Biuletyn WAT
Vol. LXVIII, Nr 2, 2019

Adaptacyjna metoda badania podobieństwa profili użytkowników w Internetowych Sieciach Społecznych

MICHAŁ ZABIELSKI, ZBIGNIEW TARAPATA, RAFAŁ KASPRZYK

Wojskowa Akademia Techniczna, Wydział Cybernetyki, Instytut Systemów Informatycznych,
ul. gen. S. Kaliskiego 2, 00-908 Warszawa, michal.zabielski@wat.edu.pl,
zbigniew.tarapata@wat.edu.pl, rafal.kasprzyk@wat.edu.pl

Streszczenie: W pracy podjęto próbę opracowania adaptacyjnej metody uwzględniającej strukturalne i ilościowe związki między kontami w Internetowej Sieci Społecznej w celu wykrywania potencjalnie sklonowanych profili użytkowników. Wprowadzono również technikę kontenerów podobieństwa, pozwalającą na grupowanie atrybutów profilu użytkownika ze względu na typ danych oraz istotność. Zaprezentowano przykład liczbowy, który ilustruje działanie opracowanej metody. Zasygnalizowano przydatność opracowania symulatora pozwalającego na badanie wpływu zawiązywania znajomości między użytkownikami Internetowej Sieci Społecznej na skuteczność wykrywania sklonowanych profili użytkowników, dając tym samym podstawy do zbudowania środowiska prognozującego klonowanie profili.
Słowa kluczowe: Internetowe Sieci Społeczne (ISS), klonowanie profili użytkowników, naruszenie prywatności w sieci
DOI: 10.5604/01.3001.0013.3002

1. Wprowadzenie

Gwałtowny rozwój sieci Internet oraz technologii Web 2.0 spowodował znaczący wzrost popularności Internetowych Sieci Społecznych (ang. *Online Social Networks, OSN*). Internetowe Sieci Społeczne (ISS) zwykle analizowane są z wykorzystaniem modeli i metod teorii grafów i sieci. Węzły reprezentują osoby posiadające konta w analizowanej sieci, natomiast gałęzie odwzorowują różnego rodzaju związki pomiędzy kontami w sieci, np. znajomość, podległość, współpracę [1]. Przykładami współcześnie istniejących ISS mogą być: Facebook, Twitter, LinkedIn czy Instagram.

ISS wyróżniają się na tle innych usług internetowych wysokim poziomem interakcji pomiędzy użytkownikami sieci, jak również dużą wrażliwością na zagadnienie prywatności, rozumianej tutaj jako możliwość jednostki lub grupy osób do utrzymania swych danych oraz osobistych zwyczajów i zachowania nieujawnionych publicznie [2]. Wynika to z faktu, że podstawowym wyróżnikiem użytkownika sieci jest tutaj element nazywany *profilem użytkownika*. Profil użytkownika w Intenetowej Sieci Społecznej jest zestawem cech opisujących osobę w tej sieci wraz ze związkami wiążącymi ją z innymi członkami sieci społecznej [3]. Stanowi on o tożsamości osoby w ISS, buduje jej wiarygodność i umożliwia komunikację z innymi członkami sieci. Ponieważ profil użytkownika i prywatność mają elementy wspólne w postaci danych i związków pomiędzy osobami, naruszając prywatność, możemy doprowadzić do utraty wiarygodności tożsamości użytkownika w ISS, co może prowadzić do konkretnych strat materialnych (wykorzystanie tożsamości osoby do autoryzowania operacji finansowych), politycznych (wykorzystanie tożsamości do wyrażania w jej imieniu kontrowersyjnych poglądów) czy społecznych (wykorzystanie tożsamości w celu zmodyfikowania związków między użytkownikami sieci).

Istotne straty, jakich można doświadczyć w przypadku naruszenia prywatności w ISS, spowodowały wzrost zainteresowania zagadnieniem jej ochrony. W wyniku intensywnych prac opracowano techniki, których stosowanie prowadzi do naruszania poczucia bezpieczeństwa w sieci. Jedną z technik jest metoda odkrywania ukrytych wartości atrybutów profili użytkownika z wykorzystaniem technik uczenia maszynowego, która szczegółowo została opisana w [4]. Innym podejściem jest wykorzystanie profilu użytkownika z innej ISS do poznania wartości atrybutów profilu osoby w badanej sieci. Takie rozwiązanie opisano na przykład w [5]. Istnieje również możliwość wykrywania ukrytych związków między użytkownikami ISS — przykładowe rozwiązanie tego problemu opisano w [6].

Poza rozpoznaniem atakujących metod działania, opracowano kilka mechanizmów pozwalających zapobiegać faktowi naruszania prywatności. Przykład kompleksowego działania w tej materii został opisany w [7].

Na szczególną uwagę w tym obszarze zasługują algorytmy, które zajmują się zagadnieniem *klonowania profilu użytkownika* w *ISS*.

Mechanizm klonowania profilu użytkownika w *ISS* polega na odtworzeniu danych ofiary wraz ze strukturą jej kontaktów w celu przejęcia jej tożsamości. Jest to możliwe do wykonania, ponieważ dziś nie istnieje jeden unikalny profil użytkownika w całej sieci Internet, zatem w przypadku takich samych danych i związków między osobą a jej bezpośrednimi kontaktami nie będzie dochodziło do konfliktów.

