилася, була цілочисельною задачею, де рішенням є масив з n цілих чисел в діапазоні від 1 до 100, і кожне значення зіставляється з відповідним ідентифікатором вузла. Максимально 100 вузлів можна було об'єднати в групи, що складаються з k елементів кожна. Набір з 100 вузлів було визначено за допомогою попереднього аналізу впливу окремих вузлів. Підхід генетичного алгоритму для знаходження критичної групи представлено у вигляді псевдокоду нижче.

1: Вхід: G(V, E)

2: Параметри ініціалізації: розмір популяції встановлено на pop = 200 з обмеженням на максимальне Ngen = 1200 поколінь

3: Створення початкової популяції: початкова популяція створюється випадковим чином із рівномірним розподілом

4: поки кількість поколінь досягає максимуму до t> Ngen

5: виконати кросовер

6: тоді як для всіх рішень у популяції

7: видалити вузли t ініціалізувати каскад

8: виконати оцінку t, значенням функції пристосованості, яка є розміром найбільшої компоненти.

9: відсортувати рішення з останнього покоління

10: повернути групу вузлів

Підхід ГА дає однакові або гірші результати для всіх критичних груп. Додаткова перевірка за допомогою генетичного алгоритму підтримує рішення зосередити пошук на відносно невеликій кількості критичних вузлів.

Таким чином, метод синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі можна умовно розділити на такі кроки:

1) представлення мережі як лінійної стаціонарної системи;
2) моделювання стійкості комп'ютерної мережі в умовах епідемій шляхом застосування віртуального розширення мережі;
3) дослідження стійкості комп'ютерної мережі в умовах невизначеної передачі даних та віртуального розширення мережі;
4) обробка вхідних даних, отриманих зі змодельованої комп'ютерної мережі;
5) виявлення впливових розповсюджувачів, що порушують стійкість мережі;
6) знаходження найбільш критичних вузлів в комп'ютерній мережі;
7) знаходження множини k найбільш критичних вузлів мережі.

Експериментальні дослідження апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі

З метою здійснення апробації та перевірки ефективності запропонованого методу синтезу апаратно-програмних засобів забезпечення стійкості корпоративної комп'ютерної мережі було здійсненого ряд експериментальних досліджень. На рисунку 5 показано приклад невеликої мережі з n = 10 вузлами. Кожен з вузлів має своє значення NiR, вказане вище. Значення NiR вказує на потужність поширення загрозу, тобто вузол космп'ютерної мережі з вищим NiR швидше заразить всю мережу або більшу її частину.

Моделювання проводилося наступним чином: інфекція зароджується в одному вузлі; інфекція поширюється зі швидкістю передачі p, і в кінцевому підсумку охоплює всю мережу; потім розраховується час, необхідний для повного інфікування. Твердження підтвердилось моделюванням динаміки поширення SI та порівнянням результатів з отриманими значеннями NiR. Моделювання проводилося наступним чином: інфекція зароджується в одному вузлі; інфекція поширюється зі швидкістю передачі p, і в кінцевому підсумку охоплює всю мережу; потім розраховується час, необхідний для повного інфікування. Якщо час повного інфікування коротший, то вузол має потенціал для швидшого поширення інфекції і вважається більш важливим (тобто більш впливовим). Для того, щоб порівняти значення NiR та змодельований потенціал розповсюдження, здійснюється сортування вузлів як за значенням NiR, так і за потужністю розповсюдження, отриманою в результаті здійсненого моделювання.

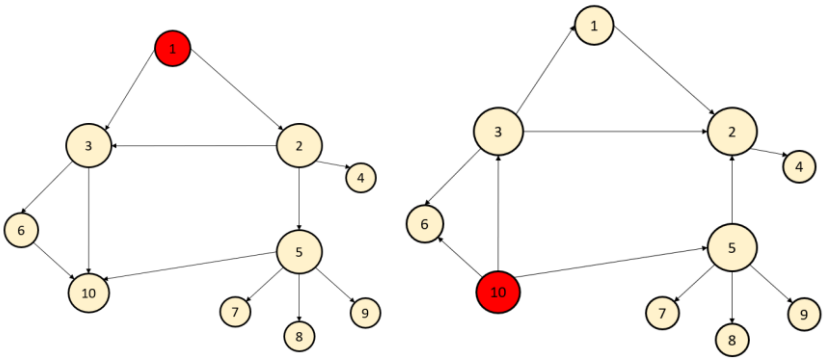

Рис. 5. Виявлення впливових розповсюджувачів, що порушують стійкість мережі

Таким чином, було визначено кілька окремих груп вузлів з різним потенціалом поширення (рис. 6).

