УДК 519.711.7:519.816

DOI: 10.15407/fmmit2025.40.005

Модифікований алгоритм процесу обтинання для виділення *k*-серцевин складних мереж

Дмитро Поліщук[1], Олександр Поліщук[2]

[1] Кандидат технічних наук, Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України, 79060, Україна, Львів, вул. Наукова 3 «б», e-mail: do.polishchuk@gmail.com

[2] Доктор технічних наук, старший науковий співробітник, Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України, 79060, Україна, Львів, вул. Наукова 3 «б», e-mail: od_polishchuk@ukr.net

Проаналізовано найбільш вживаний для виділення k-серцевин складних мереж (СМ) алгоритм процесу обтинання. Визначений основний недолік цього алгоритму, який полягає у можливості виродження k-серцевини у порожню множину навіть якщо ця мережа містить достатньо велику кількість вузлів зі ступенем не меншим ніж k. Для усунення цього недоліку запропоновано модифікований алгоритм процесу обтинання та показано його дієздатність для виділення k-серцевин на прикладах низки модельних та реальних складних мереж. k-серцевини обрані у якості груп найважливіших елементів СМ, які можуть стати метою одночасної цілеспрямованої атаки на мережу та розроблено сценарій такої атаки, який враховує потенційні спроможності нападника. Запропоновано спосіб оцінювання наслідків успішної атаки на k-серцевину, який базується на поняття області її сусідства.

Ключові слова: складна мережа, *k*-серцевина, процес обтинання, сусідство, уразливість, цілеспрямована атака, оцінювання наслідків.

Вступ. Виділення найважливіших за певними ознаками компонент великих складних систем є одним із основних способів спрощення дослідження та кращого розуміння їх структури і законів функціонування. У теорії складних мереж (ТСМ) таким способом є визначення серцевин різних типів [1, 2]. Одним із найбільш вживаних методів є виділення так званої *k*-серцевини складної мережі, тобто такої її найбільшої підмережі, ступінь вузлів якої є не меншим, ніж значення $k>1$ [3]. Визначення *k*-серцевини базується на понятті ступеня вузла. Подібним чином можна вводити різні типи серцевин СМ, використовуючи у якості характеристики вузла інші показники його важливості у мережі (центральності за посередництвом, власним значенням, Хірша тощо). Однак, для мереж, які налічують величезну кількість вузлів (галактика, людський мозок, населення Землі) це породжує неабиякі обчислювальні труднощі [4, 5]. *k*-серцевини застосовуються під час досліджень структурних особливостей складних мережевих систем у біології та екології, комп'ютерних та соціальних мереж, великих даних, поширення інформації та епідемій небезпечних інфекційних захворювань, в економіці та фінансах, пошуку спільнот та аналізі текстів, на транспорті, в енергетиці та сейсмології і навіть під час вивчення особливостей кримінального світу [6, 7]. Проблематиці застосування к-серцевин під час дослідження уразливості СМ до дії різнорідних негативних впливів також присвячено чимало публікацій. Більшість із них намагаються дати відповідь на питання: як послідовними атаками на елементи (вузли та ребра) вже виділеної *k*-серцевини

зруйнувати її структуру, як найважливішої складової СМ [8, 9]. У деяких роботах стверджується що захист всієї мережі одночасно забезпечуватиме безпеку і її *k*-серцевини [10]. Однак, жодна велика складна система не може захистити усі свої елементи і організувати захист окремої складової значно простіше, ніж СМ загалом. Ми розглядаємо дещо іншу проблему: яким чином одночасна цілеспрямована атака на *k*-серцевину відобразиться на всій системі та до яких втрат призведе. Виявляється, що застосування найбільш вживаних методів виділення таких серцевин у структурі реальних мережевих систем [11] нерідко призводить до їх виродження у порожню множину. Тобто, СМ може налічувати чимало вузлів зі ступенем к та більше, але виділити її *k*-серцевину, наприклад, використовуючи алгоритм процесу обтинання, не вдається. У цій статті ми пропонуємо модифікований варіант цього методу та використовуємо його для побудови сценаріїв одночасних цілеспрямованих групових атак на систему та оцінювання наслідків отриманих уражень.