Ze względu na charakter przeprowadzanego ataku możemy mówić o globalnej i lokalnej metodzie klonowania. W przypadku podejścia lokalnego atakujący tworzy profil użytkownika w tej samej ISS co ofiara, prowadząc do sytuacji, w której istnieje kilka potencjalnie prawdziwych kont tej samej osoby. Rozwiązanie takie jest względnie łatwe do osiągnięcia przez atakującego, natomiast stanowi trudność, jeśli chodzi

o kwestię zapewnienia przez intruza wiarygodności takiego profilu — musi bowiem przekonać znajomych ofiary, że nowo utworzone konto użytkownika należy do osoby, pod którą się podszywa. Innym rodzajem klonowania jest podejście globalne. Zakłada ono, że ofiara posiada konto w jednej ISS, natomiast atakujący wykorzystuje dane z tego konta do utworzenia sklonowanego profilu w innej sieci społecznej. Co do zasady, taki mechanizm jest łatwiejszy do zbudowania wiarygodności, ponieważ ofiara mogła nie mieć swojego profilu w sieci będącej przedmiotem ataku intruza, więc łatwiej jest przekonać do siebie znajomych osoby atakowanej. Z drugiej strony technika odtwarzania konta użytkownika może być utrudniona — należy w pierwszej kolejności znaleźć konto ofiary w innej ISS, przetworzyć jego dane na format odpowiedni dla sieci społecznej będącej przedmiotem zainteresowania atakującego i dopiero wtedy zbudować profil. W praktyce zarówno jedna, jak i druga technika klonowania znajdują szerokie zastosowanie.

Obecnie istnieje wiele metod pozwalających na wykrywanie faktu podszywania się pod tożsamość użytkownika. Część z nich opiera się na technikach uczenia maszynowego [8]. Inne wykorzystują teorię grafów i sieci w celu wykrywania podobnych struktur [9], [10]. Spotkać można również rozwiązania, które głównie analizują zachowanie użytkownika i na podstawie wzorców behawioralnych określają, czy doszło do sklonowania profilu, czy nie [11]. Dotychczas wykorzystywane techniki mają jednak kilka niedoskonałości, które utrudniają ich wykorzystanie w praktyce. W przypadku techniki opisanej w [8], [9] otrzymujemy listę podejrzanych profili, przy czym wszystkie z nich są tak samo istotne. Oznacza to, że w celu znalezienia klona należałoby przejrzeć wszystkie wyznaczone przez algorytm konta, aby odnaleźć fałszywy profil. Ponieważ w wielu przypadkach uzyskana lista węzłów jest długa, odnalezienie klona może być czasochłonne. W metodzie [10] zakłada się zbudowanie tak zwanego Grafu Zaufania Społecznego (ang. *Trusted Social Graph*), który uwzględnia w swojej budowie sposób komunikacji między kontami ISS. Ponieważ tego typu informacje są dużo trudniejsze do pozyskania niż struktura ISS, praktyczna użyteczność metody jest niewielka. Technika [11] również zakłada istnienie behawioralnych danych o użytkownikach sieci społecznej, co przekłada się na jej szybkość działania i możliwość wykorzystania.

W celu wyeliminowania niedoskonałości wcześniej opisanych metod, opracowane zostały autorski model i metoda badania podobieństwa profili użytkowników w ISS przedstawione w rozdziale 2. Rozdział 3 zawiera przykład liczbowy wykorzystania zaproponowanej w rozdziale 2 metody badania podobieństwa profili. W rozdziale 4 opisano koncepcję środowiska symulacyjnego, w którym możliwe byłoby symulowanie w czasie tworzenia się znajomości w badanej ISS. Pracę kończy podsumowanie.

2. Metoda badania podobieństwa profili użytkowników w Internetowych Sieciach Społecznych

Opracowane rozwiązanie jest wynikiem rozszerzenia modelu utworzonego przez autorów, który został szczegółowo opisany w [12], [13]. Rozszerzenie polega m.in. na wprowadzeniu tzw. kontenerów podobieństwa oraz kocepcji symulacyjnej metody badania podobieństwa profili użytkowników sieci społecznej. Kontenery umożliwiają grupowanie atrybutów profilu użytkownika ze względu na typ danych oraz ich istotność, pozwalając przy tym na nadanie kontekstu danym, co ostatecznie przekłada się na zwiększenie skuteczności znajdowania profili podobnych. Podstawą zaproponowanej metody jest model ISS zbudowany w postaci ważonego unigrafu skierowanego bez pętli, w którym węzły reprezentują konta, natomiast łuki związki między kontami użytkowników w ISS. Wagi reprezentują wartości atrybutów opisanych na wierzchołkach. W tak przygotowanej sieci badane jest podobieństwo między węzłami, uwzględniające wartości atrybutów profilu użytkownika. Na podstawie wyznaczonych wartości podobieństwa do dalszej analizy wybierane są te konta, których wartość podobieństwa jest wystarczająco wysoka. W kolejnym kroku analizowane jest sąsiedztwo podejrzanych węzłów w stosunku do sąsiadów węzła będącego wzorcem. Na podstawie tego wyznaczane jest tak zwane podobieństwo sąsiedztwa węzłów. Jeśli podobieństwo to jest wystarczająco wysokie, węzeł trafia na listę podejrzanych. W efekcie otrzymujemy listę profili użytkowników ISS będących potencjalnymi klonami, przy czym lista ta jest uporządkowana względem wartości podobieństwa węzłów i podobieństwa sąsiedztwa.