У випадку невеликої мережі значення NiR точно відображає потенціал розповсюдження, оскільки групування вузлів збігається з отриманим в результаті чисельного моделювання. Ймовірно, що для великих мереж, де n>10, буде багато вузлів з дуже схожими значеннями NiR, що відповідає вродженому принципу безмасштабності багатьох мереж, з великою часткою не-вузлів.

Для того, щоб перевірити кореляцію між NiR та результатами моделювання для всіх сімейств мереж, використаних для аналізу було проведено експерименти. Моделювання проводилось на декількох мережах з використанням моделей SI та SIR. Базовим значенням для моделі SI є час t, необхідний для часткового (50% або 70% вузлів) інфікування у випадку одного вузла-джерела i. Для моделі SIR значенням, яке використовується для порівняння, є розмір спалаху (загальна кількість вузлів, які заразилися) після t часових кроків виконання. Результати, отримані за допомогою моделювання для кожного з вузлів, порівнюються з NiR та п'ятьма іншими мірами центральності (міжцентровість, центральність, ступінь, DS та центральність за H-індексом). Показник NiR демонструє високу кореляцію з результатами моделювання разом з низькою дисперсією, часто перевершуючи всі п'ять показників як у моделях SI, так і SIR.

Єдиним показником, який показує однакові результати, є центральність DS, параметри якого залежать від динаміки поширення загроз.

У випадку відмови критичного вузла, будь-яка частка між 0,02 до 0,1 найменш навантажених вузлів може бути вилучена, щоб запобігти подальшого каскадування. На рисунку 4.4б показано порівняння розміру компоненти після каскаду з заходами захисту та без них для десяти найбільш критичних вузлів. Частка видалених вузлів після початкової атаки була обрана такою f = 0.04. Для кожного критичного вузла і каскад пом'якшується таким чином, що результуюче значення G завжди більше, якщо захисні заходи реалізовано належним чином. Ідея полягає в тому, щоб визначити набір вузлів, які слід підготувати до вилучення у випадку найнебезпечніших відмов. Відмова одного з десяти найбільш критичних вузлів з Таблиці 1 спричинить найбільшу шкоду. Тому проводиться наступний аналіз: Для кожного з найбільш критичних вузлів моделюється відмова і вибираються найменш навантажені вузли. Саме ці вузли є кандидатами на навмисне видалення після початкової атаки. Певна кількість вузлів часто з'являється у списку кандидатів на різні відмови і. Це ті вузли, які, швидше за все, матимуть менше навантаження у випадку навмисної атаки. Механізм захисту повинен видалити частку f з усіх вузлів, крім вузлів-кандидатів.

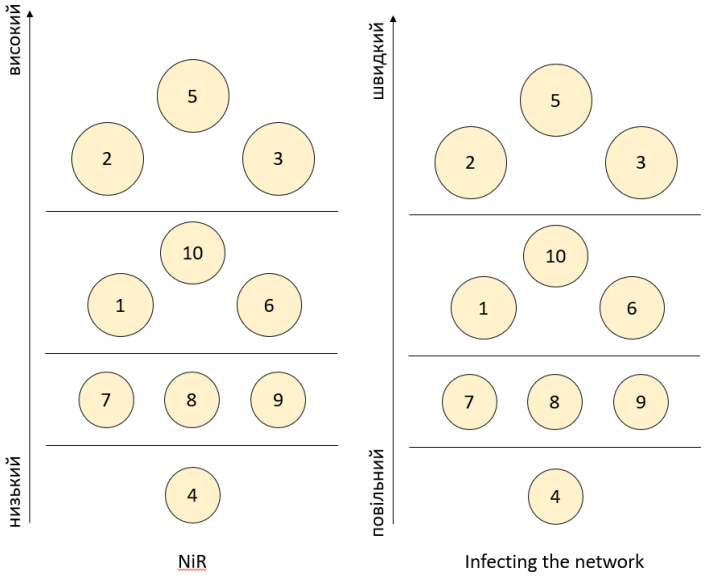

Рис. 6. Потенціал поширення

В абсолютних числах кількість вершин, які будуть навмисно видалені, становить $23 \leq nir \leq 115$. Не має значення, яку саме вершину буде видалено, доки число nir не виходить за межі.

