БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ ТА ІНТЕРНЕТ / NETWORK & INTERNET SECURITY

DOI: 10.18372/2225-5036.29.18072

ДЕКОМПОЗИЦІЯ ТЕХНОЛОГІЇ КОМП'ЮТЕРНИХ МЕРЕЖ ПРИ ЇХ ПРОЕКТУВАННІ

Володимир Хорошко, Юлія Хохлачова, Наталія Вишневська

Національний авіаційний університет

ХОРОШКО Володимир Олексійович, д.т.н., професор
Рік та місце народження: 1945 рік, м. Харків, Україна.
Освіта: Київський інститут інженерів цивільної авіації, 1968 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, технічні системи захисту інформації, аналіз функціонування складних систем.
Публікації: більше 500 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

ХОХЛАЧОВА Юлія Євгеніївна, к.т.н., доцент
Рік та місце народження: 1981 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2004 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, оцінювання уразливостей, оптимізація інформаційних систем.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

ВИШНЕВСЬКА Наталія Сергіївна, старший викладач
Рік та місце народження: 1977 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2001 рік.
Посада: старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.
Наукові інтереси: кіберзахищеність інформаційних систем, кіберризики енергетичних систем.
Публікації: більше 20 наукових публікацій.
E-mail: nataliia.vyshnevska@npp.nau.edu.ua.
Orcid ID: 0000-0001-9036-6556.

***Анотація**. У цій статті розглядається питання безпеки і топології в комп'ютерних мережах, де практичні методи захисту інформації не мають достатнього теоретичного підґрунтя. Підкреслюється важливість врахування топології мережі при забезпеченні безпеки. Висвітлено проблеми з системними підходами до системного аналізу та інтеграції, а також відсутність ефективних механізмів оцінки якості систем. Запропоновано використання методів декомпозиції для оптимального проектування топології комп'ютерних мереж та мінімізації обчислювальних ресурсів. Ми також зазначаємо, що успіх методу залежить від характеру конкретної топології системи та інформаційних потоків. Підкреслюючи дискретний підхід до оптимізації системи, методи декомпозиції можуть бути корисними для пошуку спрощень для складних систем. Ця стаття підкреслює важливість теоретичного обґрунтування методів захисту інформації в комп'ютерних мережах.*

Вона ставить під сумнів традиційний практичний підхід до захисту даних і підкреслює необхідність комплексного підходу до мережевої безпеки. Детально проаналізовано вплив топології на рівень захисту та висвітлено переваги методів декомпозиції для вирішення цієї проблеми. Показано, що різноманітність систем вимагає індивідуального підходу і що дослідження методів декомпозиції може стати кроком до ефективного забезпечення безпеки в складних інформаційних системах.

***Ключові слова**: комп'ютерна мережа, технологія комп'ютерних мереж, метод декомпозиції, топологія структури, оптимальне проєктування.*

Постановка проблеми

Не зважаючи на те, що сучасний прогрес у галузі глобальних комп'ютерних систем, мереж і засобів, мультимедіа привів до розроблення численних методів, призначених для гарантування безпечного передавання інформації каналами телекомунікацій та використання їх у цілях комунікації, алгоритмів синтезу комп'ютерних систем, ці методи часто не мають потрібного теоретичного обґрунтування, опис їх властивостей, переваг і паролів ґрунтується лише на практичному досвіді їх використання, що не гарантує їх успішної роботи у разі застосування в позаштатних ситуаціях.

Результативне використання завдань аналізу і синтезу систем не може бути забезпечено одними лише способами простого опису їх поведінки в різних умовах – системотехніка висуває проблеми, які потребують якісної оцінки характеристик.

Тому на перший план виступає проблема, як створити таку систему, яка б спроможна була з мінімальних витрат виконувати максимальні завдання. Цю проблему необхідно вирішувати поступово, починаючи з головного етапу – проектування комп'ютерної системи.

Аналіз останніх досліджень і публікацій

У таких умовах все більше поширюється аксіома, що захист інформації повинен за всіма характеристиками відповідати масштабом загроз. І при цьому слід враховувати, що топологія комп'ютерних мереж дуже впливає на захищеність інформації у них. Відхилення від цього правила призведе до подальших збитків. Для кожної комп'ютерної системи є оптимальний рівень захищеності, який базується на її топології та який необхідно постійно підтримувати. Немає сумнівів, що захист критично важливих для комп'ютерних систем масивів повинен відповідати міжнародним, державним та корпоративним нормативним і методичним документам. Однак немає відповіді на найважливіше питання - наскільки рішення, яке пропонується або реалізується, справді вдале, яка його запланована та реальна ефективність. Такому положенню, яке наявне в комп'ютерній системі, але є неможливим у галузі гарантування інформаційної безпеки, відповідає низки причин:

- ігнорування системного підходу до методології аналізу та синтезу систем;
- відсутність механізмів повного та достовірного підтвердження якості системи;
- недоліки нормативно-методичного гарантування заданого рівня безпеки, насамперед у галузі показників і критеріїв.