Podstawowe oznaczenia w modelu są następujące:

A — zbiór atrybutów opisujących profil użytkownika w sieci społecznej;

$l = |A|$ — liczba atrybutów opisujących profil użytkownika sieci społecznej;

S — model badanej sieci ISS;

$$S = \left\langle G = \langle W, U \rangle, \{a_i\}_{i=\overline{1,l}}, \varnothing \right\rangle; \tag{1}$$

$G = \langle W, U \rangle$ — unigraf skierowany bez pętli;

W — zbiór wierzchołów grafu G; U — zbiór łuków grafu G; $U \subset \{\langle x, y \rangle : x, y \in W\}$;

$a_i : W \to X_i$ — wartość i-tego atrybutu profilu użytkownika (element zbioru opisany na wierzchołkach grafu G);

$t_s \in [0,1]$ — wartość progowa podobieństwa sąsiedztwa między węzłami;

$t_{ID} \in [0,1]$ — wartość progowa podobieństwa między węzłami;

C^k — k-ty kontener podobieństwa, $k = \overline{1,c}$;

$$C^k = \left\langle A^k, D^k, P^k \right\rangle; \tag{2}$$

c — liczba tzw. kontenerów podobieństwa, $c \in \mathbb{N} \wedge c \geq 1$;

$A^k \subseteq A$ — zbiór numerów atrybutów wchodzących w skład *k*-tego kontenera podobieństwa, przy czym $(i \neq j \Rightarrow A^i \cap A^j = \varnothing) \wedge \bigcup_{k=\overline{1,c}} A^k = A$;

$n^k = |A^k|$ — moc zbioru atrybutów wchodzących w skład *k*-tego kontenera;

$D^k = \left\{d_i^k\right\}_{i=\overline{1,d^k}}$ — zbiór miar podobieństwa wartości atrybutów w *k*-tym kontenerze;

d^k — liczba miar podobieństwa wartości atrybutów w *k*-tym kontenerze, $d^k \in \mathbb{N} \wedge d^k \geq 1$;

$d_i^k : X_j \times X_j \to [0,1]$ — *i*-ta miara podobieństwa wartości atrybutów w *k*-tym kontenerze;

$P^k = \left\{p_i^k\right\}_{i=\overline{1,p^k}}$ — zbiór miar podobieństwa węzłów w *k*-tym kontenerze;

p^k — liczba miar podobieństwa węzłów w *k*-tym kontenerze, $p^k \in \mathbb{N} \wedge p^k \geq 1$;

α^k — istotność *k*-tego kontenera podobieństwa, $\alpha^k \in [0,1] \wedge \sum_{k=1}^{c} \alpha^k = 1$;

$ID : W \times W \to [0,1]$ — funkcja podobieństwa między węzłami sieci *S*;

$w_0 \in W$ — wyróżniony wierzchołek sieci *S* (np. będący potencjalną ofiarą);

$s_y^x \in \mathbb{N} \cup \{0\}$ — liczba wspólnych sąsiadów dwóch węzłów, $x, y \in W$;

N_y — zbiór wierzchołków przyległych do *y*;

$$N_y = \left\{x \in W : \langle y, x \rangle \in U \vee \langle x, y \rangle \in U\right\} \tag{3}$$

H — zbiór wierzchołków podobnych do siebie pod względem wartości atrybutów w sieci *S*,

$$H = \left\{y \in W : ID\left(y, w_0\right) \geq t_{ID}\right\} \tag{4}$$

$d_*^{zk}(a_z(w_1), a_z(w_2))$ — maksymalna wartość podobieństwa wartości atrybutów dla atrybutu *z*-tego w kontenerze *k*-tym, $w_1, w_2 \in W, z \in \{1, \ldots, l\}$;

$$d_*^{zk}(a_z(w_1), a_z(w_2)) = \max_{i=1,d^k} d_i^k(a_z(w_1), a_z(w_2)) \tag{5}$$

$p_i^k : W \times W \to [0,1]$ — *i*-ta miara podobieństwa węzłów w *k*-tym kontenerze, gdzie:

$$p_i^k\left(w_1, w_2\right) = f\left(D\left(w_1, w_2\right)\right)$$

$$D\left(w_1, w_2\right) = d_*^{1k}\left(a_1\left(w_1\right), a_1\left(w_2\right)\right), \ldots, d_*^{lk}\left(a_l\left(w_1\right), a_l\left(w_2\right)\right)$$

$p_*^k(w_1, w_2)$ — maksymalna wartość podobieństwa węzłów w kontenerze *k*-tym, $w_1, w_2 \in W$,

$$p_*^k(w_1, w_2) = \max_{i=1,p^k} p_i^k(w_1, w_2). \tag{6}$$

W obecnej postaci modelu funkcja *ID* opisana jest zależnością:

$$ID(x,y)=\sum_{k=1}^{c}\alpha^{k}\cdot p_{*}^{k}(x,y)\in[0,1]. \tag{7}$$

Zaznaczyć należy, że jest to jedna z możliwych do wykorzystania funkcji — zmieniając zależność na inną, możemy dostosowywać zaproponowany model do preferencji decydenta/analityka. Takie elastyczne rozwiązanie pozwala na dostrajanie modelu przez analityka, jak również na wprowadzenie mechanizmów wielokryterialnych do badania podobieństwa węzłów.

