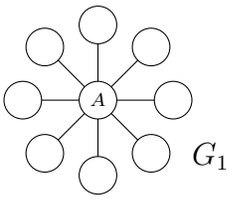
Ukrywanie się w sieciach społecznych

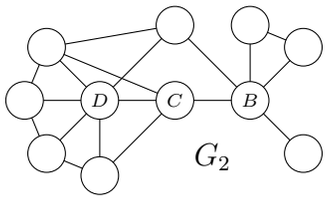
*Marcin WANIEK**

* New York University Abu Dhabi

Choć możemy nie zdawać sobie z tego sprawy, niemal wszystkie działania, które podejmujemy w Internecie (i bardzo wiele poza nim), pozostawiają po sobie cyfrowe ślady. Nieistotne, czy rozmawiamy z przyjaciółmi przez telefon, oglądamy film na YouTubie, czy zamieszczamy komentarz pod zdjęciem kota, informacje o tych wydarzeniach są gdzieś skrzętnie rejestrowane. Bardzo często tego rodzaju dane wygodnie jest reprezentować w postaci sieci społecznej, gdzie każdy wierzchołek odpowiada pojedynczej osobie, wierzchołki zaś połączone są krawędzią, jeżeli zachodzi między nimi określona relacja (na przykład jeżeli te osoby są znajomymi na Facebooku albo jeżeli doszło między nimi do spotkania w ciągu ostatniego roku).



G_1



G_2

Co można zrobić z tak skonstruowaną siecią społeczną? Można na przykład próbować wyciągnąć z niej dodatkowe informacje przy użyciu różnego rodzaju narzędzi analizy sieci społecznych (*social network analysis*). Jednym z najpopularniejszych typów takich narzędzi są miary centralności. Pozwalają one określić na podstawie struktury sieci, który z wierzchołków jest najważniejszy. Warto w tym momencie zwrócić uwagę, że mogą kierować się przy tym bardzo różnorodnymi kryteriami. O ile w przypadku sieci G_1, pokazanej na marginesie, każdy z was zgodzi się pewnie, że wierzchołek A wydaje się najistotniejszy, o tyle w przypadku sieci G_2 trudno o tak oczywistego kandydata. *Miara centralności stopnia* (*degree*) stwierdziłaby na przykład, że najważniejszy jest wierzchołek D, ponieważ ma najwięcej przyjaciół. *Miara centralności bliskości* (*closeness*) doszłaby z kolei do wniosku, że to wierzchołek C jest najbardziej znaczący, ponieważ średnio najmniej „uścisków dłoni" dzieli go od innych członków sieci. *Miara centralności pośredniczenia* (*betweenness*) orzekłaby zaś, że to B jest kluczowy, pośredniczy bowiem w przekazywaniu informacji między różnymi częściami sieci.

O tych i innych miarach centralności pisaliśmy już w Δ_{08}^{08} , Δ_{16}^{11} oraz Δ_{21}^{09} .

Super, zatem wiemy, że miary centralności potrafią wskazać najważniejszy (w jakimś sensie) wierzchołek w sieci społecznej. Dlaczego mielibyśmy się tym przejmować? Pamiętajmy, że sieci, których jesteśmy częścią, można konstruować i analizować bez naszej wiedzy i zgody. Wyobraźmy sobie na przykład, że jesteśmy opozycyjnymi blogerami w autorytarnym społeczeństwie, a rząd wykorzysta miary centralności, aby wybrać tych spośród nas, wobec których zastosowane zostaną surowe represje. Miary centralności mogą też zostać wykorzystane przez grupy hakerskie, aby wybrać najbardziej kuszące cele ataków, albo przez firmy marketingowe, aby wyselekcjonować użytkowników, którzy nękani będą ciągłymi telefonami. Czy istnieje zatem jakiś sposób na ukrycie się przed miarami centralności?

Załóżmy, że jesteśmy wierzchołkiem w sieci i naszym celem jest sprawienie, że będziemy wydawać się mniej istotni, niż jesteśmy naprawdę. Aby to zrobić, możemy dodawać i usuwać z sieci krawędzie. Dodanie krawędzi można zinterpretować jako zawarcie nowej znajomości lub odbycie z kimś rozmowy telefonicznej, pozbycie się krawędzi zaś jako usunięcie kogoś z grona znajomych lub zaniechanie kontaktów z określoną osobą.