1. Складна мережа та її *k*-серцевина

Складна мережа зазвичай описується у вигляді графу $G=(V, E)$, у якому $V=\{v_n\}_{n=1}^{N}$ позначає множину вузлів, а $E=\{e_l\}_{l=1}^{L}$ – множину зв'язків (ребер), які поєднують вузли СМ, N та L – кількості цих вузлів та ребер відповідно. Структура мережі повністю описується матрицею суміжності $\mathbf{A}=\{a_{ij}\}_{i,j=1}^{N}$, елементи якої $a_{ij}=1$, якщо існує зв'язок між вузлами v_i та v_j (такі вузли називаються суміжними), і $a_{ij}=0$, $i, j=\overline{1,N}$, якщо такого зв'язку немає [12].

Під час дослідження уразливості СМ насамперед постає проблема ідентифікації тих її вузлів, які потребують першочергового захисту. Для визначення важливості вузлів у складній мережі використовуються так звані центральності різних типів. Серед них насамперед назвемо центральність за ступенем або ступінь $d(v_i)$ вузла v_i, який дорівнює кількості ребер, які поєднують даний вузол із суміжними вузлами, центральність за посередництвом, яка дорівнює відношенню кількості усіх найкоротших шляхів, які проходять через даний вузол, до кількості усіх найкоротших шляхів мережі, центральність за близькістю, тобто середньою відстанню від даного вузла до всіх інших вузлів СМ, власним значенням у матриці Лапласа мережі тощо [13]. Натепер введено більш ніж 20 видів таких центральностей, що вносить певну неоднозначність у визначення важливості вузла, оскільки їх значення загалом не є пропорційними одне одному [14]. У цій статті у якості показника важливості вузла у СМ ми застосовуватимемо його ступінь, оскільки саме він використовується для побудови *k*-серцевин мережі.

Особливістю реальних складних мереж є наявність величезної кількості вузлів (мільйони, мільярди і більше). Тому моделювання структури нашої галактики, яка налічує приблизно 100 мільярдів зірок, або головного мозку людини, який містить трильйони нейронів можливе лише на сучасних суперкомп'ютерах. Однак, у багатьох випадках дослідження СМ можна обмежити лише її частиною, наприклад, коли така мережа має фрактальну структуру. Практично у кожній країні світу існує залізнична транспортна система (ЗТС). У поєднанні вони утворюють загальну ЗТС світу. Але для

детального дослідження властивостей залізниці окремої країни, зовсім не обов'язково розглядати загальну ЗТС. Залізниці деяких країн (США, Китай, Індія), протяжність яких налічує сотні тисяч кілометрів, також доцільно поділяти на окремі регіональні складові. Аналогічно, для дослідження автотранспортної системи великого міста зовсім не обов'язково брати до уваги автотранспортну систему всієї країни чи її регіону. Такий підхід (фрагментація, поділ на складові) часто використовується під час вивчення транспортних мереж [15]-[17] та інших мережевих систем великої розмірності. Також для спрощення дослідження можна виділяти найважливіші за певною ознакою складові системи, наприклад, визначені у вступі їх *k*-серцевини. Опишемо деякі з підходів виділення *k*-серцевин складних мереж.

2. Виділення *k*-серцевини за допомогою процесу обтинання

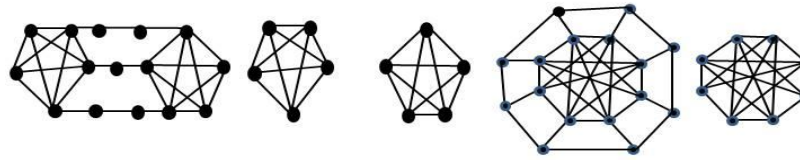
Одним із найбільш вживаних способів виділення *k*-серцевин є запропонований у [11] процес обтинання (pruning process – PP). Цей метод, який надалі називатимемо PP-алгоритмом, полягає у послідовному виконанні наступних кроків:

