

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

DOI: [10.18372/2225-5036.26.14668](https://doi.org/10.18372/2225-5036.26.14668)

МОДЕЛЬ ПОШУКУ СПІВТОВАРИСТВ В СОЦІАЛЬНІЙ МЕРЕЖІ

Володимир Ахрамович¹, Сергій Лазаренко²,
Ганна Мартинюк², Юрій Баланюк²

¹Державного університету телекомунікацій, Україна

²Національний авіаційний університет, Україна



АХРАМОВИЧ Володимир Миколайович, к.т.н., доцент

Рік та місце народження: 1951 рік, м. Київ, Україна.

Освіта: Київський політехнічний інститут (з 2000 року - Національний технічний університет ім. Сікорського), 1980 рік.

Посада: доцент кафедри інформаційної та кібернетичної безпеки з 2016 року.

Наукові інтереси: інформаційна та кібернетична безпека.

Публікації: більше 150 наукових публікацій, серед яких, підручники, навчальні посібники, наукові статті та патенти на винаходи.

E-mail: 12z@ukr.net.

Orcid ID: 0000-0002-6174-5300.



ЛАЗАРЕНКО Сергій Володимирович, д.т.н., доцент

Рік та місце народження: 1971 рік, м. Київ, Україна.

Освіта: Київський військовий інститут управління та зв'язку, 1994 рік; Національна юридична академія ім. Я. Мудрого, 2009 рік.

Посада: завідувач кафедри засобів захисту інформації з 2018 року.

Наукові інтереси: системи технічного захисту, цивільний захист, інформаційна/кібербезпека.

Публікації: більше 68 наукових публікацій, серед яких монографії, навчальний посібник, наукові статті та патент на винахід.

E-mail: zzi.lazarenko@nau.edu.ua.

Orcid ID: 0000-0003-3529-4806.



МАРТИНЮК Ганна Вадимівна, к.т.н.

Рік та місце народження: 1989 рік, м. Херсон, Україна.

Освіта: Національний авіаційний університет, 20011 рік.

Посада: доцент кафедри засобів захисту інформації з 2019 року.

Наукові інтереси: формаційне забезпечення шумометрії; статистичні моделі інформаційних сигналів; статистичні методи вимірювання характеристик випадкових процесів і полів; методи математичного та комп'ютерного моделювання сигналів і даних вимірювань.

Публікації: більше 40 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях та патенти.

E-mail: ganna.martyniuk@gmail.com.

Orcid ID: 0000-0003-4234-025X.



БАЛАНЮК Юрій Вікторович, к.т.н.

Рік та місце народження: 1985 рік, м. Львів, Україна.

Освіта: Національний університет «Львівська політехніка», 20007 рік.

Посада: доцент кафедри засобів захисту інформації з 2018 року.

Наукові інтереси: інформаційна та кібербезпека.

Публікації: більше 30 наукових публікацій, серед яких наукові статті, матеріали та тези доповідей на конференціях та патенти.

E-mail: kzzi@nau.edu.ua.

Orcid ID: 0000-0003-3036-5804.

Анотація. З метою забезпечення безперервного функціонування соціальної мережі з великою кількістю абонентів її доцільно поділити на підмережі. Поділ на підмережі забезпечить якісний контроль трафіку та інших параметрів, у тому числі параметрів безпеки. Перша причина розбиття мережі на підмережі полягає в тому, щоб не отримати величезний broadcast домен. Другою важливою причиною поділу мережі на підмережі є забезпечення певного рівня безпеки. Третя причина – виявлення співтовариств у мережі. Визначено необхідність створення моделі, в якій граф генерується випадковим чином із заданими параметрами для внутрішніх і зовнішніх зв'язків між вершинами, а спільноти покладаються непересічними. Запропоновано метод виділення структури спільнот на основі методу максимальної правдоподібності, і на його основі описано чисельний алгоритм випадкового пошуку. Графи, що представляють реальні соціальні та комунікаційні мережі, швидко змінюються, при цьому ефективним інструментом їх вивчення являються випадкові графи. Важливим завданням є виявлення структури спільнот в мережах. В умовах великої розмірності мереж особливо актуальними є наближені методи, які дозволяють за обмежений час знаходити рішення, близьке до оптимального. Для вирішення такої проблеми пропонується створення моделі виділення структури спільнот на основі методу максимальної правдоподібності, і на його основі опис чисельного алгоритму випадкового пошуку таких спільнот. Досліджено поведінку цільової функції.