Metoda badania podobieństwa profili użytkowników bazująca na przedstawionym modelu wygląda następująco:

1. Definiujemy początkowe wartości t_{ID}, t_s, oraz ustalamy S i w_0.
2. $K := \varnothing$
3. $N_{w_0} := \{x \in W : \langle w_0, x\rangle \in U \vee \langle x, w_0\rangle \in U\}$
4. Dla każdego $y \in W\{w_0\}$:
   4.1. Wyznaczamy *ID* (y, w_0)
5. Tworzymy zbiór $H := \{y \in W : ID(y, w_0) \geq t_{ID}\}$
6. Dla każdego $\mathrm{h} \in H$:
   6.1. $s_{w_0}^{h} := 0$
   6.2. $N_h := \{x \in W : \langle h, x\rangle \in U \vee \langle x, h\rangle \in U\}$
   6.3. $s_{w_0}^{h} := |N_h \cap N_{w_0}|$
   6.4. Jeżeli $\dfrac{s_{w_0}^{h}}{|N_h \cup N_{w_0}|} \geq t_s$, to $K := K \cup \{h\}$
7. KONIEC.

Metoda przyjmuje dwa istotne założenia:

1) Badamy jedynie bezpośrednich sąsiadów potencjalnej ofiary oraz potencjalnego klona.
2) Stopień podobieństwa wartości atrybutów musi być dostatecznie duży (przekraczający t_{ID}), by móc przystąpić do badania podobieństwa pod względem sąsiedztwa.

Założenie 1 wynika z obserwacji działań atakujących i z pobudek praktycznych przy wykonywaniu ataku: w przypadku gdy atakujący chce sklonować profil, przystępuje do odtwarzania tożsamości ofiary. Nie czyni tego jednak dla profili znajomych ofiary, gdyż zależy mu przede wszystkim na tym, by z tymi osobami się skomunikować. Ponadto, jeśli intruz będzie chciał sklonować profil, musi zawrzeć znajomości z tymi samymi bezpośrednimi znajomymi co ofiara — dalsze stopnie pogłębienia znajomości powinny wtedy automatycznie być tożsame z profilem

ofiary. Założenie 2 natomiast zakłada, że jeśli nie zachodzi istotne podobieństwo wartości atrybutów, to badanie podobieństwa sąsiedztwa dla takiego węzła nie ma sensu, ponieważ samo sąsiedztwo nie jest w stanie jednoznacznie określić tożsamości osoby w ISS. Rozpatrywane założenie znacząco zmniejsza przestrzeń węzłów wykorzystywanych w dalszej analizie, co przekłada się na przyspieszenie obliczeń w omawianej metodzie.

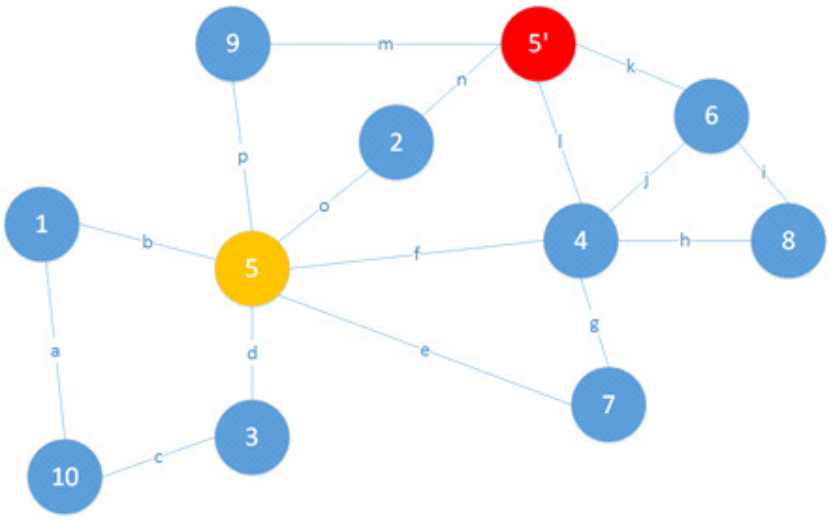
Nowatorstwo zaproponowanej metody polega na uwzględnieniu podobieństwa wartości atrybutów analizowanych kont. Dzięki temu, biorąc pod uwagę niepewność danych profilu użytkownika, możliwe staje się uwzględnianie wartości wystarczająco podobnych, by uznać je za wiarygodne do odtworzenia profilu ofiary. Ponadto model pozwala na kalibrację istotności atrybutów profilu użytkownika w procesie identyfikacji węzłów jako potencjalnych klonów oraz nadawanie kontekstu danym z profilu poprzez zastosowanie autorskiego mechanizmu — tzw. *kontenerów podobieństwa*.

Kontenery podobieństwa pozwalają na grupowanie atrybutów profilu użytkownika, zarówno pod względem typu danych, jak i ich istotności. W pojedynczym kontenerze podobieństwa jesteśmy w stanie określić zestaw miar podobieństwa wartości atrybutów i miar podobieństwa węzłów, które chcemy zaaplikować dla wybranego podzbioru atrybutów. Dzięki takiemu podejściu mamy możliwość stosowania różnych technik badania podobieństwa w zależności od wybranego zestawu atrybutów [14]. Oprócz tego, każdemu z kontenerów nadawana jest wartość istotności α^k, na podstawie której możemy określić, które wartości atrybutów z kontenerów są ważniejsze w procesie badania podobieństwa. Pozwala to ekspertowi na kalibrowanie modelu stosownie do potrzeby, nadając danym pewien kontekst, co wpływa znacząco na skuteczność wykrywania sklonowanych profili.