1) створюємо перелік вузлів мережі, ступінь яких є меншим ніж *k*;
2) видаляємо перший із вузлів переліку разом із усіма ребрами, які пов'язують його із суміжними вузлами;
3) зменшуємо на 1 ступінь усіх суміжних до видаленого вузлів;
4) оскільки ступінь частини вузлів мережі, що залишились, змінився, то корегуємо існуючий перелік вузлів, ступінь яких є меншим ніж *k*;
5) якщо перелік вузлів зі ступенем, меншим ніж *k*, є непорожнім, то переходимо до кроку 2; інакше закінчуємо виконання алгоритму.

PP-алгоритм можна виконувати поетапно, а саме:

1) формуємо перелік вузлів мережі зі ступенем, меншим ніж *k*;
2) видаляємо зі структури СМ вузли із створеного переліку разом із ребрами, які з них виходять;
3) якщо в структурі мережі не залишилось вузлів зі ступенем, меншим ніж *k*, то закінчуємо виконання алгоритму; інакше переходимо до кроку 1 (наступного етапу).

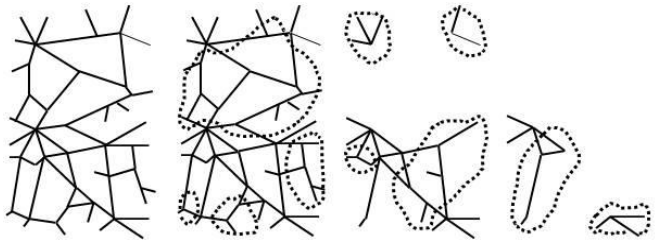
Вважається, що у результаті виконання PP-алгоритму у мережі залишаються лише вузли зі ступенем *k* та вище, тобто її *k* -серцевина. У багатьох випадках це твердження дійсно справджується. Приклади мереж (рис. 1а та 1в) та виділених за допомогою PP-алгоритму їх 4- (рис. 1б) та 5-серцевин (рис. 1г) навести достатньо просто. Однак, саме застосування описаного варіанту PP-алгоритму робить *k*-серцевини нестійкими до виділення структурами [18]. Дійсно, видалення будь-якого вузла однієї з 4-серцевин, зображених на рис. 1б та подальше застосування PP-алгоритму призводить до її виродження у порожню множину.



а) б) в) г)

Рис. 1. Результати виділення *k* -серцевини мережі за допомогою PP-алгоритму

Розглянемо приклад реальної спатіальної СМ, яка описує структуру залізничної транспортної системи західного регіону України та містить 365 вузлів. Виділимо за допомогою поетапного РР-алгоритму 4-серцевину цієї мережі. Рис. 2а містить схематичне зображення цієї ЗТС без відображення (для кращого візуального сприйняття) транзитних вузлів зі ступенем 2. Максимальний ступінь вузла цієї мережі дорівнює 7. Окрім того, вона містить один вузол зі ступенем 6, три вузли зі ступенем 5 та 7 вузлів зі ступенем 4.



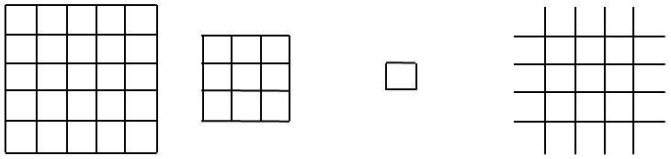
а) б) в) г)

Рис. 2. Застосування поетапного РР-алгоритму для виділення 4-серцевини ЗТС західного регіону України

На рис. 2б точковими лініями обмежені складові цієї мережі, ступінь вузлів яких не перевищує значення 3 (перший етап). Послідовно видаляємо вузли та ребра цих складових згідно РР-алгоритму. У результаті отримуємо відображену на рис.2в частину вихідної мережі, що залишилась, на якій точковими лініями виділені ті складові, що також містять вузли зі ступенем, меншим ніж 4. Застосовуємо РР-алгоритм для цієї мережі (другий етап) та отримуємо мережу, зображену на рис. 2г. Послідовно використовуючи описаний алгоритм до неї (третій та четвертий етапи), отримуємо порожню множину. Тобто, застосування РР-алгоритму для виділення 4-серцевини реальної мережі, яка містить 12 вузлів зі ступенями 4 і більше призводить до виродження цієї мережі у порожню множину. Легко переконатись, що до такого ж результату призводить використання цього алгоритму для виділення 5- та 6-серцевин.