Мета та постановка завдання

У цій роботі пропонується опис та умова застосування метода декомпозиції, який дозволяє значно скоротити витрату обчислювальних ресурсів при вирішенні завдання оптимального проектування загальної топологічної структури комп'ютерних мереж.

Виклад основного матеріалу дослідження

Розглянутий спосіб зниження трудомісткості задачі заснований на тому, що в процесі вирішення задачі оптимізації достатньо знати не точне значення цільової функції на кожному кроці, а лише значення її зміни. Тому якщо можна побудувати таку функцію, яка буде простіше в обчислювальному відношенні і в певному сенсі еквівалентна вихідної цільової функції, то за рахунок побудови такої функції та використання її як цільової можна зменшити трудомісткість розв'язання задачі.

У задачі, що розглядається, основні складності при обчисленні цільової функції пов'язані з розмірністю задачі. Так, наприклад, в мережі з 10 вузлів існує 2^{45} варіантів розташування каналів зв'язку. При сучасному рівні розвитку обчислювальної техніки (ОТ) виконати аналіз усіх варіантів неможливо. Тому мета даного методу зниження розмірності системи.

Основним способом у аналізованій процедурі є фіксація певних компонент матриці злучень в залежності від виконання деяких умов.

Завдання загального топологічного синтезу формується так [1]:

Нехай задана матриця інформаційних потоків між кожною парою вузлів: $\Lambda = \|\Lambda_{ij}\|$.

Матриця вартості оренди каналів: $\mathrm{C} = \|\mathrm{c}_{ij}\|$.

Необхідно знайти кількість і тип каналів зв'язку n_{rh} в кожному з'єднані (r,h) зі швидкістю передачі V_{rh}, тобто матрицю злучень: $N = \|n_{rh}\|$; і величини потоків у кожному злученні: $F = \|f_{rh}\|$.

Таким чином, щоб:

$$f_1(n_{rh}) = \sum_r \sum_h C_{rh} n_{rh} \to \min_N , \qquad (1)$$

$$f_2(n_{rh}) = \sum_r \sum_h V_{rh} n_{rh} \to max\, N , \qquad (2)$$

при обмеженнях:

$$\sum_r \sum_h f_{rh} = \sum_i \sum_j \Lambda_{ij} , \qquad (3)$$

$$f_{rh} \le V_{rh} n_{rh} . \qquad (4)$$

Пропонується звести задачу (1)-(4) до послідовності підзавдань, у яких екстремум шукається на деяких підмножинах матриці злучень $N^k \subset N$ і вирішується системою меншої розмірності:

$$f_1^k(n_{rh}, n_{rh}^k) \to \min_{N^k} f_1(n_{rh}), \quad (5)$$

$$f_2^k(n_{rh}, n_{rh}^k) \to \min_{N^k} f_2(n_{rh}), \quad (6)$$

$$\sum_{r\in j}\sum_{h\in j}\left(f_{rh}^{(n_{eh})} + \delta f_{rh}\right) = \sum_{i\in J}\sum_{j\in J}\Lambda_{ij} + \sum_{r\in S}\sum_{h\in S} f_{rk}^k, \quad (7)$$

$$f_{rh} \le V_{rh} n_{rh} (r \in J, n \in j), \quad (8)$$

де $J \cap S = 0$, $J \cup S = (1, 2, \ldots, j)$ – множина вузлів мережі, $n_{rk}^k - arg arg\, min\left\{f_1^{k-1}\left(n_{rh}, n_{rh}^{k-1}\right), n_{rh} \in N^{k-1}\right\} \cap$ $arg\, max\left\{f_2^{k-1}\left(n_{rh}, n_{rh}^{k-1}\right), n_{rh} \in N_S^{k-1}\right\}$.

Тут екстремум розуміється в значенні оптимальності за Парето, а δf_{rh}, має сенс похибки, що виникає при обчисленні f_{rh} в результаті формально зафіксованих змінних Π_{rh}. З умови (7) отримуємо матрицю $\left\| f_{rh}\left(n_{rh}\right) + \delta f_{rh}(n_{rh}^k) \right\|$.