Таблиця 1

Вплив видалення вузлів з синтезованої мережі

№ вузла мережі	$G_{\alpha=1.01}$	$G_{\alpha=1.10}$	$G_{\alpha=1.30}$	$G_{\alpha=1.50}$
10	0.312	0.230	0.310	0.409
19	0.289	0.348	0.528	0.542
42	0,439	0.467	0.455	0.387
12	0.458	0.492	0.912	0.915
41	0.532	0.485	0.676	0.687

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У роботі було досліджено наявні методи забезпечення стійкості корпоративної комп'ютерної мережі, а також розроблено удосконалений метод, який враховує різні загрози у мережах.

Також було запропоновано вдосконалений метод синтезу апаратно-програмних засобів для забезпечення стійкості корпоративної комп'ютерної мережі. Цей метод використовує теорію лінійних стаціонарних систем та метрику NiR, яка дозволяє відображати важливість вузлів в контексті динаміки поширення епідемії для різних мережевих моделей. Метод був протестований шляхом моделювання, результати якого показали високу кореляцію з фактичною динамікою поширення, що була змодельована за допомогою процесів SI та SIR. Метрика NiR також демонструє невелику дисперсію, що свідчить про її надійність для різних топологій комп'ютерних мереж. Парадигма, на якій базується підхід ЛСС, дозволяє використовувати різні варіації вихідної метрики, наприклад, вибір декількох вхідних та вихідних точок, що дозволяє оцінити вплив багатьох вузлів мережі на процес поширення.

Більш вразливі вузли з більшою ймовірністю будуть досягнуті з набору обраних вхідних вузлів. Аналіз не обмежується незваженими мережами. Той самий підхід може бути використаний навіть для зважених мереж, просто включивши ваги в матрицю системи.

Також метод передбачає знаходження найбільш критичних вузлів в комп'ютерній мережі, для чого було використано модель каскадних відмов, яка моделює перевантажені вузли як нефункціональні.