Ще одним прикладом, для якого РР-алгоритм не спрацьовує, є обмежені регулярні мережі, усі вузли яких, окрім граничних, мають однаковий ступінь. Такі мережі достатньо часто зустрічаються у фізичному світі, живій природі та людському соціумі: кристалічні гратки металів і мінералів (хлориду натрію, алмазу, міді, графіту), бджолині соти та нейронні мережі мозку, енергетичні мережі Європи та США, мережі мобільного зв'язку, організаційні структури у війську, релігійних концесіях та дорожній інфраструктурі великих міст (Чикаго, Буено-Айрес, Пекін, Торонто) тощо. Такі мережі можуть налічувати велику кількість вузлів, але все одно є скінченними, тобто мають певну границю. Проілюструємо «непрацездатність» РР-алгоритму на найпростішому прикладі регулярної мережі. Візьмемо одиничний квадрат і побудуємо у ньому прямокутну сітку з кроком $h=1/N$. У результаті отримаємо мережу розмірністю $(N+1)^2$, кутові вузли якої мають ступінь 2, некутові вузли, що лежать на сторонах квадрата – ступінь 3, а внутрішні вузли, кількість яких дорівнює $(N+1)^2 - 4N$, – ступінь 4. Виконавши перший етап РР-алгоритму до зображеної на рис. 3а сіткової області (тут прийнято $N=5$) з метою виділення 4-

серцевини, отримаємо квадратну мережу розмірністю $(N-1)^2$, відображену на рис. 3б. Послідовно виконуючи (N/2+1) етап РР-алгоритму (у даному випадку лише 2 етапи, рис. 3в) отримаємо порожню множину. Таким чином, виникає парадокс: у структурі системи може бути чимало вузлів зі ступенем k і більше, але виділити її k-серцевину за допомогою РР-алгоритму ми не можемо.



а) б) в) г)

Рис. 3. Застосування РР-алгоритму для виділення 4-серцевини мережі з регулярною структурою

4. Модифікований РР-алгоритм

Для уникнення описаної у попередньому пункті можливості виродження к-серцевини у порожню множину використовуватимемо для її виділення модифікований процес обтинання або МРР-алгоритм. Для його опису використаємо поняття відкритого зв'язку, тобто ребра, яке виходить з одного вузла, але не є формально приєднаним до іншого вузла, оскільки такий вузол знаходиться поза межами підмережі, що розглядається [18]. Відкритий кінець ребра називатимемо граничною точкою мережі. Відкриті ребра зручно використовувати під час дослідження підмереж СМ багатьох типів, наприклад, фракталів мережі, окремих ділянок мозгу, територій з різними геофізичними та кліматичними особливостями, залізниць окремих країн, автотранспортної мережі мегаполісу тощо. Покажемо, що використання відкритих ребер також є зручним засобом під час виділення та відображення k-серцевин СМ. Під довжиною шляху між двома вузлами мережі, як звично, розумітимемо кількість ребер, які лежать на цьому шляху. Розглянемо МРР-алгоритм, який полягає у послідовному виконанні наступних кроків:

1) створюємо перелік вузлів мережі, ступінь яких $q \geq k$, у порядку зменшення значень цих ступенів; нумеруємо вузли створеного переліку у порядку $n = \overline{1, N^k}$, і приймаємо $n = 1$;
2) для вузла створеного переліку із номером n впорядковуємо ребра, які пов'язують його із суміжними вузлами або граничними точками мережі у порядку $m = \overline{1, d(v_n)}$ та приймаємо $m = 1$;
   2.1) починаючи з ребра із номером m шукаємо найкоротший шлях, який поєднує вузол v_n із вузлом мережі зі ступенем $q \geq k$ чи граничною точкою мережі;
   2.2) якщо довжина знайденого шляху є більшою 1, то замінюємо його ребром, а всі вузли зі ступенем $q < k$, які лежали на цьому шляху, разом із ребрами, які виходили з них, не належали цьому шляху та не поєднувались з вузлами зі ступенем $q \geq k$, видаляємо зі структури мережі;
   2.3) приймаємо $m = m + 1$; якщо $m \leq d(v_n)$, то переходимо до кроку 2.1, інакше переходимо до кроку 3;

3) приймаємо $n = n+1$; якщо $n \le N^k$, то переходимо до кроку 2, інакше – переходимо до кроку 4;
4) видаляємо зі структури мережі усі вузли зі ступенем $q < k$, із ребрами, які виходять з них і не поєднуються з вузлами зі ступенем $q \ge k$, та закінчуємо виконання алгоритму.

Згаданий на першому кроці МРР-алгоритму перелік вузлів формується на підставі значень їх ступенів. Для неорієнтованих мереж значення цих ступенів отримуються із матриці суміжності **A** за співвідношенням

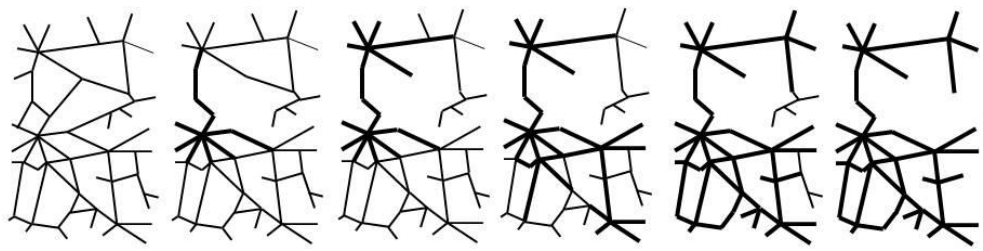
$$d(v_n) = \sum_{l=1}^{N} (a_{nl} + a_{ln}), \quad n = \overline{1, N}, \tag{1}$$

тобто дорівнюють сумі вхідних та вихідних зв'язків вузла. Очевидно, що якщо ми розглядаємо всю СМ, то граничні точки у ній відсутні, і пошук найкоротших шляхів до таких точок ми прибираємо із описаного вище алгоритму. Для пошуку найкоротшого шляху використовуємо модифікований алгоритм Дейкстри [19]. МРР-алгоритм виділення *k*-серцевини також можна виконувати поетапно для кожного заданого $k \le k_{\max}$, починаючи з найбільшого. Значення $k_{\max}$ отримуємо із співвідношення (1) за формулою:

$$k_{\max} = \max_{n=1,N} d(v_n).$$

Застосувавши МРР-алгоритм для виділення 4-серцевини регулярної мережі, зображеної на рис. 3а, отримаємо підмережу цієї мережі, відображену на рис. 3г. Використання МРР-алгоритму до мережі, яка міститься на рис. 1а, призведе до цієїж мережі за виключенням вузлів зі ступенем 2. Результати виділення 5-серцевини для мережі, відображеної на рис. 1в, отримані за допомогою РР- та МРР-алгоритмів, є тотожними.

На рис. 4а відображена мережа ЗТС західного регіону України. Рис. 4б – 4д містять результати послідовного застосування МРР-алгоритму на етапах виділення 7-, 6-, 5- та 4-серцевин цієї мережі відповідно. Потовщеними лініями позначені ребра, які входять до складу відповідної *k*-серцевини. Для збереження відповідності зображення до вихідної мережі ребра *k*-серцевин у деяких випадках мають вигляд ламаних ліній. На рис. 4е відображений остаточний результат роботи МРР-алгоритму.