3. Przykład liczbowy wykorzystania metody badania podobieństwa profili użytkowników w Internetowych Sieciach Społecznych

W celu zaprezentowania działania metody rozpatrzmy Internetową Sieć Społeczną, której struktura została zaprezentowana na rysunku 1.

Wierzchołek o numerze 5 reprezentuje ofiarę, natomiast wierzchołek o numerze 5′ profil sklonowany. Wartości atrybutów składających się na profil użytkowników ISS opisuje tabela 1.



Rys. 1. Przykładowy model ISS
Źródło: opracowanie własne

Tabela 1

Tabela wartości atrybutów profili użytkowników w przykładowej ISS

ID	Imię	Nazwisko	E-mail	Wiek	Uczelnia	Zawód	Płeć
1	Maciej	Zabielski	zdobdol@gmail.com	24	SGGW	Ekonomista	M
2	Iwona	Zabielska	izabielska@gmail.com	27	UW	Analityk danych	K
3	Zbigniew	Zabielski	zzabielski@gmail.com	50	UW	Historyk	M
4	Krzysztof	Szkółka	kszkolka@gmail.com	30	WAT	Informatyk	M
5	Michał	Zabielski	mzabielski@wat.edu.pl	27	WAT	Informatyk	M
5’	Michał	Zabielski	mz@op.pl	26	WAT	Informatyk	M
6	Złodziej	Danych	haker@gmail.com	21	PW	Haker	M
7	Kamil	Banach	kbanach@gmail.com	24	WAT	Informatyk	M
8	Marcin	Cieślewicz	mcieslewicz@gmail.com	28	WAT	Informatyk	M
9	Robert	Baker	rbaker@gmail.com	52	SGH	CEO	M
10	Emilia	Włostowska	ewlostowska@gmail.com	22	SGGW	Ekonomista	K

Źródło: opracowanie własne

Dla tak przygotowanych danych określone zostały parametry modelu zgodnie z wprowadzonymi wcześniej oznaczeniami, opisane poniżej.
Zbiór atrybutów A jest następujący:

A = {imię, nazwisko, e-mail, wiek, uczelnia, zawód, płeć}

Przyjęto subiektywnie $c = 4$ kontenery podobieństwa. Ich wybór był uzasadniony rodzajem danych, które zawarte są w tabeli 1. Kontenery są następujące:

$$C^1 = \left\langle A^1, D^1, P^1 \right\rangle = \left\langle \{\text{imie,nazwisko,e-mail}\}, \{compare\}, \{common\} \right\rangle$$
$$C^2 = \left\langle A^2, D^2, P^2 \right\rangle = \left\langle \{\text{wiek}\}, \{delta\}, \{negatedEuclidean\} \right\rangle$$
$$C^3 = \left\langle A^3, D^3, P^3 \right\rangle = \left\langle \{\text{uczelnia,zawód}\}, \{maxSubstring\}, \{negatedEuclidean\} \right\rangle$$
$$C^4 = \left\langle A^4, D^4, P^4 \right\rangle = \left\langle \{\text{plec}\}, \{compare\}, \{common\} \right\rangle.$$

Definicje miar podobieństwa między węzłami i atrybutami węzłów w każdym kontenerze są następujące:

$$d_1^k(a,b) = compare(a,b) = \begin{cases} 1 & \text{gdy a=b} \\ 0 & \text{w przeciwnym przypadku} \end{cases}, \text{dla } k = 1,4 \tag{8}$$

$$d_1^k(a,b) = delta(a,b) = 1 - \frac{|a-b|}{\max(a,b)}, \text{dla } k = 2 \tag{9}$$

$$d_1^k(a,b) = maxSubstring(a,b), \text{dla } k = 3 \tag{10}$$

$$p_1^k(x,y) = \begin{cases} common_1^k(x,y) = \dfrac{\sum_{i \in A^k} d_*^{ik}\left(a_i(x), a_i(y)\right)}{n^k}, \text{dla } k = 1,4 \\ negatedEuclidean_1^k(x,y) = 1 - \dfrac{\sqrt{\sum_{i \in A^k} \left(1 - d_*^{ik}(a_i(x), a_i(y))\right)^2}}{n^k}, \text{dla } k = 2,3 \end{cases} \tag{11}$$

```
maxSubstring(x, y) = {
  result=0;
  for(i=0;i<min(length(x),length(y));i++){
    if(x[i]=y[i]){
      result++;
    }else{
      break;
    }
  }

  return result/min(length(x),length(y));
}
```

$\alpha^1 = 0.25,\ \alpha^2 = 0.25,\ \alpha^3 = 0.25,\ \alpha^4 = 0.25$

$w_0 = 5,\ t_{ID} = 0.7,\ t_s = 0.5$

Wyznaczając wartości *ID*, otrzymujemy:

$$ID(1,5) = 0.555,\ ID(2,5) = 0.25,\ ID(3,5) = 0.468,\ ID(4,5) = 0.725,$$
$$ID(5',5) = 0.905,\ ID(6,5) = 0.444,\ ID(7,5) = 0.722,\ ID(8,5) = 0.741,$$
$$ID(9,5) = 0.379,\ ID(10,5) = 0.204$$