Ключові слова: мережа, безпека, граф, структура, співтовариства, моделювання, алгоритм, вершини.

Вступ

З метою забезпечення безперервного функціонування соціальної мережі з великою кількістю абонентів доцільно здійснити її поділ (розділення) на підмережі. Поділ великої мережі на підмережі здійснюється з метою контролю трафіку та інших параметрів, у тому числі параметрів безпеки. Перша причина розбиття мережі на підмережі полягає в тому, щоб не отримати величезний broadcast домен [1]. Наприклад, за допомогою широкомовних запитів працює протокол ARP, операційна система Windows постійно розсилає запити в мережу, щоб виявити інші комп'ютери [3]. Якщо ми підключимо в одну мережу велику кількість пристроїв, тоді в мережі з'являться так звані колізії, а саме – відбудеться накладання інформації від різних комп'ютерів. У зв'язку з такими колізіями буде порушена працездатність мережі, в тому числі, тому що ПЕОМ будуть зайняті одержанням великої кількості широкомовних пакетів [2]. Якщо розбити таку мережу, наприклад на 256 підмереж кожна з яких буде мати по 254 хости, то ми отримаємо 256 окремих невеликих broadcast доменів, у кожному з яких діє порівняно невелика кількість джерел широкомовного трафіку. Такі мережі, як показує практика, працюють достатньо надійно. Хост (від англ. host - «господар, який приймає гостей») – будь-який пристрій, що надає послуги формату «клієнт-сервер» в режимі сервера з яким-небудь інтерфейсом та який унікально визначений на вказаних інтерфейсах. У більш окремому випадку під хостом можуть розуміти будь-який комп'ютер, сервер, підключений до локальної або глобальної мережі.

Насправді, обсяг широкомовного трафіку є основним обмежувачем, що не дозволяє створювати до-

статньо великі мережі. За умовною шкалою, опираючись на практику роботи мереж [3], мережа на 254 хоста (254/ 24) працює стабільно, на 510 (510/ 24) - сурдинь, та залежить від додатків. Існують мережі з множинним доступом (NBMA мережі).

Другою важливою причиною поділу мережі на підмережі є забезпечення певного рівня безпеки [4]. У межах локальної мережі є можливості забезпечення контролю за трафіком. Наприклад, можливо контролювати на комутаторах MAC адреси, налаштувати централізовану фільтрацію пакетів, захищати ПЕОМ за рахунок налаштування мережевого екрану. Але, найкраще це робити централізовано при переході трафіку з однієї мережі в іншу. Одним із елементів забезпечення безпеки підмережі є налаштування Firewall - мережевого екрану (апаратного, програмного або апаратно-програмного). Інша поширена назва мережевого екрану – фаєрвол, від транслітерації англійського терміну firewall. Іноді мережевий екран називають ще брандмауером (нім. brandmauer) - це німецький еквівалент слова firewall. Основне завдання мережевого екрану - не пропускати (фільтрувати) пакети, що не підходять під критерії, визначені в конфігурації мережевого екрану.

З точки зору безпеки небажано підключати до мережі одночасно, наприклад, камери відеоспостереження, робочі місця бухгалтерії, сервера організації, комп'ютерів програмістів та менеджерів. Абсолютно логічним кроком є розбиття мережі на підмережі, щоб у кожній мережі були пристрої певного типу. Тоді у нас з'явиться можливість заборонити доступ, наприклад програмістів до робочих місць бухгалтерії, всім – до камер відеоспостереження тощо. При

цьому, можливо надати права доступу до корпоративних серверів відповідним користувачам та адміністраторам мережі.

Постановка проблеми

Потреба в соціалізації є фундаментальною для кожної людини. Групи спілкування складаються на основі спільних інтересів, професії, вірувань, хобі, політичних уподобань тощо. До появи глобальної мережі передачі даних «Інтернет» розвиток таких груп стримував географічний фактор, але зараз наше фізичне місце розташування практично не має значення. Коли спільнота існує лише віртуально, її чисельність (кількість її користувачів) може збільшуватися практично необмежено, а самі учасники - перебувати в різних частинах світу.

Інтернет-спільноти з'явилися ще на зорі розвитку глобальної мережі. З тих пір їх форми багаторазово змінювалися. Спочатку це були іміджборди, чати і форуми, їм на заміну прийшли блоги. Потім настав «зоряний час» для соціальних мереж: у 2003 році був запущений LinkedIn, в 2004 - Facebook, в 2006 - Twitter, в 2011 - Google+.