Похибка $\delta f_{rh}(n_{rh}^k)$ виникає як результат того що величини f_{rh}^k задані у точці n_{rh}^k, а не у точці n_{rh}, для якої розв'язується система. Значення функції f_1^k і f_2^k однозначно визначається елементами множини N^k або розбиття процесів J і S, а її значення залежать від точки n_{rh} і точки n_{rh}^k якій обчислюється f_{rh}^k.

Таким чином основна ідея пропонованого методу полягає в тому, що для кожної множини N^k виділяється матриця сполук $\left\|n_{rh}^k\right\|$, що містить такі змінні $n_{rh}, (r, h) \in S$, які відносно мало змінюються в процесі прийняття рішення k –ої підзадачі. Компоненти цієї матриці обчислюються лише початковій точці даної підзадачі, а в подальшому процесі її вирішення вважаються постійними. У цій же точці n_{rh}^k для кожної підзадачі можуть визначатися залежно від конкретних реалізацій методу наступні величини: значення функції $f_1\left(n_{rh}^k\right)$, $f_2(n_{rh}^k)$ та їх збільшення у цій точці, безліч N^k та безлічі процесів J та S.

Обчислення $f_1\left(n_{rh}^k\right)$ та $f_2(n_{rh}^k)$ проводиться з метою контроля за перебігом процесу оптимізації (5)-(8). Це означає, що у випадках, коли умови, що забезпечують збіжність процесу (5)-(8) до Парето-оптимальної множини виконується не для всіх підзадач, то на множині $n_{rh} \in arg\, min\left\{f_1^{k-1}\left(n_{rh}, n_{rh}^k\right) \middle| n_{rk} \in N^{k-1}\right\} \cap$ $arg\, max\left\{f_1^{k-1}\left(n_{rh}, n_{rh}^k\right) \middle| n_{rk} \in N^{k-1}\right\}$.

Значення функції f_1 може стати не менше (f_2 – не більше), ніж у початковій точці n_{rh}^{k-1} для цієї підзадачі. В цьому випадку для множини N^{k-1} може бути визначена більш точна функція $f_1^{k-1}(f_2^{k-1})$ та $(k-1)$ підзадача розв'язку ще раз або в кількісті початкової точки для k - ї підзадачі обирається n_{rh}^{k-1}. За рахунок застосування даної процедури основний обсяг обчислень проводиться при вирішенні більш простих підзадач виду (5)-(8), а обчислення f_1 та f_2 в точках n_{rh}^k гарантує побудову оптимізуючої послідовності.

Збільшення функції f_1 та f_2 обчислюється в тих випадках, коли множини J та S заздалегідь не задані, і підзавдання генеруються безпосередньо в ході рішення.

Визначимо зв'язок похибок для компонент n_{rh}^k та поточної n_{rh} часток змінних. Розглянемо вираз (7). Він може бути записаний у вигляді:

$$\sum_{r\in J}\sum_{h\in J} f_{rh}\left(n_{rh}\right) = \sum_{i\in J}\sum_{j\in J}\Lambda_{ij} + \sum_{r\in S}\sum_{h\in S}(f_{rh}^k + \delta f_{rh}^k). \quad (9)$$

Обчислюючи (9) з (8) отримуємо:

$$\sum_{r\in J}\sum_{h\in J}\delta f_{rh} = \sum_{r\in S}\sum_{h\in S}\delta f_{rh}^k. \quad (10)$$

Нехай у (4) має місце граничний випадок $f_{rh} = V_{rh} n_{rh}$, тоді:

$$\begin{cases} \delta f_{rh} = V_{rh}\delta n_{rh} \\ \delta f_{rh}^k = V_{rh}\delta n_{rh}^k \end{cases}. \quad (11)$$

Підставляючи (11) до (10), отримуємо: $\sum_{r\in J}\sum_{h\in J} V_{rh}$ $\delta n_{rh} = \sum_{r\in S}\sum_{h\in S} V_{rh}\delta n_{rh}^k$.

Звідси, зв'язок між похибками визначення фіксованої частини каналів і змінюваної, визначається структурою множин J і S, а також швидкостями передачі інформації по каналах і структурі цих множин. Далі представимо інтерпретацію методу фіксації змінних на основі теорії ієрархічних багаторівневих систем.