Dla przykładu:

$$ID(5',5) = \sum_{k=1}^{4} \alpha^k p_*^k(5',5) = \alpha^1 p_*^1(5',5) + \alpha^2 p_*^2(5',5) + \alpha^3 p_*^3(5',5) + \alpha^4 p_*^4(5',5) =$$
$$= 0.25 \cdot 0.66 + 0.25 \cdot 0.96 + 0.25 \cdot 1 + 0.25 \cdot 1 = 0.905$$

gdyż

$$p_*^1(5',5) = \max_{i=1,p^k} p_i^1(5',5) = p_1^1(5',5)$$

oraz zgodnie z (11)

$$p_1^1(5',5) = common_1^1(5',5) = \frac{\sum_{i \in A^1} d_*^{i,1}\left(a_i(5'), a_i(5)\right)}{n^1} =$$
$$= \frac{d_*^{imie,1}\left(a_{imie}(5'), a_{imie}(5)\right) + d_*^{nazwisko,1}\left(a_{nazwisko}(5'), a_{nazwisko}(5)\right) + d_*^{e-mail,1}\left(a_{e-mail}(5'), a_{e-mail}(5)\right)}{n^1} =$$
$$= \frac{d_1^1\left(Michal, Michal\right) + d_1^1\left(Zabielski, Zabielski\right) + d_1^1\left(mz@op.pl, mzabielski@wat.edu.pl\right)}{3} =$$
$$= \frac{1+1+0}{3} = \frac{2}{3} = 0.66$$
$$p_*^2(5',5) = \max_{i=1,p^k} p_i^2(5',5) = p_1^2(5',5)$$

oraz zgodnie z (11)

$$p_1^2(5',5) = negatedEuclidean_1^2(5',5) = 1 - \frac{\sqrt{\sum_{i \in A^2}\left(1 - d_*^{i2}(a_i(x), a_i(y))\right)^2}}{n^2} =$$
$$= 1 - \frac{\sqrt{\left(1 - d_1^2(26,27)\right)^2}}{n^2} = 1 - \frac{\sqrt{\left(1 - \left(1 - \frac{|26-27|}{\max(26,27)}\right)\right)^2}}{n^2} = 1 - \frac{\sqrt{(1/27)^2}}{1} \approx 0.96$$
$$p_*^3(5',5) = \max_{i=1,p^k} p_i^3(5',5) = p_1^3(5',5)$$

oraz zgodnie z (11)

$$p_1^3(5',5) = negatedEuclidean_1^3(5',5) = 1 - \frac{\sqrt{\sum_{i\in A^3}\left(1 - d_*^{i3}(a_i(x), a_i(y))\right)^2}}{n^3} =$$

$$= 1 - \frac{\sqrt{\left(1 - d_1^3(WAT, WAT)\right)^2 + \left(1 - d_1^3(Informatyk, Informatyk)\right)^2}}{n^3} =$$

$$= 1 - \frac{\sqrt{0+0}}{n^3} = 1 - \frac{0}{1} = 1$$

$$p_*^4(5',5) = \max_{i=1,p^k} p_i^4(5',5) = p_1^4(5',5)$$

oraz zgodnie z (11)

$$p_1^4(5',5) = common_1^4(5',5) = \frac{\sum_{i\in A^4} compare\left(a_i(5'), a_i(5)\right)}{n^4} = \frac{\sum_{i\in A^4} d_*^{i4}\left(a_i(5'), a_i(5)\right)}{n^4} =$$

$$= \frac{d_1^4\left(a_{plec}(5'), a_{plec}(5)\right)}{n^4} = \frac{d_1^4\left(M, M\right)}{1} = \frac{1}{1} = 1$$

Mamy wtedy:

$$H = \left\{y \in W : ID\left(y, w_0\right) \geq t_{ID}\right\} = \left\{4,5',7,8\right\} \quad dla \quad t_{ID} = 0.7.$$

Kolejnym krokiem jest wyznaczenie wspólnych sąsiadów wierzchołków ze zbioru H i wzorca w_0.

Dla $h = 4$:

$$N_4 = \left\{5,5',6,7,8\right\},\ s_5^4 = 1$$

Dla $h = 5'$:

$$N_{5'} = \left\{2,4,6,9\right\},\ s_5^{5'} = 3$$

Dla $h = 7$:

$$N_7 = \left\{4,5\right\},\ s_5^7 = 1$$

Dla $h = 8$:

$$N_8 = \left\{4,6\right\},\ s_5^8 = 1$$

Dla tak wyznaczonych wielkości otrzymujemy następujące wartości podobieństwa sąsiedztwa:

$$\frac{s_5^4}{\left|N_4 \cup N_5\right|} = \frac{1}{6} \approx 0.167 < t_S$$

$$\frac{s_5^{5'}}{\left|N_{5'} \cup N_5\right|} = \frac{3}{6} = 0.5 \geq t_S$$

$$\frac{s_5^7}{\left|N_7 \cup N_5\right|} = \frac{1}{6} \approx 0.167 < t_S$$

$$\frac{s_5^8}{\left|N_8 \cup N_5\right|} = \frac{1}{6} \approx 0.167 < t_S$$

Na tej podstawie:

$$K = \{5'\}.$$

Przedstawiony przykład nie uwzględniał kalibracji istotności kontenerów. Gdyby ustalić przykładowe wartości istotności jako następujące: $\alpha_1 = 0{,}5$, $\alpha_2 = 0{,}1$, $\alpha_3 = 0{,}3$, $\alpha_4 = 0{,}1$, to już na etapie badania podobieństwa węzłów dostalibyśmy:

$$ID(1,5) = 0.354,\ ID(2,5) = 0.1,\ ID(3,5) = 0.319,\ ID(4,5) = 0.49,$$
$$ID(5',5) = 0.83,\ ID(6,5) = 0.178,\ ID(7,5) = 0.489,\ ID(8,5) = 0.496,$$
$$ID(9,5) = 0.152,\ ID(10,5) = 0.081.$$