Сьогодні саме ці соціальні мережі є лідерами за кількістю спільнот. Інтернет-форуми продовжують існувати, проте вже не користуються колишньою популярністю.

У даній статті, на основі вищезазначеного, авторами пропонується розробка моделі пошуку співтовариств соціальної мережі на основі методу максимальної правдоподібності.

Математична модель

Максимізуючи найбільш ймовірну структуру розбиття мережі на співтовариства, отримуємо таке розбиття, яке відповідає реальним даним [9, 10, 12]. З цією метою розроблено математичну модель розбиття соціальної мережі на співтовариства на основі методу максимальної правдоподібності.

Розглянемо мережу $G = (N, E)$, в якій безліч вершин має вигляд $N = \{1, 2, \dots, n\}$. Так $m = m(E)$ - число ребер в мережі, $E(i, j) = 1$, якщо між вершинами i та j є зв'язок, і $E(i, j) = 0$, якщо немає. Назвемо спільнотою S непорожню підмножину вершин мережі, а розбиттям $\Pi(N)$ - сукупність непересічних спільнот, об'єднання яких становить безліч N : $\Pi(N) = \{S_1, \dots, S_K\}$, де $U_{k=1}^K S_k = N$. Припустимо, що справжнє розбиття мережі $\Pi = \{S_1, \dots, S_K\}$. Хай змінні $n_k = n(S_k)$ і $m_k = m(S_k)$ позначають число вершин і ребер в співтоваристві $n = \sum_{k=1}^K n_k$ і $m = \sum_{k=1}^K m_k \leq m$, де n - кількість вершин в мережі, m - кількість ребер.

Дамо початкове поняття графа. Граф - абстрактний математичний об'єкт, який представляє собою безліч вершин графа і набір ребер, тобто з'єднань між парами вершин. Наприклад, за безліч вершин можливо взяти безліч аеропортів, що обслуговуються деякою авіакомпанією, а за безліч ребер взяти регулярні рейси цієї авіакомпанії між аеропортами.

Для різних областей застосування види графів можуть відрізнятися спрямованістю, обмеженнями на

кількість зв'язків і додатковими даними про вершини або ребра. Багато структур, які мають практичний інтерес в математиці та інформатиці, можуть бути представлені графами.

Видів графів багато, пропонується розглянути ті, що використовуються частіше для обрахунку параметрів мереж.

Види графів можуть визначатися загальними принципами їх побудови (такі як двочастковий граф і граф Ейлера), а можуть залежати від тих чи інших властивостей вершин або ребер (наприклад, орієнтований і неорієнтований граф, звичайний граф).

Орієнтовані і неорієнтовані графи

Графи, в яких всі ребра є ланками (порядок двох кінців ребер графа не суттєвий), називаються неорієнтованими.

Графи, в яких всі ребра є дугами (порядок двох кінців ребра графа істотний), називаються орієнтованими графами або орграфом.

Неорієнтований граф може бути представлений у вигляді орієнтованого графа, якщо кожне його ребро замінити на дві дуги, що мають протилежні напрямки.

Якщо граф містить петлі, то цю обставину спеціально обумовлюють, додаючи до основної характеристики графа слова "з петлями", наприклад, "орграф з петлями". Якщо граф не містить петель, то додають слова "без петель".

Змішаним називають граф, в якому є ребра хоча б двох із згаданих трьох різновидів (ланки, дуги, петлі).

Граф, що складається тільки з вершин, називається порожнім.

Мультиграфом називається граф, в якому пари вершин можуть бути з'єднані більш ніж одним ребром, тобто який містить кратні ребра, але не містить петель.

Граф без дуг (тобто неорієнтовний), без петель і кратних ребер називається звичайним.

Простий граф - граф, в якому немає кратних ребер і петель.

Розглянемо побудову мережі за структурою простого графу, представлену на рисунку 1.