Література

1. Agarwal P.K., Efrat A., Ganjugunte, S., Hay, D., Sankararaman, S., Zussman, G.: The resilience of WDM networks to probabilistic geographical failures. *Proc. 30th Annual Joint Conference of the IEEE Computer and Communications Societie*s, 2013. pp. 1521–1529.
2. Asthana R., Singh Y.N., Grover W. p-cycles: an overview. *IEEE Commun. Surv. Tutorials*. 2013. 12(1), 97–111.
3. Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable and Secure Comput*. 2014. 1(1), 11–33.
4. Caini C., Cruickshank, H., Farrell, S., Marchese, M.: Delay- and disruption-tolerant networking (DTN): an alternative solution for future satellite networking applications. *Proc. IEEE* 2021. 99(11).
5. Cetinkaya, E.K., Sterbenz, J.P.G.: A taxonomy of network challenges. *Proc. 9th International Conference on Design of Reliable Communication Networks*, 2013. pp. 322–330 ()
6. Chołda P., Jajszczyk A. Recovery and its quality in multilayer networks. IEEE/OSA J. *Lightwave Technol.* 2010. 28(4), 372–389.
7. Chołda, P., Tapolcai, J., Cinkler, T., Wajda, K., Jajszczyk, A.: Quality of Resilience as a network reliability characterization tool. *IEEE Netw.* 2011, 23(2), 11–19.
8. Colle, D., De Maesschalck, S., Develder, C., Van Heuven, P., Groebbens, A., Cheyns, J., Lievens, U., Pickavet, M., Lagasse, P., Demeester, P.: Data-centric optical networks and their survivability. *IEEE J. Sel. Areas Commun.* 2012. 20(1), 6–20.
9. Cucurull, J., Asplund, M., Nadjm-Tehrani, S., Santoro, T.: Surviving attacks in challenged networks. IEEE Trans. Dependable and Secure Comput. 2015. 9(6), 917–929.
10. Fangming L., Bo L., Lili Z., Baochun L., Hai J., Xiaofei L. Flash crowd in P2P livestreaming systems: fundamental characteristics and design implications. *IEEE Trans. Parallel. Distrib. Syst.* 2012. 23(7), 1227–1239.
11. Geva M., Herzberg A., Gev Y. Bandwidth Distributed Denial of Service: attacks and defences. *IEEE Secur. Priv.* 2014. 12(1), 54–61 ()
12. Grover, W.D. Mesh-based Survivable Networks. Options and Strategies for Optical, MPLS, SONET, and ATM Networks. Prentice Hall PTR, Upper Saddle River (2014) Grover, W.D.: The protected working capacity envelope concept: an alternate paradigm for automated service provisioning. *IEEE Commun. Mag.* 2014. 42(1), 62–69 ()
13. Grover, W.D., Shen, G. Extending the p-cycle concept to path-segment protection. In: Proc. IEEE International Conference on Communications (IEEE ICC'03), 2, pp. 1314–1319 (2013)
14. Haddadi H., Rio, M., Iannaccone G., Moore A., Mortier R. Network topologies: inference, modeling, and generation. IEEE Commun. Surv. Tutorials 10(2), 48–69 (2009)
15. Haider, A., Harris, R. Recovery techniques in Next Generation Networks. *IEEE Commun. Surv. Tutorials,* 2014 9(3), 2–17
16. Heegaard, P.E., Trivedi, K.S. Network survivability modeling. *Comput. Netw*. 53(8), 1215–1234 (2011)
17. Ho, P.-H. State of the art progress in developing survivable routing schemes in mesh WDM networks. *IEEE Commun. Surv. Tutorials* 6(4), 2–16 (2014)
18. Ho, P.-H., Tapolcai, J., Cinkler, T. Segment shared protection in mesh communication networks with bandwidth guaranteed tunnels. *IEEE/ACM Trans. Networking* 12(6), 1105–1118 (2022)
19. Ho, P.-H., Tapolcai, J., Mouftah, H.: On achieving optimal survivable routing for shared protection in survivable Next-Generation Internet. *IEEE Trans. Reliab.* 53(2), 216–225 (2014)
20. Jaumard, B., Rocha, C., Baloukov, D., Grover, W.D. A column generation approach fordesign of networks using path-protecting p-cycles. *In: Proc. 6th International Workshop on Design of Reliable Communication Networks (DRCN'07)*, pp. 1–8 (2017)
21. Jung J., Krishnamurthy B., Rabinovich M. Flash crowds and denial of service attacks: characterization and implication for CDNs and web sites. *Proc. 11th International Conference on World Wide Web (WWW'02*), 2012. pp. 293–304.
22. Kappenman, J. A perfect storm of planetary proportions. *IEEE Spect. Mag*. 2012. 49(2), 26–31.
23. Khabbaz, M.J., Assi, C.M., Fawaz, W.F. Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges. *IEEE Commun. Surv. Tutorials* 14(2), 2012. 607–640.
24. Kitamura, Y., Lee, Y., Sakiyama, R., Okamura, K. Experience with restoration of Asia Pacific network failures from Taiwan earthquake. *IEICE Trans. Commun*. E90-B(11), 2017. 3095–3103.
25. Kodian, A., Grover, W.D. Failure-independent path-protecting p-cycles: efficient and simple fully preconnected optical-path protection. *IEEE/OSA J. Lightwave Technol.* 2015. 23(10), 3241–3259.
26. Kompella, K., Swallow, G. Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures, IETF RFC 4379. 2016.
27. Maruyama, H., Legaspi, R., Minami, K., Yamagata, Y. General resilience: taxonomy and strategies. *Proc. 2014 International Conference and Utility Exhibition on Green Energ for Sustainable Development (ICUE'14),* 2014. pp. 1–8.
28. Mingsen X., Wen-Zhan S., Deukhyoun H., Jong-Hoon K., Byeong-Sam K. ECPC: preserve downtime data persistence in disruptive sensor networks. *Proc. IEEE Mobile Ad-Hoc and Sensor Systems* (MASS'13), 2013 pp. 281–289.
29. Misseri X., Gojmerac I., Rougier J.-L. IDRD: enabling inter-domain route diversity. *Proc. IEEE International Conference on Communications*, 2013. pp. 3536–3541.
30. Mukherjee, B.: Optical WDM Networks. Springer, New York. 2016.
31. *Nicol D.M., Sanders W.H., Trivedi K.S. Model-based evaluation: from dependability to security. IEEE Trans. Dependable and Secure Comput.* 2017. 1(1), 48–65.