UNIWERSYTET WARSZAWSKI

Biuro Prasowe

30.01.2018

PRYWATNOŚĆ W SIECI

W sieci pojawia się coraz więcej wyrafinowanych narzędzi do analizy danych, które potrafią wykrywać społeczności i identyfikować konkretne osoby. O działaniu tych narzędzi i tym, jak chronić prywatność w sieci, można przeczytać w artykule opublikowanym w magazynie *Nature Human Behaviour.* Jednym z jego autorów jest dr Tomasz Michalak z UW.

Rosnąca digitalizacja stosunków międzyludzkich, a w szczególności media społecznościowe, wzbudzają ogromne zainteresowanie narzędziami do analizy osobistych powiązań. Szczególnie rozwijane są metody wykrywania specyficznych grup i identyfikowania kluczowych osób w sieciach. Pomimo wielu zalet, narzędzia analizy sieci społecznych zagrażają prywatności.

Miary centralności

W pracy „Hiding Individuals and Communities in a Social Network" opublikowanej w czasopiśmie *Nature Human Behaviour* autorzy pytają czy pojedyncze osoby, jak i całe społeczności, mogą aktywnie zarządzać swoimi połączeniami, tak aby zmylić ewentualną analizę dotyczącą ich pozycji w sieci. – Chcemy zrozumieć nie tylko to, jak ogół społeczeństwa może lepiej chronić swoją prywatność, ale także jak grupy aktywistów politycznych (blogerów) w reżimach autorytarnych mogą lepiej ukrywać swoją działalność. Sprawdzamy również, w jaki sposób przestępcy mogą manipulować kształtem sieci kryminalnych – mówi dr Tomasz Michalak z Wydziału Matematyki, Informatyki i Mechaniki UW.

Autorzy pracy skoncentrowali się na najważniejszych miarach centralności (sposobach pomiaru, czy dana osoba bądź grupa jest ważna w sieci) – tj. centralnościach stopnia, bliskości, pośrednictwa oraz wektora własnego. W szczególności badano, w jaki sposób kluczowe jednostki mogą obniżyć swoją centralność bez zmniejszenia swojego wpływu na sieć (czyli, mimo że osoba ma istotny wpływ na innych, nie można tego dostrzec, analizując sieć podstawowymi miarami centralności).

Sieci kryminalne i terrorystyczne

Naukowcy udowodnili, że optymalne rozwiązanie problemu jest obliczeniowo trudne, nie zawsze jednak poszukiwane są rozwiązania optymalne. – Okazuje się, że nawet prosty

Krakowskie Przedmieście 26/28, Pałac Kazimierzowski, pokój 11
tel.: 22 55 24 066
e-mail: media@uw.edu.pl

algorytm heurystyczny, w którym manipulacje połączeniami ograniczone są do sąsiedztwa ukrywającej się osoby, może być zaskakująco skuteczny w praktyce – mówi dr Michalak. – Ten wynik nie tylko może pomóc zwykłym ludziom chronić swoją prywatność, ale jest również wskazówką dla organów ścigania w kontekście analizy sieci kryminalnych i terrorystycznych. Okazuje się, że liderzy sieci przestępczych, którzy coraz sprawniej poruszają się w świecie cyfrowym, mogą w bardzo prosty sposób ukryć swoją prawdziwą rolę. Na przykład, jak wykazaliśmy w pracy, wprowadzając tylko niewielkie zmiany do swojego otoczenia, Mohamed Atta mógłby łatwo zamaskować swoją wiodącą pozycję w sieci terrorystycznej, która przeprowadziła atak na World Trade Center w 2001 roku – dodaje.

Autorzy publikacji: Marcin Waniek (Masdar Institute of Science and Technology, UAE), Tomasz Michalak (Wydział Matematyki, Informatyki i Mechaniki UW), Michael Wooldridge (Department of Computer Science, Oxford University), Talal Rahwan (Masdar Institute of Science and Technology, UAE).