Розглянемо співтовариство $S_k \in \Pi$. Імовірність реалізації m_k зв'язків серед n_k вершин в співтоваристві S_k дорівнює:

$$P_{in}^{m_k} (1 - p_{in})^{\frac{n_k(n_k-1)}{2} - m_k} \quad (1)$$

У кожній вершині i зі співтовариства S_k може бути в цілому $n - n_k$ зв'язків з вершинами з інших спільнот, а в реальності вона має $\sum_{j \in S_k} E(i, j)$ зв'язків з вершинами з інших спільнот. Імовірність реалізації мережі із заданою структурою дорівнює:

$$L_n = \prod_{k=1}^K P_{in}^{m_k} (1 - p_{in})^{\frac{n_k(n_k-1)}{2} - m_k} \prod_{i \in S_k} P_{out}^{1/2(\sum_{j \in S_k} E(i, j))} \times (1 - p_{out})^{1/2(n - n_k = \sum_{j \in S_k} E(i, j))} \quad (2)$$

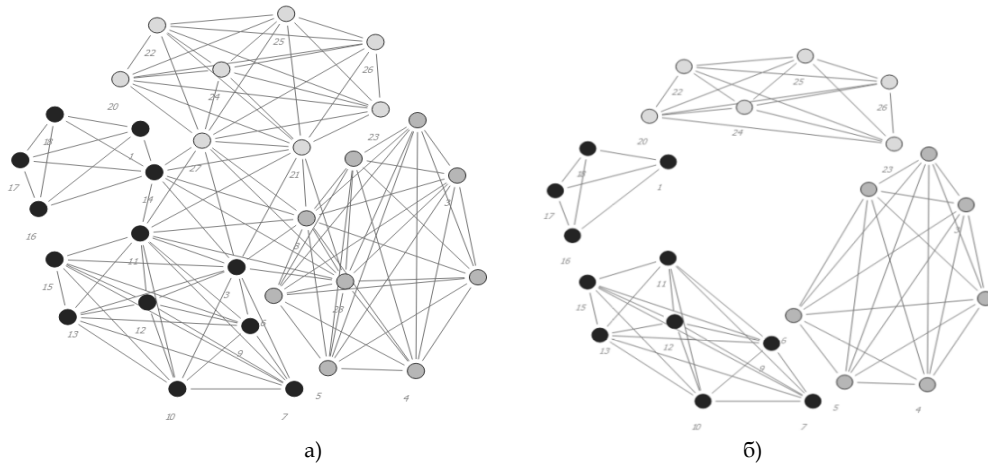


Рис. 1. а) загальна структура мережі; б) виділені з мережі співтовариства.

Беручи логарифм від функції правдоподібності L_n (1) і спрощуючи його, отримуємо вираз:

$$l_n = \log L_n = \sum_{k=1}^K (m_k \log p_{in} + \sum_{k=1}^K (\frac{n_k(n_k-1)}{2} - m_k) \log(1-p_{in}) + (m - \sum_{k=1}^K m_k) \log p_{out} + (\frac{1}{2} \sum_{k=1}^K n_k(n-n_k) - (m - \sum_{k=1}^K m_k)) \log(1-p_{out})). \quad (3)$$

Розбиття, для якого функція L_n досягає максимуму, назвемо оптимальним. Відмітимо, що все ще залишається невизначеність у виборі ймовірностей p_{in} і p_{out} . Функція $L_n = l_n(p_{in}, p_{out})$ залежить від аргументів p_{in}, p_{out} , де p_{in} - ймовірність виникнення зв'язку між будь-якими двома вершинами всередині спільноти, а p_{out} - ймовірність виникнення зв'язку між двома вершинами з різних спільнот. Для фіксованого розбиття L_n функція $L_n(p_{in}, p_{out})$ досягає максимуму за умов:

$$p_{in} = \frac{2 \sum_{k=1}^K m_k}{\sum_{k=1}^K n_k^2 - n}, p_{out} = \frac{2(m - \sum_{k=1}^K m_k)}{n^2 - \sum_{k=1}^K n_k^2}. \quad (4)$$

Підставивши вираз (4) в (3), отримуємо вираз який залежить тільки від структури мережі. Наведені значення параметрів максимізують і функцію правдоподібності (2).