Введемо безліч точок $\overline{N}$, що є розв'язанням задач виду (5)-(8):

$$\overline{N} = \left\{ n_{rh}^{k} \in N : n_{rh}^{k} = argmin\left[f_{1}^{k-1}\left(n_{rh}, n_{rh}^{k-1}\right)\right] \cap argmax\left[f_{2}^{k-1}\left(n_{rh}, n_{rh}^{k-1}\right) n_{rh} \in N^{k-1}, k = 1, 2 \ldots \right] \right\}.$$

Нехай у процесі (5)-(8) використовується 2m різних функцій f_1^k, $f_2^k (k = 1, 2, \ldots, m)$. Тоді декомпозиційну схему розв'язання задачі, яка розглядалася раніше (1)-(4), можна представити у вигляді дворівневої системи з кінцевим числом підсистем, координація в яких здійснюється за допомогою прогнозування взаємодій і зміни обмежень [2]. Перший рівень ієрархічної системи (рис.1), що розглядається, містить одну підсистему-задачу-координатор, другий рівень місить з сукупності m задач або підзадач (підсистем). На вхід кожної підсистеми другого рівня подається координуючий сигнал $\gamma \in \Gamma$, вироблений підсистемою першого рівня. В свою чергу на вхід підсистеми першого рівня подається результат роботи (в цьому випадку (n_{rh}^k) кожної підсистеми другого рівня.

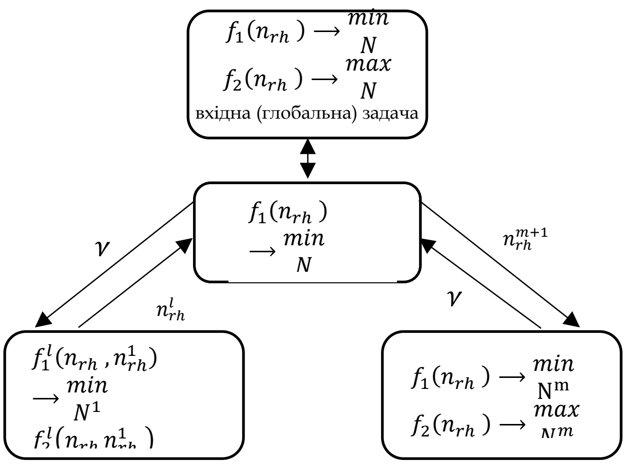

Рис. 1. Перший рівень ієрархічної системи

Координація шляхом прогнозування взаємодій має на увазі задане за допомогою сигналу γ фіксованих значень (прогнозів) для відповідних входів локальних підзадач. Сполучними входами в даному випадку є значення f_{rh}^k, а координуючий сигнал γ містить номер $k, (k = 1, 2, \ldots, m)$ чергової локальної задачі, яка буде вирішуватися, множина N^k, початкова точка n_{rh}^k.

Координація шляхом змін обмежень має на увазі задане за допомогою сигналу γ множини доступних рішень, що й відбувається у цьому випадку, як завдання множин N^k для k-ої підзадачі.

В [1,2] наводяться твердження про застосування різних принципів координації і, в тому числі, принципу прогнозування взаємодій.

Однак, при цьому передбачається, що допустимі множини N^k є перерізом множини N і кожна підсистема знаходить свою оптимальну компоненту рішення n_{rh}^{*k}, таку, що рішення глобальної задачі (1)-(4) представлено у вигляді $n_{rh}^* = (n_{rh}^{*1}, \ldots, n_{rh}^{*m})$.

Таке припущення буде виконуватися для запропонованого методу, якщо він реалізований за допомогою ділення проектованої системи на m частин (підсистем), що не перетинаються. При цьому кожна k-а підсистема оптимізується окремо за допомогою своїх функцій f_1^k і f_2^k. Тоді підсистеми другого рівня відповідають оптимізованим частинам об'єкта, що проектується. Кожна множина N^k визначається обмеженнями на величину проектованих параметрів елементів до k-ї підсистеми, а величини $f_{rh}^k(n_{rh}^k)$ містять інформацію про значення змінних у вузлах, що належать решті підсистем.

У використаних позначеннях твердження, що розглядається в [2] про застосування принципу прогнозування взаємодій, можна сформулювати в наступному вигляді:

- принцип застосовний, якщо з твердження випливає:

1. n_{rh}^{*k} є рішеннями відповідних локальних підзадач і при цьому для всіх підзадач $f_{rh}^k = 0$;

2. n_{rh}^* є рішеннями глобальної задачі.

На відміну від [2] у цій роботі в загальному випадку розмірність будь-якої з множин N^k може збігатися з розмірністю множини N, тобто в k-ї локальної підзадачі з такою безліччю допустимих рішень змінюються всі компоненти n_{rh}. Такий спосіб реалізації методу фіксації змінних не вкладається у схему принципів координації, викладених у [2] та є їх узагальненням.

Твердження про застосування принципу прогнозування взаємодій для нашого випадку можна сформулювати наступним чином.

