УДК 004.424.5.032.24(043.2)

Гончаренко А.В

Лежух В.В

Добровольська Н.В.

МОДЕЛЮВАННЯ РОЗПОВСЮДЖЕННЯ ВІРУСІВ У СОЦІАЛЬНИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ ГРАФОВИХ СТРУКТУР

Вінницький національний технічний університет

Анотація

У роботі розглянуто моделювання процесу розповсюдження вірусів у соціальних мережах із використанням графових структур. Застосовано епідеміологічну модель SIR для аналізу динаміки зараження в мережах трьох типів: випадкових (ER), малого світу (WS) та безмасштабних (BA). Проведене моделювання дозволило виявити, як топологія мережі впливає на швидкість поширення вірусу та масштаби зараження. Зокрема, встановлено, що безмасштабні графи є найбільш уразливими до вірусного поширення через наявність високозв'язних вузлів. Отримані результати демонструють важливість врахування структури соціальної мережі при оцінці ризиків масового розповсюдження інформації чи шкідливого програмного забезпечення.

Ключові слова: граф, соціальна мережа, SIR, вірус, моделювання, вершина, епідемія.

Abstract

This work examines the modeling of virus spread in social networks using graph structures. The SIR epidemiological model is applied to analyze infection dynamics across three types of networks: Erdős–Rényi (ER), Watts–Strogatz (WS), and Barabási–Albert (BA). The simulations demonstrate how network topology influences the speed and scale of infection spread. In particular, scale-free networks (BA) show higher vulnerability due to the presence of highly connected nodes. The results highlight the importance of considering network structure when assessing the risks of large-scale information or malware dissemination.

Keywords: graph, social network, SIR, virus, modeling, node, epidemic.

Вступ

У сучасному цифровому просторі соціальні мережі стали потужним інструментом для обміну інформацією. Проте їхня відкритість також робить їх вразливими до шкідливих програм, фейкових новин або іншого «вірусного» контенту. Розуміння механізмів поширення таких об'єктів дозволяє не лише ефективніше їх контролювати, а й розробляти методи захисту. Соціальні мережі зручно моделювати у вигляді графів, де вузли — це користувачі, а ребра — зв'язки між ними. Такий підхід дозволяє застосувати математичні та комп'ютерні методи для аналізу динаміки поширення вірусів.

Основна частина

У наш час соціальні мережі перетворилися на ключовий елемент цифрової комунікації, де інформація поширюється надзвичайно швидко та масштабно. Водночас така відкритість середовища робить його вразливим до дезінформації, фейкових новин і шкідливого контенту. Така «вірусна» інформація може мати серйозні наслідки як для окремих користувачів, так і для суспільства загалом. Тому питання моделювання розповсюдження інформаційних вірусів у соціальних мережах є вкрай актуальним і важливим для сфери кібербезпеки.

У нашій роботі ми поставили собі за мету дослідити, як топологія соціальної мережі впливає на швидкість і масштаб поширення вірусної інформації. Для цього було використано епідеміологічну модель SIR, яка добре підходить для подібного аналізу, оскільки дозволяє описати три основні стани користувача: здоровий (sensitive), інфікований (infected) і вилікуваний (recovered).

Для моделювання структури самих соціальних мереж було згенеровано три типи графів:

- ER (випадковий граф) — моделює випадкове з'єднання користувачів;
- WS (граф малого світу) — дозволяє враховувати кластери, як у реальних спільнотах;
- BA (безмасштабна мережа) — імітує ситуації, коли деякі користувачі (вузли) мають значно більше зв'язків, ніж інші, що характерно для соцмереж.

Ми реалізували симуляцію поширення вірусу у цих мережах і провели порівняння. Найшвидше вірус поширювався в BA-графах, особливо якщо інфікувався «хаб» — вузол з великою кількістю зв'язків. У такому випадку зараження охоплювало понад 90 % мережі вже за кілька ітерацій. У WS-графах вірус поширювався кластерно, тоді як у ER-графах — більш випадково та залежно від ймовірності з'єднань.

Результати дослідження свідчать, що для аналізу ризиків та розробки стратегій протидії вірусному поширенню (як інформаційному, так і програмному) необхідно враховувати тип структури мережі. Найбільш уразливими до поширення шкідливої інформації виявились безмасштабні графи, через наявність вузлів, які можуть швидко інфікувати більшість мережі.

Математична модель

Використано адаптовану модель SIR, де кожна вершина графа перебуває у стані здорової (S), інфікованої (I) або вилікуваної (R):

$$\begin{cases} S(t+1) = S(t) - \beta \cdot \dfrac{\mathrm{S(t)} \cdot \mathrm{I(t)}}{\mathrm{N}} \\ I(t+1) = (t) + \beta \cdot \dfrac{\mathrm{S(t)} \cdot \mathrm{I(t)}}{\mathrm{N}} - \gamma \cdot \mathrm{I(t)} \\ R(t+1) = R(t) + \gamma \cdot \mathrm{I(t)} \end{cases}$$

де S — кількість здорових, I — інфікованих, R — вилікуваних користувачів; β — ймовірність зараження, γ — ймовірність одужання, N = S + I + R — загальна кількість користувачів.