Представимо функцію (3) у вигляді:

$$l_n = \sum_{k=1}^K m_k \log \frac{p_{in}(1-p_{out})}{p_{out}(1-p_{in})} - \frac{1}{2} \sum_{k=1}^K n_k^2 \log \frac{1-p_{out}}{1-p_{in}} + R, \quad (5)$$

де вираз: $R = -\frac{n}{2} \log(1-p_{in}) + m \log p_{out} + (\frac{1}{2} n^2 - m) \log(1-p_{out})$ залежить від введених параметрів мережі, але не залежить від конкретного розбиття. Доцільно представити вираз (5) у наступному вигляді:

$$l_n = \log \frac{p_{in}(1-p_{out})}{p_{out}(1-p_{in})} (\sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \frac{\log \frac{1-p_{out}}{1-p_{in}}}{\log \frac{p_{in}(1-p_{out})}{p_{out}(1-p_{in})}}) + R. \quad (6)$$

Якщо позначити:

$$\alpha = \frac{\log \frac{1-p_{out}}{1-p_{in}}}{\log \frac{p_{in}(1-p_{out})}{p_{out}(1-p_{in})}} = \frac{\log \frac{1-p_{out}}{1-p_{in}}}{\log \frac{p_{in}}{p_{out}} + \log \frac{1-p_{out}}{1-p_{in}}}, \quad (7)$$

тоді метод максимальної правдоподібності зведеться до задачі максимізації цільової функції:

$$P(\Pi) = \sum_{k=1}^K m_k - \frac{1}{2} \sum_{k=1}^K n_k^2 \alpha. \quad (8)$$

Відзначимо, що ця функція в гедонічній грі, пов'язана з графом. Завдання знаходження рівноваги Неша [5], у даному випадку еквівалентне задачі знаходження максимуму цільової функції. Аналогічним чином, у випадку графа з парними ребрами, метод максимальної правдоподібності зводиться до задачі максимізації цільової функції:

$$P(\Pi) = \sum_{k=1}^K m_k - \frac{M}{2} \sum_{k=1}^K n_k^2 \alpha. \quad (9)$$

Параметр α використовується для алгоритму розбиття мережі. Так, в [5, 11] розглянуті два граничних випадки $\alpha \rightarrow 0$ і $\alpha \rightarrow 1$ та доведено, що в першому випадку максимум цільової функції досягається при розбитті графа в ігровій постановці відповідній гранд-коаліції $\Pi_N = \{N\}$, а в другому - виявленні в графі співтовариств.

Для знаходження максимуму цільової функції можливо застосувати моделювання випадкової конфігурації Π з розподілом Больцмана (Гіббса):

$$p(\Pi) = \frac{\exp(\beta P(\Pi))}{\sum_{v \in \Pi} \exp(\beta P(\Pi))}. \quad (10)$$

При цьому, коефіцієнт β використовується в ході випадкового пошуку:

$$P_{\Pi \rightarrow \Pi'} = \frac{1}{n} \begin{cases} \frac{\exp(\beta P(\Pi))}{\sum_{s \in \Sigma} \exp(\beta P(\Pi_{i \rightarrow s}))}, & \text{якщо } \Pi' = \Pi, \\ \frac{\exp(\beta P(\Pi'))}{\sum_{s \in \Sigma} \exp(\beta P(\Pi_{i \rightarrow s}))}, & \text{якщо } \Pi' = \Pi_{i \rightarrow s}, \\ 0, & \text{інакше.} \end{cases} \quad (11)$$

Позначимо Σ безліч міток спільнот в мережі, $\Pi_i \rightarrow \sigma$ - розбиття, отримане з початкового розбиття Π передачею вершини i в співтовариство σ . Алгоритм пошуку максимуму цільової функції полягає в наступному. Визначимо число спільнот $K = K_0$ і зробимо деяке розбиття Π_0 в якості початкового. Для кожної вершини $i \in N$ випадковим чином виберемо співтовариство $\sigma \in \{1, \dots, K\}$ і переведемо в нове співтовариство, згідно з розподілом ймовірностей.

Під ітерацією алгоритму будемо розуміти n таких оновлень вершин. Відомо, що випадкове блукання, описане імовірнісним розподілом (11), за тривалий час призведе систему в стійку конфігурацію [5, 6]. При цьому динаміка збіжності алгоритму залежить від параметру β .

Наведемо результати чисельних експериментів з виділення співтовариств в мережі за допомогою запропонованого алгоритму. Алгоритм був програмно реалізований в системі MathCad 13. Чисельні експерименти проводилися на трьох графах, для кож-

ного з яких відома «справжня» структура співтовариств. У кожному разі було проведено моделювання випадкового блукання по графу, який підкоряється розподілу (10) методом Монте-Карло для знаходження наближеного рішення - глобального максимуму цільової функції (9). Інтервал зміни параметра α був обраний таким чином, щоб включити максимальні значення критеріїв якості знаходження співтовариств, яких вдалося досягти, а подальше зменшення кроку зміни параметру не приводило б до поліпшення результатів.