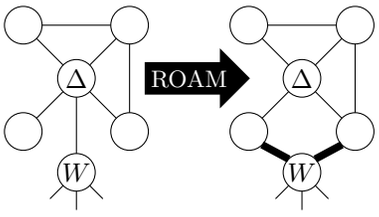
Mamy tu na myśli problem optymalizacyjny odpowiadający następującemu problemowi decyzyjnemu: czy dla danej centralności, grafu $G = (V, E)$, wierzchołka $v \in V$, liczby $k \in \mathbb{N}$ oraz progu $r \in \mathbb{R}$ istnieje k krawędzi, które możemy dodać lub usunąć w G, aby zmniejszyć centralność v o co najmniej r?

Marcin Waniek, Tomasz P. Michalak, Michael J. Wooldridge and Talal Rahwan. *Hiding individuals and communities in a social network*. „Nature Human Behaviour" (2018).

Okazuje się, że problem optymalnego ukrywania się jest NP–zupełny dla większości popularnych miar centralności. Tłumacząc z informatycznego na polski, znalezienie najbardziej efektywnego sposobu na ukrycie się przed miarami centralności jest niemożliwe dla większych sieci. Co więcej, nawet gdyby taki optymalny algorytm istniał, byłby pewnie trudny do zastosowania w praktyce. Wymagałby bowiem wiedzy na temat struktury całej sieci. Większość z nas posiada natomiast informacje na temat swojego bezpośredniego sieciowego otoczenia (wiemy zazwyczaj, czy dwoje z naszych przyjaciół zna siebie nawzajem), ale nie na temat bardziej odległych fragmentów sieci (nie wiemy nic na temat znajomości przypadkowego przechodnia).

Co jednak, jeżeli nie aspirujemy do znalezienia optymalnego sposobu na ukrycie się, a wystarczy nam metoda skuteczna w praktyce, którą będziemy w stanie zastosować, posiadając jedynie ograniczoną wiedzę o sieci? Wówczas dobrym

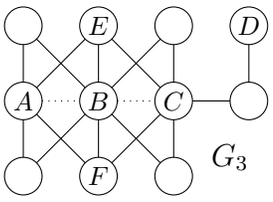
wyborem jest użycie algorytmu ROAM (*Remove One, Add Many*, „usuń jedną, dodaj wiele”). Aby go zastosować, trzeba najpierw zidentyfikować swojego sąsiada, który ma najwyższy stopień (tj. ma najwięcej znajomych), nazwijmy go W. Następnie należy utworzyć krawędzie pomiędzy W a kilkoma naszymi sąsiadami z niewielką liczbą znajomych, po czym usunąć swoje własne połączenie z W (przykład zastosowania ROAM możecie zobaczyć poniżej, ukrywający się węzeł to Δ). W ten sposób nie tylko możemy obniżyć swoją centralność, stając się mniej narażonymi na wykrycie, ale również podtrzymać swój wpływ na sieć (zamiast łączyć się z W bezpośrednio, czynimy to za pośrednictwem naszych nowych wspólnych znajomych).



Aby zilustrować skuteczność ROAM, posłużmy się przykładem. Pokazuje on, jak niebezpieczne mogą być algorytmiczne techniki ukrywania się, gdy wykorzystane są przez nieodpowiednie osoby. W sieci trzydziestu sześciu terrorystów odpowiedzialnych za przygotowanie i przeprowadzenie ataków z 11 września 2001 roku ich przywódca, Mohamed Atta, jest identyfikowany jako najważniejszy wierzchołek przez wszystkie trzy wspomniane wyżej miary centralności. Po zaledwie dwukrotnym zastosowaniu ROAM (a więc usunięciu dwóch i dodaniu czterech krawędzi) Atta spada na, odpowiednio, piąte miejsce dla centralności stopnia, czwarte dla centralności bliskości i jedenaste dla centralności pośredniczenia.

Mniejsza wersja tej sieci, uwzględniająca tylko zamachowców–samobójców, pojawiła się w artykule *Rozbijanie sieci terrorystycznych za pomocą teorii gier*, Δ_{16}^{11}.