а) б) в) г) д) е)

Рис. 4. Застосування МРР-алгоритму для поетапного виділення 4-серцевини ЗТС західного регіону України

4. Цілеспрямовані групові атаки на складні мережі

Особливістю цілеспрямованих атак на СМ є наявність «зловмисника», який такі атаки планує та здійснює, та цілі (або набору цілей), які він намагається знищити або критично пошкодити [20]. Водночас, цілеспрямована атака на «зловмисника» або джерело нецільового ураження може бути ефективним засобом активного захисту системи (нейтралізація терористичних та хакерських груп, застосування засобів боротьби із сільськогосподарськими шкідниками тощо). Зазвичай такі дії, спрямовані на упередження негативних впливів, є значно ефективнішими ніж застосування пасивних засобів захисту (вакцинація порівняно з карантином).

Групові атаки можуть бути одноразовими (напад Хамасу на Ізраїль 7 жовтня 2024р.), повторюваними, якщо ціль атаки не змінюється (18 ракетних ударів по Києву у травні 2024 р.) та послідовними, якщо ціль атаки змінюється (удари по енергетичній системі України протягом 2022-2025 рр.). Найбільш небезпечними є послідовні групові атаки, оскільки вони можуть призвести до загальносистемного ураження, наприклад, блекауту в країні. Під час розроблення стратегій захисту від одночасних групових атак, насамперед виникає проблема вибору групи, ураження якої завдасть атакованій стороні якнайбільшої шкоди [10, 20]. Така група може формуватись на підставі обраних за певною ознакою показників важливості вузлів МС. Саме цей принцип використовується під час розроблення сценаріїв послідовних поелементних атак на систему. Тоді група, яка формується із найважливіших за обраними показниками елементів МС, стає ціллю ураження. Група може формуватися на підставі ієрархії вкладеності [1]. У цьому випадку ціллю стає одна із найважливіших підсистем системи, наприклад, регіон країни із найбільшою кількістю населення або промислова галузь (військово-промисловий комплекс чи енергетичний сектор економіки і т. ін.). У цій статті для вибору групи вузлів, як цілі одночасної атаки, ми використовуватимемо *k*-серцевину СМ.

4.1. Сценарій цілеспрямованої атаки на *k*-серцевину складної мережі

Сценарій цілеспрямованої атаки на *k*-серцевину СМ доцільно розробляти враховуючи (чи передбачаючи) спроможність атакуючої сторони уразити певну кількість цілей g. Такий сценарій, у який доцільно вбудовувати MPP-алгоритм, полягає у послідовному виконанні наступних кроків:

1) обираємо максимальний для даної мережі ступінь вузла $k = k_{\max}$;
2) виділяємо за допомогою поетапного MPP-алгоритму *k*-серцевину СМ (або доповнюємо вже виділену $(k+1)$-серцевину);
3) якщо кількість вузлів виділеної к-серцевини є меншим значення g, то приймаємо $k = k-1$ та переходимо до кроку 2; інакше переходимо до наступного кроку;
4) моделюємо атаку на виділену *k*-серцевину мережі та завершуємо виконання сценарію.

Перевагою наведеного сценарію цілеспрямованої атаки із вбудованим MPP-алгоритмом є динамічне визначення підмереж СМ, які можуть бути одночасно атаковані із врахуванням спроможності атакуючої сторони уразити наперед визначену кількість цілей.

4.2. Оцінювання наслідків ураження *k*-серцевини складної мережі

Оскільки, як один із варіантів одночасної групової атаки, ми розглядаємо ураження її *k*-серцевини, то для оцінювання наслідків такої атаки використовуватимемо поняття ступеня цієї серцевини. А саме, кількість ребер, які поєднують вузли *k*-серцевини із зовнішніми по відношенню до неї вузлами (враховуючи відкриті ребра), по аналогії зі ступенем вузла називатимемо ступенем *k*-серцевини. Позначимо через C_k – сукупність вузлів *k*-серцевини (N^k – кількість елементів множини C_k). У разі успішної атаки на *k*-серцевину СМ будемо вважати усі елементи сукупності C_k безпосередньо ураженими.