Нехай всі локальні підзадачі такі, що розмірність будь якої множини N^k збігається з розмірністю N. Тоді твердження про застосовність принципу прогнозування взаємодій має вигляд:

- принцип застосовується, якщо з твердження випливає:

1. Існує підзадача з номером k, така, що вирішення глобальної задачі n_{rh}^* міститься в N^k, $n_{rh}^* =$

$argmin\left\{ f_1^k(n_{rh}, n_{rh}^k) \right\} \cap argmax\left\{ f_2^k(n_{rh}, n_{rh}^k) \right\} n_{rh} \in N^k$ і при цьому для цієї задачі правильно прогнозується взаємодія, а саме $f_{rh}^k = 0$;

2. f_{rh}^* є розв'язком глобальної задачі.

Коли поміж m підзадач другого рівня містяться такі підзадачі де шукається компонента рішення $n_{rh}^* = (n_{rh}^{*1}, \ldots, n_{rh}^{*l})$, а в інших підзадачах змінюються всі компоненти n_{rh}, твердження про застосовність має такий вигляд:

- принцип застосовний, якщо з твердження випливає:

1. Або $n_{rh}^* = (n_{rh}^{*1}, \ldots, n_{rh}^{*l})$ є розв'язком відповідних локальних підзадач і при цьому для всіх підзадач $f_{rh}^k = 0$ або існує підзадача з номером k, $(k = l+1, \ldots, m)$, така що розв'язок глобальної задачі міститься в N^k є, n_{rh}^* розв'язком k-ї підзадачі і при цьому для даної підзадачі $f_{rh}^k = 0$;

2. n_{rh}^* є рішенням глобальної задачі.

Дворівнева система складатиметься з підсистем такого виду в тому випадку, коли, наприклад, спочатку знаходиться деяке наближення рішення за допомогою підсистем з номерами $k = 1, k, l$, далі отриманий результат уточнюється за допомогою систем з номерами $k = l+1, K, m$, які шукають рішення на множинах з меншими лінійними розмірами, ніж вихідне і, можливо, з використанням більш простих цільових функцій, ніж f_1 та f_2. В цьому випадку шуканий результат може бути отриманий як при вирішені перших l локальних підзадач, так і при вирішені однієї з підзадач з номером $k = l+1, K, m$.

Проведемо порівняльний аналіз запропонованого методу з відомими методами релаксації та закріплення змінних. Основним наслідком застосування цього методу є зменшення кількості варіантів стану системи, що підлягають аналізу. В методах релаксації обмежень типу Джоффріона або Розена [3,4] спрощення задачі відбувається за рахунок менших витрат ресурсів на задоволення обмежень, що є в задачі, тоді як в даному випадку знижується трудомісткість обчислень цільової функції.

Додамо до сказаного, що у методах релаксації частина обмежень просто відкидається, тоді як у цьому разі зменшення кількості варіантів відбувається за рахунок штучного фіксування значень деяких компонент матриці N, об'єднаних в матрицю N^k, і вирази інших компонент через фіксовані. Завдяки такому прийому виключаються варіанти, що відповідають змінним з N^k.

Порівняно з методами закріплення змінних [5, 6, 7] однією з відмінностей є те, що в існуючих методах закріплення вважаються константами деякі змінні, які при цьому дійсно мають постійні значення, а в даному методі лише формально вважається, що частина змінних має фіксовані значення, а фактично ці значення у певних точках просто не обчислюються. Тим самим знімається будь-який контроль за зміною цих змінних і діляться завдяки використанню апріорної інформації про те, що дані змінні досить мало змінюються в цій підзадачі.

Далі розглянемо умови збіжності ітераційного процесу (5)-(8) до вирішення вихідних задач.

Введемо наступні позначення: $g(n_{rk})$ – напрямок потоку, який визначається методом математичного програмування що використовується. Передбачається, що $g(n_{rk})$ однозначна функція для всіх $n_{rk} \in N$. Далі застосовуючи це визначення аргумент будемо опускати. $\overset{j}{N}$ - множина точок оптимізуючою послідовністю, яка будується використаним методом математичного програмування, тобто:

$$\overset{j}{N} = \left\{ n_{rh}^k \in N : \left\{ f_1(n_{rh}^{k+1}) < f_1(n_{rh}^k) \right\} \cap \right.$$

$$\left. \cap \left\{ f_2(n_{rh}^{k+1}) < f_2(n_{rh}^k) \right\}, k = 0,1 \right\},$$

де n_{rh}^0 – задана початкова точка; G - множина напрямів g, що є m-м наближенням задачі одновимірного пошуку на g, а саме $n_{rh}^{mg} = n_{rh}^{(m-1)g} + \rho \frac{g}{\|g\|}$, де ρ – крок одновимірного пошуку, де ρ такий, що $n_{rh}^{(m-1)} \in N$; N^g – множина точок одновимірного пошуку на напрямку $g \in G$,що вибирається в деякій точці $n_{rh}^k \in \hat{N}$, тобто

$$N^g = \left\{ n_{rh}^{mg} \in N : n_{rh}^{mg} = n_{rh}^{(m-1)g} + \right.$$

$$\left. \rho \frac{g}{\|g\|}, n_{rh}^{oj} = n_{rh}^k, n_{rh}^k \in \hat{N} \right\}.$$