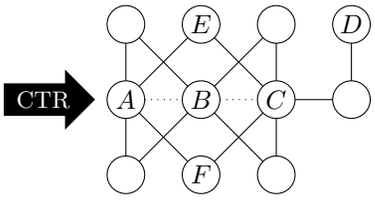
Świetnie, potrafimy zatem poradzić sobie (przynajmniej do pewnego stopnia) z miarami centralności. Czy istnieją jakieś inne narzędzia analizy sieci społecznych, których powinniśmy się obawiać? Jednym z przykładów mogą być algorytmy przewidywania połączeń (*link prediction algorithms*). Pozwalają one, na podstawie aktualnego stanu sieci, wydedukować, które pary wierzchołków nawiążą znajomość w przyszłości albo też są połączone krawędzią, która już istnieje, ale o niej nie wiemy. Jak działają tego rodzaju algorytmy? Spójrzmy na sieć G_3 przedstawioną na górze po prawej stronie. Wierzchołki A i B (jak również B i C) są położone bardzo blisko siebie i mają wielu wspólnych znajomych, większość algorytmów przewidywania połączeń przypisałaby im zatem wysokie prawdopodobieństwo nawiązania znajomości w przyszłości (albo istnienia niewidocznej krawędzi pomiędzy nimi). W szczególności fakt posiadania dużej liczby wspólnych znajomych często jest bardzo znaczący. Kiedy natomiast spojrzymy na wierzchołki A i D, nie wydaje się, aby miały ze sobą zbyt wiele wspólnego, większość algorytmów przypisałaby krawędzi między nimi niskie prawdopodobieństwo istnienia (lub zaistnienia w przyszłości).



Wszystko to brzmi bardzo niewinnie, czy mogą istnieć zatem powody, dla których mielibyśmy się obawiać algorytmów przewidywania połączeń? Mają one w końcu wiele pożytecznych zastosowań, na przykład za każdym razem, kiedy Facebook sugeruje nam „osobę, którą możemy znać”, widzimy efekt działania algorytmu. Co jednak, jeżeli nie jesteśmy gotowi dzielić się z całym światem niektórymi z naszych znajomości? A nawet gdy nie mamy absolutnie nic do ukrycia, co jeżeli algorytm omyłkowo powiąże nas z osobą, z którą absolutnie nie chcielibyśmy być kojarzeni? Czy możemy jakoś zmylić algorytmy przewidywania połączeń?

Marcin Waniek, Kai Zhou, Yevgeniy Vorobeychik, Esteban Moro, Tomasz P. Michalak and Talal Rahwan. *How to hide one's relationships from link prediction algorithms.* „Scientific reports” (2018).

Podobnie jak dla miar centralności, również i w tym przypadku okazuje się, że znalezienie sposobu na optymalne ukrycie kilku krawędzi jest problemem NP–zupełnym. Jest to prawda nawet dla stosunkowo prostych algorytmów przewidywania połączeń. Na szczęście i tutaj da się zastosować heurystyczną (czyli niegwarantującą znalezienia optymalnego rozwiązania) metodę ukrywania się o nazwie CTR (*Closed Triad Removal*, usuwanie zamkniętych triad). Polega ona na usuwaniu z sieci krawędzi, które należą do największej liczby takich „trójkątów”, czyli cykli długości 3 (w nomenklaturze sieciowej zwanych triadami), w których dokładnie jedną z krawędzi chcemy ukryć. Na rysunku poniżej przykład zastosowania CTR w sytuacji, gdy chcemy ukryć krawędzie AB oraz BC w sieci G_3. Usunięcie każdej z krawędzi BE i BF spowodowało, że zarówno para węzłów AB, jak i para BC straciły wspólnego sąsiada, zmniejszając w ten sposób ryzyko wykrycia krawędzi pomiędzy nimi. Czy potrafisz, Czytelniku, wskazać, do jakich „zamkniętych triad” należały krawędzie BE i BF?



Dowiedzieliśmy się, jak możemy (próbować) ukryć się przed miarami centralności i algorytmami przewidywania połączeń. Jest jednak jeszcze jeden wniosek płynący z naszych rozważań. Bądźmy świadomi, że ślady, które pozostawiamy online, mogą zostać użyte do wydedukowania na nasz temat informacji, których nigdzie nie zamieściliśmy (a którymi nie chcielibyśmy się dzielić). Być może przed wrzuceniem kolejnego kawałka naszego prywatnego życia na nowy portal społecznościowy warto zastanowić się, czy przebiegły obserwator nie odkryje dzięki temu czegoś, co wolelibyśmy zachować dla siebie.