Введемо поняття області сусідства к-серцевини СМ. Під $\mathcal{N}_1^k$-сусідством розумітимемо усі вузли мережі, суміжні до вузлів к-серцевини, які не входять до її складу. Очевидно, що кількість елементів $\mathcal{N}_1^k$-сусідства дорівнює ступеню відповідної *k*-серцевини. Саме ці вузли зазвичай вважаються опосередковано постраждалими елементами мережі. Слід враховувати, що максимізація кількості опосередковано постраждалих елементів системи також може бути метою атаки. $\mathcal{N}_i^k$-сусідством к-серцевини називатимемо сукупність вузлів СМ, суміжних до вузлів області $C_k \bigcup \mathcal{N}_1^k \bigcup \mathcal{N}_2^k \bigcup \ldots \bigcup \mathcal{N}_{i-1}^k$, які не входять до складу цієї області, i=2,3,… У випадку асортативних мереж [21] область $\mathcal{N}_1^k$-сусідства зазвичай достатньо точно визначає елементи СМ, які опосередковано тим або іншим чином постраждали унаслідок ураження її *k*-серцевини. У випадку дисасортативних мереж елементами, які опосередковано постраждали унаслідок ураження *k*-серцевини формально можна вважати вузли $\mathcal{N}_i^k$-сусідств, *i*=1,2,…, але очевидно, що результати такого оцінювання наслідків ураження може бути далеким від реальності.

Висновки. У статті проаналізовані недоліки найбільш вживаного для виділення *k*-серцевини мережі алгоритм процесу обтинання та запропоновано його модифікований варіант. На прикладах низки модельних та реальних мереж показано, що він не призводить до виродження *k*-серцевини у порожню множину. Процес виділення *k*-серцевини за допомогою МРР-алгоритму є значно стійкішим порівняно з РР-алгоритмом, оскільки під час його виконання не відбувається зменшення ступенів вузлів, значення яких є більшими або рівними *k*. Проаналізована проблема уразливості СМ до одночасних групових цілеспрямованих атак у яких у якості мети обрано *k*-серцевину мережі. Розроблено сценарій атаки на *k*-серцевину у якій враховано потенційні спроможності нападника. Запропоновано метод оцінювання наслідків ураження *k*-серцевини асортативної мережі на підставі поняття її області сусідства. Показано, що цей метод оцінювання є малопридатним у випадку дисасортативних мереж. Подальшими кроками наших досліджень є застосування потокових моделей та їх серцевин для визначення уразливості складних мережевих систем до дії різнорідних негативних впливів та оцінювання їх наслідків з метою якнайшвидшого відновлення системи та її повернення до нормальної життєдіяльності.

Література

[1] *Поліщук О., Яджак М.,* Моделі та методи комплексного дослідження складних мережевих систем та міжсистемних взаємодій. Львів: Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України, 2023.

[2] *Dorogovtsev S.N., Goltsev A.V., Mendes J.F.F.*, K-core organization of complex networks. Physical review letters, Vol. 96, No. 4, 2006, 040601. doi: 10.1103/PhysRevLett.96.040601.

[3] *Burleson-Lesser K.*, A Network Theoretical Approach to Real-World Problems: Application of the K-Core Algorithm to Various Systems. Dissertation of PhD Doctor of Philosophy, New York, USA: The City University of New York, 2018.

[4] *Tavares F.*, Illuminating the Gas Between Galaxies with Supercomputing. Available: https://www.nasa.gov/centers-and-facilities/ames/illuminating-the-gas-between-galaxies-with-supercomputing, Nov 20, 2019.

[5] *Svitlyk Y.*, Human Brain Project: Attempt to imitate the human brain. Available: https://root-nation.com/en/articles-en/tech-en/en-human-brain-project , Nov 5, 2023.

[6] *Kong X. et al*, *k*-core: Theories and applications. Physics Reports, Vol. 832, 2019, 1-32. doi: 10.1016/j.physrep.2019.10.004.