Визначимо прирощування в точці n_{rh}^{mg} за напрямом g для значень f_{rh} та цільових функцій:

$$\Delta_g f_{rh}(n_{rh}^{mg}) = f_{rh}(n_{rh}^{(m+1)g}) - f_{rh}(n_{rh}^{mg}),$$

$$\Delta_g f_i(n_{rh}^{mg}) = f_i(n_{rh}^{(m+1)g}) - f_i(n_{rh}^{mg}), (i = 1, 2),$$

$$\Delta_g f_i^k(n_{rh}^{mg}, n_{rh}^k) = f_i(n_{rh}^{(m+1)g}, \delta n_{rh}^{(m+1)gk}) - f_i(n_{rh}^{mg} - n_{rh}^{mgk}), (i = 1, 2).$$

Сформуємо теорему. Для цього приймемо наступне припущення:

1. $f_1(\bullet)$ та $f_2(\bullet)$ задовольняють на N вимогам збіжність використовуваного методу математичного програмування до Парето оптимальної області;

2. Функції $f_i^k(n_{rh}^{mg}, n_{rh}^k), (i = 1, 2)$ задовольняють на множині вимогам збіжності до відповідним точок $n_{rh}^k \in N$;

3. Існує номер k, такий що відповідає k-ой під задачі $\arg\min\{f_1(n_{rh})n_{rh} \in N\} \cap \arg\max\{f_2(n_{rh})\ n_{rh} \in N\} \in N^k$;

4. для будь якого $k = 0, 1, k, g \in G$ та будь якої точки $\{n_{rh}^{mg} \in N^k\}$ рівності:

$$\begin{cases} sign\Delta_g f_1^k(n_{rh}^{mg}, n_{rh}^k) = sign\Delta_g f_1(n_{rh}^{mg}) \\ sign\Delta_g f_2^k(n_{rh}^{mg}, n_{rh}^k) = sign\Delta_g f_2(n_{rh}^{mg}) \end{cases},$$

тоді:

$$\lim_{k \to \infty} n_{rh}^k = n_{rh}^* = \arg\min\{f_1(n_{rh}), n_{rh} \in N\} \cap$$
$$\cap \arg\max\{f_2(n_{rh}), n_{rh} \in N\},$$

де n_{rh}^* належить Парето – оптимальній множині, а ітераційний процес (5)-(8) сходиться до розв'язання задачі (1)-(4).

Доведення

Оскільки послідовність чисел $\{f_1(n_{rh}^k)\}$, $n_{rh}^k \in \hat{N}$ монотонно спадає за побудовою та обмежена знизу, а послідовність $\{f_2(n_{rh}^k)\}, n_{rh}^k \in \hat{N}$ монотонно зростає та обмежена зверху, то існує $\left\{\lim_{k \to \infty} f_1(n_{rh}^k)\right\}$ та $\left\{\lim_{k \to \infty} f_2(n_{rh}^k)\right\}$. Точку з множини Парето – оптимальних рішень, є результатом ітераційного процесу (5)-(6) позначимо n_{rh}^*.

Припустимо протилежне n_{rh}^* не є розв'язком задачі (5)-(8), тобто відповідно до пропозиції 1, існує точка $n_{rh}^o \neq n_{rh}^*$ така, що $n_{rh}^o = \arg\min\{f_1^k(n_{rh})n_{rh} \in N\} \cap \arg\max\{f_2(n_{rh})n_{rh} \in N\}$.

Розглянемо k-ту під задачу, для якої виконується пропозиція 3. За пропозицією 1 існує точка $n_{rh}^j \notin \hat{N}$ і $g(n_{rh}^j) \in G$ така, що $g = n_{rh}^o - n_{rh}^j$ і для деякої точки n_{rh}^{mg} на напрямі g при $\rho = \|n_{rh}^o - n_{rh}^{mg}\|$ виконується нерівність $\Delta g f_1(n_{rh}^{mg}) < 0, \Delta g f_2(n_{rh}^{mg}) > 0$, в той же час із пропозиції про те, що $n_{rh}^o \neq n_{rh}^*$, з цього випливає те, що якщо:

$$n_{rh}^o \neq \arg\min\{f_1^k(n_{rh}, n_{rh}^k), n_{rh} \in N^k\} \cap$$
$$\arg\max\{f_2^k(n_{rh}, n_{rh}^k), n_{rh} \in N^k\},$$