Приклад дослідження графа

Граф G_d містить 62 вершини і 159 ребер. Зробимо припущення, що вершини всередині одного і того ж співтовариства в розбитті Π^* спілкуються один з одним частіше, ніж вершини з різних спільнот.

Було виконано моделювання випадкового блукання по графу методом Монте-Карло для знаходження наближеного рішення - глобального максимуму цільової функції (8) (рис. 2, 3).

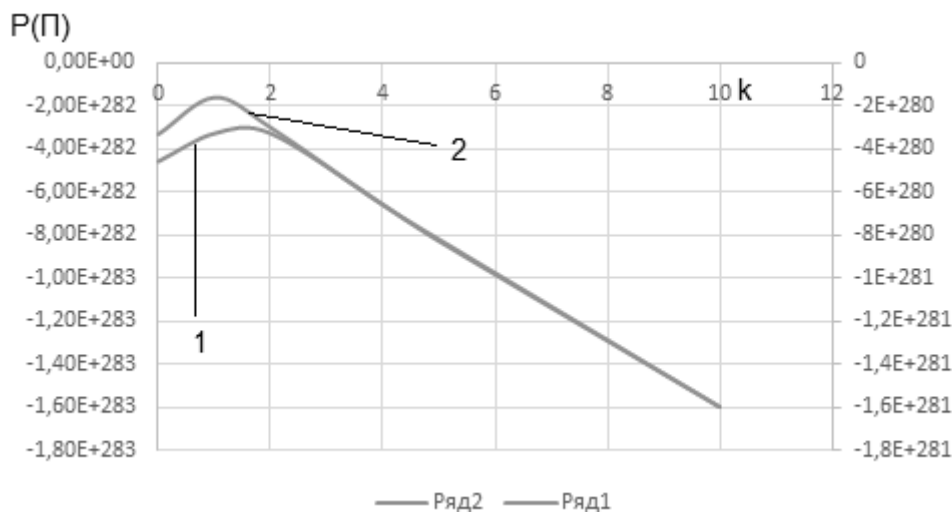


Рис. 2. Залежність функції $P(\Pi)$ від k ;

крива 1 $m_k = (100, 1000, 16000)$, $n_k = (200, 200 \dots 6200)$, $\alpha = (0,0,1, 1)$, $k = (0,1, 10)$ шкала ординат зліва;
 крива 2 $m_k = (1, 10, 160)$, $n_k = (2, 4 \dots 62)$, $\alpha = (0,0,1, 1)$, $k = (0,1, 10)$ шкала ординат праворуч.

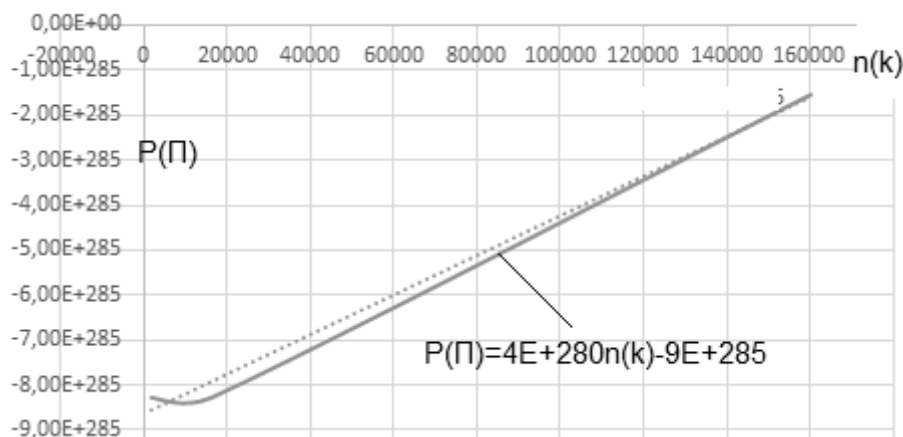


Рис. 3. Залежність цільової функції від $n(k)$

Висновки

Графи, що представляють реальні соціальні та комунікаційні мережі, швидко змінюються, при цьому ефективним інструментом їх вивчення є випад-

кові графи. Важливим завданням є виділення структури спільнот в мережах. В умовах великої розмірності мереж особливо актуальні наближені методи, які дозволяють за обмежений час знаходити рішення, на-

ближене до оптимального. У даній роботі описана математична модель, в якій граф генерується випадковим чином із заданими параметрами для внутрішніх і зовнішніх зв'язків між вершинами, а спільноти покладаються непересічними. Запропоновано метод виділення структури спільнот на основі методу максимальної правдоподібності, і на його основі описаний чисельний алгоритм випадкового пошуку з використанням розподілу Больцмана-Гіббса.