Wtedy:

$$H = \left\{y \in W : ID(y, w_0) \geq t_{ID}\right\} = \{5'\} \quad dla \quad t_{ID} = 0.7$$

Widać więc, że możliwość nadawania kontekstu danym z wykorzystaniem kontenerów podobieństwa może mieć znaczący wpływ na zmniejszenie przestrzeni węzłów do dalszych działań, co przekłada się znacząco na szybkość działania.

Przedstawiona metoda nie ogranicza się jedynie do wykrywania sklonowanych profili użytkowników w ISS. Może mieć zastosowanie wszędzie tam, gdzie zależy nam na wykryciu podobnych elementów z jednoczesnym uwzględnieniem struktury powiązań między nimi. Byłaby ona zatem użyteczna dla takich zadań jak np.:

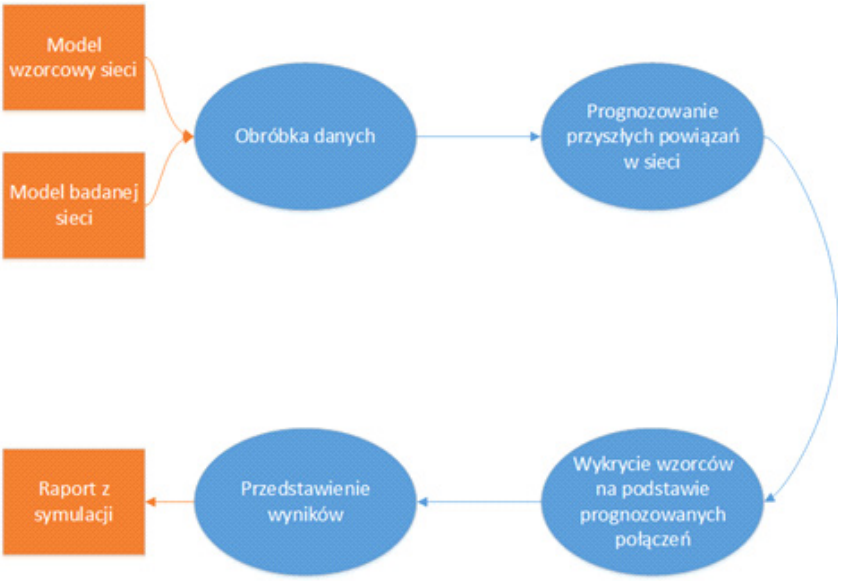
- wykrywanie profili tej samej osoby w ISS;
- systemy rekomendacyjne (na przykład podpowiadanie zamienników dla produktów, wskazywanie potencjalnych klientów);
- wyszukiwanie tworzących się społeczności o profilu zbliżonym do podanego wzorca (np. szukanie tworzącej się na nowo sieci przestępczej na podstawie poprzedniej struktury);

— wyszukiwanie osób o podobnym profilu aktywności w firmie (ten sam networking i kompetencje);
— odkrywanie nieznanych wartości atrybutów profilu użytkownika.

4. Idea symulatora do wykrywania klonowania profili użytkowników

Przedstawiona metoda badania podobieństwa profili użytkowników w ISS pozwala na wykrywanie faktu podszywania się pod tożsamość użytkownika w sytuacji, gdy do klonowania profilu już dojdzie. Ciekawym rozszerzeniem metody byłoby umożliwienie wykrywania faktu klonowania, zanim zostanie to wykonane. Chodzi tu o sytuację, w której atakujący postanowił sklonować profil ofiary i zaczął budować jej tożsamość.

W oparciu o taką ideę powstała koncepcja środowiska symulacyjnego, w którym na podstawie modelu zawierania znajomości, opisanym na przykład w [15], możliwe byłoby symulowanie w czasie tworzenia się znajomości w badanej ISS. W każdym kroku symulacyjnym aplikowana byłaby metoda badania podobieństwa profili użytkowników opisana w rozdziale 3. Jeśli doszłoby do wykrycia faktu sklonowania tożsamości ofiary, informacja wraz z chwilą czasową zajścia tego zdarzenia zostałaby zapisana w raporcie końcowym. Na tej podstawie uzyskalibyśmy informację, czy jakiś profil jest w trakcie klonowania w sieci rzeczywistej i w jakim stadium procesu odtwarzania tożsamości znajduje się atakujący. Schematycznie przedstawia to rysunek 2.



Rys. 2. Schemat działania proponowanego symulatora
Źródło: opracowanie własne

Proponowane rozwiązanie umożliwiłoby wykrywanie procesu klonowania profili użytkowników, co pozwoliłoby na zminimalizowanie znaczenia jednego z powszechnie wykorzystywanych mechanizmów naruszania prywatności we współczesnych ISS.