тоді:

$$\Delta g f_1^k(n_{rh}^{mg}, n_{rh}^k) \geq 0,$$
$$\Delta g f_2^k(n_{rh}^{mg}, n_{rh}^k) \leq 0,$$

і означає що для цих k, g та n_{rh}^{mg}:

$$sign\Delta g f_1^k(n_{rh}^{mg}, n_{rh}^k) \neq sign\Delta g f_1(n_{rh}^{mg}),$$
$$sign\Delta g f_2^k(n_{rh}^{mg}, n_{rh}^k) \neq sign\Delta g f_2(n_{rh}^{mg}),$$

що суперечить умові теореми, отже $n_{rh}^o = n_{rh}^*$.Отже, теорема доведена.

Розглянемо деякі конкретні властивості задачі (1)-(4), які сприяють успішному застосуванню метода:

1. Наявність в системі, що оптимізують слабо зв'язаних підсистем. Що менше ступень зв'язності системи, яку розглядають, то більше можлива похибка методу, яка мало впливає на загальне значення цільової функції. Це дозволяє формувати більше число компонент змінних, які підвищують ефективність методу. Зокрема, якщо дозволяє специфіка задачі, матрицю $\|f_{rh}\|$ бажано перетворити до блокового-діагонального вигляду. В цьому випадку, степінь зв'язності підсистем, що складаються з вузлів, та відповідають ненульовим блокам матриці з іншими вузлами буде дорівнювати нулю. У випадку, коли пошук слабо зв'язаної підсистеми проходить в матриці загального вигляду, важливим фактором, що сприяє застосуванню декомпозиції, є непогана обумовленість матриць $\|N^k\|$;

2. Наявність для деяких множин $N^g, g \in G$ слабо змінюваних змінних, які об'єднуються в фіксовану матрицю $\|f_{rh}^S\|$. Зазначимо, що цей фактор э одним з найбільш важливих, оскільки прийом штучного фіксування матриці є єдиним джерелом похибок даного методу;

3. Монотонність функцій $f_1(n_{rh})$ та $f_2(n_{rh})$;

4.Невелике число l кроків одновимірного потоку. Ця умова зв'язана з процесом накопичення похибки, йому відповідає величина $\left\| \sum \Delta_g f_{rh}^S (n_{nh}^{jg}) \right\|$. Оскільки основна мета декомпозиції – економія ресурсів при вирішенні задачі, бажано за рахунок, невикористання інших факторів, які сприяють використанню декомпозиції забезпечити таке значення l, яке, з одного боку відповідає вимогам розв'язуваної задачі, а з іншого боку дозволяє в l точках даного направлення обраховувати наближені функції $f_i^k\left(n_{rh}, n_{rh}^k\right)$, $(i=1,2)$.

На підставі цих факторів пропонуємо варіанти їх використання при побудові підзадач вигляду (5)-(8):

1. Нехай властивості мережі дозволяють виділити підсистеми, які для будь якого $n_{rh} \in N^g, g \in G$, будуть слабко зв'язані з мережевими вузлами системи (наприклад, мережі в топології «зірка» - можна вважати слабозв'язаними). Тоді для будь якої множини N^g визначається матриця $\left\| f_{rh}^j \right\|$, що відповідає одній із слабозв'язуючих підсистем, так щоб матриця $\left\| f_{rh}^j \right\|$ достатньо мало змінилася на множині N^g. Матриця $\left\| f_{rh}^j \right\|$ однозначно визначає функції $f_i^k\left(n_{rh}, n_{rh}^k\right), (i=1,2)$, які будуть аналізуватися;

2.Нехай властивості мережі дозволяють класифікувати змінні по сегментам їх зміни для будь якого $n_{rh} \in N^g$ (це може бути зумовлено, наприклад, очевидними відмінностями в поведінці різних груп вузлів проектованої системи). Тоді для будь якої множини N^g з вузлів що відповідають найбільш змінюваним компонентам матриці $\left\| f_{rh} \right\|$ обирається достатньо слабка зв'язана підсистема. Іншими словами, матриця $\|f_{rh}^j\|$ формується з найбільш сильно змінюваних змінних таким чином, щоб вона містила як найменшу кількість компонент і при цьому виконувались умови застосування декомпозиції. Нехай для задачі (1)-(4) побудована відповідність між множинами N^k і множиною функцій $f_i^k (i=1,2)$, тобто задача представлена у вигляді (5)-(8).