Приведені результати чисельних розрахунків для одного прикладу реальної мережі. Розрахунки для реальних мереж малої розмірності дозволили прийти до висновків про ефективність запропонованого алгоритму при виборі відповідних значень його параметрів, які залежать від структури мережі. Параметр α заданий аналітичним виразом (6), який залежить від механізмів (соціальна мотивація користувачів, адміністраторів мереж, адміністрації закладів та установ, програмне та технічне забезпечення тощо), що лежать в основі формування мережі.

Параметр β використовується в ході випадкового пошуку і визначає амплітуду коливань цільової функції. Загальна кількість ітерацій алгоритму також є параметром, який залежить від бажаного балансу між швидкістю і точністю пошуку. При аналізі мереж великої розмірності можливе адаптивне налагодження значень параметрів алгоритму на основі інформації, отриманої на попередніх етапах. При цьому, початкові оцінки параметрів можуть бути отримані на основі апріорних уявлень про структуру конкретної мережі. У даний час науковою проблемою являється розробка математичної моделі, яка описує структуру пересічних співтовариств в графі. Така структура співтовариств властива для сучасних складних мереж великої розмірності. Крім того, ці мережі часто розвиваються динамічно (наприклад, представляючи собою мережу рухомих об'єктів, забезпечених датчиками), що задає ще один напрямок подальших досліджень. У разі динамічної мережі математична модель повинна дозволити виділити ключові групи вершин, динаміка яких задає зміни іншої частини мережі.

УДК 004.056:004.738.5(045)

Ахрамович В.Н., Лазаренко С.В., Мартинюк А.В., Баланюк Ю.В. Модель поиска сообществ в социальной сети

Аннотация. С целью обеспечения бесперебойного функционирования социальной сети с большим количеством абонентов ее целесообразно разделить на подсети. Разделение на подсети обеспечит качественный контроль трафика и других параметров, в том числе параметров безопасности. Первая причина разделения сети на подсети состоит в том, чтобы не получить огромный broadcast домен. Второй важной причиной разделения сети на подсети является обеспечение определенного уровня безопасности. Третья причина - выявление сообществ в сети. Определена необходимость создания модели, в которой граф генерируется случайным образом с заданными параметрами для внутренних и внешних связей между вершинами, а сообщества полагаются незаурядными. Предложен метод выделения структуры сообществ на основе метода максимального правдоподобия, и на его основе описан численный алгоритм случайного поиска. Графы, представляющие реальные социальные и коммуникационные сети, быстро изменяются, при этом эффективным инструментом их изучения являются случайные графы. Важной задачей является выявление структуры сообществ в сетях. В условиях большой размерности сетей особенно актуальными являются приближенные методы, которые позволяют за ограниченное время находить решение, близкое к оптимальному. Для решения такой проблемы предлагается создание модели выделения структуры сообществ на основе метода максимального правдоподобия, и на его основе описан численный алгоритм случайного поиска. Предложена модель разбиения социальной сети на сообщества на основе метода максимального правдоподобия, и на ее основе разработан численный алгоритм случайного поиска. Исследовано поведение целевой функции.

Ключевые слова: сеть, безопасность, граф, структура, сообщества, моделирование, алгоритм, вершины.