5. Podsumowanie

W pracy przedstawiona została autorska, adaptacyjna metoda badania podobieństwa profili użytkowników w ISS. Omawiana metoda, mimo swojej przewagi nad innymi znanymi z literatury, o których pisano wcześniej, wciąż zawiera obszary, które można udoskonalić, aby zwiększyć jej skuteczność i użyteczność, czego dowodem jest zaproponowana koncepcja symulatora. Innym elementem, który zwiększyłby aplikowalność rozpatrywanej techniki, byłaby możliwość zautomatyzowania procesu tworzenia kontenerów podobieństwa w oparciu o wprowadzone dane ISS. Trwają również prace nad uwzględnieniem różnych rodzajów miar podobieństwa atrybutów oraz zastosowaniem podejścia wielokryterialnego do badania podobieństwa węzłów, co mogłoby przyczynić się do zwiększenia elastyczności modelu.

Praca finansowana z Pracy Badawczej Statutowej 871/2018 Instytutu Systemów Informatycznych Wydziału Cybernetyki WAT.

Artykuł opracowany na podstawie referatu pt. *Metoda prognozowania klonowania profili w internetowych sieciach społecznych* wygłoszonego na Warsztatach PTSK (Polskie Towarzystwo Symulacji Komputerowej), Szymbark, 20-23 maja 2015 r.

Artykuł wpłynął do redakcji 10.05.2018 r. Zweryfikowaną wersję po recenzjach otrzymano 27.03.2019 r.

Zbigniew Tarapata https://orcid.org/0000-0001-8143-7869

Rafał Kasprzyk https://orcid.org/0000-0002-4938-1874

LITERATURA

[1] Barnes J.A., Class and Committees in a Norwegian Island Parish, Human Relations, vol. 7, 1, 1954, pp. 39-58.

[2] He J., Chu W.W., Liu Z., *Inferring Privacy Information from Social Networks*, International Conference on Intelligence and Security Informatics ISI 2006, Lecture Notes in Computer Science, vol. 3975, 2006, pp. 154-165.

[3] Nabeth T., *Understanding the identity concept in the context of digital social environments*, CALT-FIDIS working paper, January 2005.

[4] Mo M., Wang D., Li B., Hong D., King I., *Exploit of Online Social Networks with Semi-Supervised Learning*, International Conference on Neural Information Processing ICONIP 2010: Neural Information Processing. Theory and Algorithms, Lecture Notes in Computer Science, vol. 6443, 2010, pp. 669-678.

[5] Xiaojin Z., Ghahramani Z, Lafferty J.D., Semi-supervised learning using gaussian fields and harmonic functions, Proceedings of the 20th International Conference on Machine Learning (ICML-03), August 21-24, Washington DC, USA, 2003.

[6] Burattin A., Cascavilla G., Conti M., Socialspy: Browsing (supposedly) hidden information in online social networks, International Conference on Risks and Security of Internet and Systems, CRiSIS 2014: Risks and Security of Internet and Systems, Lecture Notes in Computer Science, vol. 8924, 2014, pp. 83-99.

[7] Özgür K., Günay A., Yolum P., Protoss: A run time tool for detecting privacy violations in online social networks, Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on. IEEE, 2012.

[8] Khayyambashi M., Fatemeh S.R., An approach for detecting profile cloning in online social networks, E-Commerce in Developing Countries: With Focus on E-Security (ECDC), 2013 7th Intenational Conference on. IEEE, 2013.

[9] Kharaji M.Y., Fatemeh S.R., An IAC Approach for Detecting Profile Cloning in Online Social Networks, arXiv preprint arXiv:1403.2006, 2014.

[10] Ali M., Ibrahim H., Torky M., A Framework for Detecting Cloning Attacks in OSN Based on a Novel Social Graph Topology, International Journal of Intelligent Systems and Applications, vol. 7, no. 3, 2015, pp. 13-20.

[11] Ali M., Ibrahim H., Torky M., Identity Verification Mechanism for Detecting Fake Profiles in Online Social Networks, International Journal of Computer Network and Information Security, vol. 9, 2017, pp. 31-39.

[12] Zabielski M., Kasprzyk R., Tarapata Z., Szkółka K., Methods of Profile Cloning Detection in Online Social Networks, [in:] Proceedings of the 20th International Conference on Circuits, Systems, Communications and Computers (CSCC 2016), Corfu Island (Greece), July 14-17, 2016.

[13] Zabielski M., Tarapata Z., Kasprzyk R., Szkółka K., Profile Cloning Detection in Online Social Networks, Computer Science and Mathematical Modelling, vol. 3, 2016, pp. 39-46.

[14] Choi S., Cha S., Tappert C., A Survey of Binary Similarity and Distance Measures, Systemics, Cybernetics and Informatics, vol. 8, 2010, pp. 43-48.

[15] Liben-Nowell D., Kleinberg J., The Link-Prediction Problem for Social Networks, Journal of the American Society for Information Science and Technology, New Orleans, LA, USA — November 3-8, 2003, pp. 556-559.

M. ZABIELSKI, Z. TARAPATA, R. KASPRZYK

Adaptive method of similarity detection of user profiles on Online Social Networks

Summary. The paper presents a method, based on graph and network theory, which allows to detect cloned user profiles on Online Social Networks. Moreover, an idea of similarity containers, which gives an opportunity to incorporate importance and context of data into a model, was introduced. The presented solutions were adapted to the idea of simulation environment, which will allow to detect a profile cloning process before that activity will be completely performed by an attacker.

Keywords: *Online Social Networks*, user profile cloning, violation of privacy on the web
DOI: 10.5604/01.3001.0013.3002