При розв'язку цієї задачі можна виділити наступну послідовність дій:

- крок 1. $k := 0$ вибрати початкову точку n_{rh}^0;
- крок 2. Вибрати в точці n_{rh}^k направлення пошуку g, тобто визначити множину N^k;
- крок 3. Розв'язується підзадача:

$$f_1^k (n_{rh}^{mg}, n_{rh}^k) \to \min_{N^k},$$

$$f_2^k (n_{rh}^{mg}, n_{rh}^k) \to \max_{N^k};$$

- крок 4. Якщо:

$$f_1\left[\arg\min\left\{ f_1^k (n_{rh}, n_{rh}^k), n_{rh} \in N^k \right\}\right] < f_1(n_{rh}^k),$$

$$f_1\left[\arg\max\left\{ f_2^k (n_{rh}, n_{rh}^k), n_{rh} \in N^k \right\}\right] < f_2(n_{rh}^k),$$

тоді можна припустити:

$$n_{rh}^{k+1} = arg\min\left\{ f_1^k(\bullet)\right\} \cap \arg\max\left\{ f_2^k(\circ)\right\}, k = k+1,$$

інакше множині N^k можна представити у відповідність більш точну цільову функцію f_i^k та перейти до кроку 2;

- крок 5. Якщо:

$$n_{rh}^k = \arg\min\left\{ f_1^k (n_{rh}, n_{rh}^k), n_{rh} \in N^k \right\} \cap$$
$$\arg\max\left\{ f_2^k (n_{rh}, n_{rh}^k), n_{rh} \in N^k \right\},$$

то необхідно зупинитися, інакше перейти до кроку 1 та повторити послідовність дій.

Висновки. Розглянутий метод дозволяє значно скоротити витрати обчислювальних ресурсів при розв'язку задач оптимального проектування загальної топології комп'ютерних мереж. Подібні специфічні закономірності в оптимізаційних системах, що дозволяють застосувати метод фіксації змінних, залежить від топології системи та характеру інформаційних потоків. Тому важко дати будь які універсальні рекомендації для системи будь якого виду. Але, як показує практика, більшість складних систем володіє тією чи іншою властивістю, яка дозволяє спростити задачу, а умови застосовності декомпозиції орієнтують на пошук таких властивостей.

Список літератури

[1]. Згуровський М.З., Панкратова Н.Д. Основи систематичного аналізу. К:Вид. група BHV, 2007. 544 с.

[2]. Месарович М., Мако Д., Такахара І. Теорія ієрархічних багаторівневих систем. К:Техніка, 1993. 248 с.

[3]. Лесдок Л.С. Оптимизация больших систем М:Наука, 1975. 432с.

[4]. Geoffrion A.M. Elements of logre-scecele mathematical programing. Paris–Management Scsence, 2000, №11. pp.652-691.

[5]. Тамашевський В.М. Моделювання систем. К:Вид.група BHV, 2007. 352 с.

[6]. Левин Г.М. Ганаев В.С. Декомпозиционные методы оптимизации проектных решений. Минск: Наука и техника, 1998. 240 с.

[7]. Изурнов В.И. Декомпозиции в задачах большой размерности. 2-е изд. Минск: Наука и техника, 2001. 352 с.

УДК 004.681.3

Khoroshko V., Khokhlachova Y., Vyshnevska N. Decomposition of computer network technology in their design

Abstract*. This article discusses the issue of security and topology in computer networks, where practical methods of protecting information do not have a sufficient theoretical basis. The importance of considering the network topology in ensuring security is emphasized. The problems with system approaches to system analysis and integration, as well as the lack of effective mechanisms for assessing the quality of systems are highlighted. It is proposed to use decomposition methods to optimally design the topology of computer networks and minimize computing resources. We also note that the success of the method depends on the nature of the specific system topology and information flows. By emphasizing a discrete approach to system optimization, decomposition techniques can be useful for finding simplifications for complex systems. This article emphasizes the importance of the theoretical justification of information protection methods in computer networks. It challenges the traditional practical approach to data protection and emphasizes the non-workability of an integrated approach to network security. The influence of topology on the level of protection is analyzed in detail and the advantages of decomposition methods for solving this problem are highlighted. It is shown that the diversity of systems requires an individual approach and that the study of decomposition methods can become a step towards to effectively ensure security in complex information systems.*

Keywords*: computer network, computer network technology, decomposition method, structure topology, optimal design.*

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Volodymyr Khoroshko, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Yuliia Khokhlachova, candidate of technical sciences, associate professor, associate professor of the department of security of information technologies of the National Aviation University.

Вишневська Наталія Сергіївна, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.
Nataliya Vyshnevska, senior lecturer at the Information Technology Security Department of the National Aviation University.

Отримано *29 вересня 2023 року*, затверджено редколегією *30 жовтня 2023 року*