ЛІТЕРАТУРА

- [1] В. Ахрамович, "Идентификация и аутентификация, керування доступом", *Сучасний захист інформації*, К.:ДУТ, №4, С. 47-51, 2016.
- [2] В. Ахрамович, В. Чегринець, "Уразливості та способи захисту бездротових мереж. Тенденції розвитку конвергентних мереж: рішення пост - NGN, 4G и 5G", *II Міжнародна науково-практична конференція, 17-18 листопада 2016 року: тези доп.*, К., С. 163-166, 2016.
- [3] В. Ахрамович, В. Чегринець, *Інформаційна безпека [практикум]*, К.: ДУТ, 2017, 396 с.
- [4] В. Чегринець, В. Ахрамович, Н. Руденко, "Хмарні технології та можливості використання в комп'ютерних телекомунікаційних системах", *Наукові записки Українського науково-дослідного інституту зв'язку*, №2 (42), С. 121-129, 2016.
- [5] K. Avrachenkov, A. Kondratev, V. Mazalov, "Cooperative Game Theory approaches for network partitioning", *Computing and Combinatorics. Eds. by Y. Cao, J. Chen. COCOON, 2017, LNCS, 2017, vol. 10392, pp. 591-603.*
- [6] J. Copic, M. Jackson, A. Kirman, "Identifying community structures from network data via maximum likelihood methods", *The B. E. Journal of Theoretical Economics*, vol. 9, iss. 1, pp. 1935-1704, 2009.
- [7] M. Jackson, *Social and economic networks. Princeton*, Princeton University Press, 2010, 520 p.
- [8] R. Kaur, S. Singh, "A survey of data mining and social network analysis based anomaly detection techniques", *Egypt Inf. Journal*, vol. 17(2), pp. 199-216, 2016.
- [9] M. Newman, M. Girvan, "Finding and evaluating community structure in networks", *Physical Review E*, vol. 69(2), pp. 26-53, 2004.
- [10] M. Meila, J. Shi, "A Random Walks View of spectral segmentation", *Proceedings of AISTATS*, pp. 1-6, 2001.
- [11] R. Myerson, "Graphs and cooperation in games", *Math. Oper. Res.*, vol. 2, pp. 225-229, 1977.

Akhramovych V., Lazarenko S., Martyniuk H., Balanyuk Y. Social network communities' search model

Abstract. In order to ensure the smooth functioning of a social network with a large number of subscribers, it is advisable to divide it into subnets. Division into subnets will provide high-quality control of traffic and other parameters, including security parameters. The first reason for dividing the network into subnets is not to get a huge broadcast domain. The second important reason for dividing the network into subnets is to provide a certain level of security. The third reason is identifying online communities. The necessity of creating a model is determined. In this model graph is randomly generated with specified parameters for internal and external relationships between vertices, and communities are considered extraordinary. A method for isolating the structure of communities based on the maximum likelihood method is proposed, and a numerical random search algorithm is described on its basis. Graphs which representing real social and communication networks are changed rapidly. Moreover, random graphs are an effective tool for studying these networks. An important task is to identify the structure of communities in networks. In conditions of large dimensionality of networks, approximate methods are especially relevant. That allow finding a solution close to the optimal for a limited time. To solve this problem, it is proposed to create a model for distinguishing the structure of communities based on the maximum likelihood method. And a description of a numerical random search algorithm based on created model. This paper describes a mathematical model in which a graph is randomly generated with specified parameters for internal and external relationships between vertices, and communities are considered extraordinary. A method for isolating the structure of communities based on the maximum likelihood method is proposed, and a numerical random search algorithm using the Boltzmann-Gibbs distribution is described on its basis. The behavior of the objective function is investigated.

Keywords: network, security, graph, structure, communities, modeling, algorithm, vertices.

Ахрамович Володимир Миколайович, к.т.н., доцент, доцент кафедри Систем інформаційного та кібернетичного захисту Державного університету телекомунікацій.

Ахрамович Владимир Николаевич, к.т.н., доцент, доцент кафедри Систем информационной и кибернетической защиты Государственного университета телекоммуникаций.

Akhramovych Volodymyr, Ph.D., associate professor of the Department of Information and Cyber Security Systems, State University of Telecommunications.

Лазаренко Сергій Володимирович, доктор технічних наук, доцент, завідувач кафедри засобів захисту інформації Національного авіаційного університету.

Лазаренко Сергей Владимирович, доктор технических наук, доцент, заведующий кафедрой средств защиты информации Национального авиационного университета.

Lazarenko Serhii, Doctor of Science, associate professor, Head of Information Security Department of National Aviation University.

Мартинюк Ганна Вадимівна, кандидат технічних наук, доцент кафедри засобів захисту інформації Національного авіаційного університету.

Мартынюк Анна Вадимовна, кандидат технических наук, доцент кафедры средств защиты информации Национального авиационного университета.

Martyniuk Hanna, Ph.D., associate professor of Information Security Department of National Aviation University.

Баланюк Юрій Вікторович, кандидат технічних наук, доцент кафедри засобів захисту інформації Національного авіаційного університету.

Баланюк Юрий Викторович, кандидат технических наук, доцент кафедры средств защиты информации Национального авиационного университета.

Balanyuk Yuriy, Ph.D., associate professor of Information Security Department of National Aviation University.

Отримано 28 лютого 2020 року, затверджено редколегією 20 березня 2020 року