У нашому дослідженні ми використали епідеміологічну модель SIR для того, щоб змоделювати процес поширення інформаційного вірусу в соціальній мережі. Ця модель дозволяє поділити користувачів на три стани: здорові (які ще не «заражені» фейком), інфіковані (ті, хто повірив у фейкову інформацію) та вилікувані (ті, хто перестав реагувати на фейки). Завдяки цьому ми змогли прослідкувати динаміку зараження та оцінити, як швидко фейкова інформація поширюється у різних типах мереж. Модель SIR допомогла нам виявити залежність між структурою мережі та масштабами інфікування, що є важливим для розробки ефективних методів протидії дезінформації.

Результати дослідження

У межах виконаної роботи було реалізовано модель поширення вірусу в соціальних мережах за допомогою епідеміологічної моделі SIR на основі трьох типів графів: випадкових (Erdős–Rényi), графів малого світу (Watts–Strogatz) та безмасштабних (Barabási–Albert). Основною метою експериментального моделювання було виявлення, як саме топологія соціальної мережі впливає на швидкість та масштаб поширення інформаційного вірусу.

Для кожного типу графа було згенеровано мережу з однаковою кількістю вершин (користувачів), після чого проводилась серія симуляцій із фіксованими параметрами ймовірності зараження (β) та одужання (γ).

Основні результати:

- у випадкових графах (ER) при низькому рівні ймовірності з'єднань вірус не міг охопити значну частину мережі. Проте при p = 0,2 спостерігалося зараження до 80–85 % користувачів;
- графи малого світу (WS) показали кластерний характер поширення. Хоча зв'язки були більш упорядковані, інформаційний вірус швидко переходив від одного «осередку» до іншого, охоплюючи до 75 % мережі;
- безмасштабні графи (BA) виявилися найбільш вразливими. Якщо інфікувався вузол із великою кількістю зв'язків (так званий «хаб»), то зараження охоплювало понад 90 % мережі вже за кілька ітерацій.

Також було виявлено, що саме структура мережі визначає ефективність можливих стратегій стримування вірусу. У безмасштабних мережах найкращою тактикою виявилось ізолювання високозв'язних вузлів. Водночас у графах малого світу ефективніше працювало блокування каналів передачі між кластерами.

Висновки

Проведене моделювання дозволило зробити висновок, що топологія соціальної мережі суттєво впливає на швидкість і масштаби поширення вірусів. Зокрема, безмасштабні графи, що характерні для реальних соціальних мереж, виявилися найбільш уразливими до швидкого зараження через наявність вузлів із великою кількістю зв'язків. Епідеміологічна модель SIR продемонструвала свою ефективність для опису динаміки вірусного поширення в різних типах мереж, дозволяючи наочно проаналізувати, як зміни в структурі зв'язків можуть впливати на результати зараження. Отримані результати підкреслюють важливість застосування графових підходів для аналізу та прогнозування інформаційних або шкідливих впливів у цифровому середовищі, а також дають змогу формувати рекомендації для підвищення стійкості соціальних платформ до таких загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Newman M. Networks: An Introduction. – Oxford: Oxford University Press, 2010. – 784 с. DOI: https://doi.org/10.1093/acprof:oso/9780199206650.001.0001

2. Pastor-Satorras R., Vespignani A. Epidemic spreading in scale-free networks // Physical Review Letters. – 2001. – Vol. 86, No. 14. – С. 3200–3203. DOI: https://doi.org/10.1103/PhysRevLett.86.3200

3. Ulichev O. S. Дослідження моделей розповсюдження інформації та інформаційних впливів в соціальних мережах // Системи управління, навігації та зв'язку. – 2018. – № 4(50). – С. 147–151. DOI: https://doi.org/10.26906/SUNZ.2018.4.147

4. Дудатьєв А. В. Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту : монографія. – Вінниця : ВНТУ, 2017. – 128 с. URL: https://press.vntu.edu.ua/index.php/vntu/catalog/view/352/680/756-1?inline=1

Лежух Владислав Віталійович, студент групи 1СП-23Б, факультет інформаційних технологій та комп'ютерної інеженерії, Вінницький національний технічний університет, м. Вінниця, email: lezhuhvladd@gmail.com

Гончаренко Анастасія Володимирівна, студентка групи 1СП-23Б, факультет інформаційних технологій та комп'ютерної інеженерії, Вінницький національний технічний університет, м. Вінниця, email: goncharenkoanastasia13@gmail.com

Науковий керівник: ***Добровольська Наталія Вікторівна,*** к.т.н., доцент, кафедра ОТ, ВНТУ

Lezhukh Vladislav V. - student, 1SP-23b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, email: lezhuhvladd@gmail.com

Honcharenko Anastasiia V. - student, 1SP-23b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, email: goncharenkoanastasia13@gmail.com

Supervisor**:** ***Dobrovolska Nataliia Victorivna*** - Assosiate Professor at the Department of Computer Engineering, innytsia National Technical University, email: dobr_n_v@vntu.edu.ua