[7] *Mimar S.*, Learning Dynamical Processes from Structure in Complex Networks. Rochester: University of Rochester, 2022.

[8] *Hossain J., Soundarajan S., Sarıyüce A. E.*, Quantifying node-based core resilience. In: Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Cham: Springer Nature Switzerland, 2023, 259-276.

[9] *Li J., et al*, Large-Scale Social Network Privacy Protection Method for Protecting K-Core. International Journal of Network Security, Vol. 23, 2021, 612-622. doi: 10.1109/ACCESS.2019. 2933151.

[10] *Bellingerio M., Cassi D., Vincenzi S.*, Efficiency of attack strategies on complex model and real-world networks. Physica A: Statistical Mechanics and its Applications, Vol. 414, 2014, 174-180. doi: 10.1016/j.physa.2014.06.079.

[11] *Batagelj V., Zaversnik M.*, An O (m) algorithm for cores decomposition of networks. arXiv: cs/0310049, 2003.

[12] *Boccaletti S., et al*, Complex networks: Structure and dynamics. Physics reports, Vol. 424, No. 4, 2006, 175-308. doi: 10.1016/j.physrep.2005.10.009.

[13] *Wan Z., et al*, A survey on centrality metrics and their network resilience analysis. IEEE Access, Vol. 9, 2021, 104773-104819. doi: 10.1109/ACCESS.2021.3094196.

[14] *Ugurlu O.*, Comparative analysis of centrality measures for identifying critical nodes in complex networks. Journal of Computational Science, Vol. 62, 2022, 101738. doi: 0.1016/j.jocs.2022. 101738.

[15] *Polishchuk O.*, Vulnerability of Complex Network Structures and Systems. Cybernetics and Systems Analysis, Vol. 56, No. 2, 2020, 312 – 321. doi: 10.1007/s10559-020-00247-4.

[16] *Polishchuk D., Polishchuk O., Yadzhak M.*, Complex evaluation of hierarchically-network systems Automatic Control and Information Sciences, Vol. 2, No. 2, 2014, 32-44.

[17] *Tokhirov R., Rahmonov N.*, Technologies of using local networks efficiently. Asian Journal Of Multidimensional Research, Vol. 10, No. 6, 2021, 250-254. doi: 10.5958/2278-4853.2021.00535.8.

[18] *Zhou B., et al*, Attacking the core structure of complex network. IEEE Transactions on Computational Social Systems, Vol. 10, No. 4, 2022, 1428-1442. doi: 10.1109/TCSS.2022.3188522.

[19] *Ahuja R. K., et al*, Faster algorithms for the shortest path problem. Journal of the ACM, Vol. 37, No. 2, 1990, 213-223. doi: 10.1145/77600.77615.

[20] *Nguyen Q., et al*, Conditional attack strategy for real-world complex networks. Physica A: Statistical Mechanics and its Applications, Vol. 530, 2019, 12156. doi: 10.1016/j.physa.2019.121561.

[21] *Noldus R., Van Mieghem P.*, Assortativity in complex networks. Journal of Complex Networks, Vol. 3, No. 4, 2015, 507-542. doi: 10.1093/comnet/cnv005.

Modified pruning process algorithm for k-cores decomposition in a complex networks

Dmytro Polishchuk, Olexandr Polishchuk

The most commonly used algorithm for extracting k-cores of complex networks (CNs) is analyzed. The main drawback of this algorithm is identified, which is the possibility of degenerating the k-core into an empty set even if this network contains a sufficiently large number of nodes with a degree not less than k. To eliminate this drawback, a modified pruning process algorithm is proposed and its effectiveness for extracting k-cores is shown on the examples of a number of model and real-world complex networks. k-cores are formed as groups of the most important CN elements, which can become the target of simultaneous targeted attack on the network, and a scenario of such attack is formed, which takes into account the potential capabilities of intruder. A method for evaluation the consequences of successful attack on k-core is proposed, which is based on the concept of its neighborhood domain.

Отримано 20 05 2025 р.