To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles

E. Zheleva, L. Getoor.
Department of Computer Science
University of Maryland

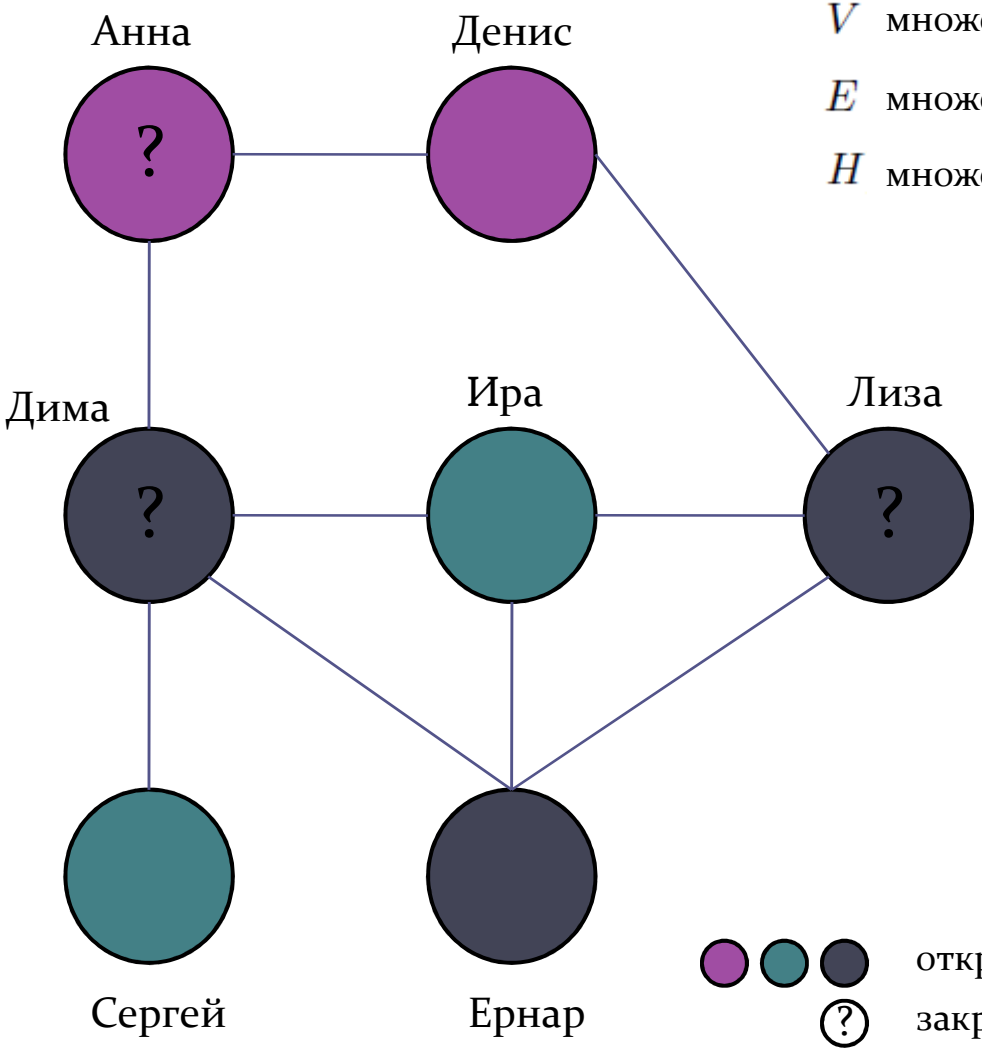
Presentation by N. Levitskiy

Цели работы

- Рассмотреть проблему приватности в социальных сетях
- Разобрать методы получения приватной информации
- Показать преимущество методов, использующих информацию о принадлежности к группам
- Предложить возможные варианты решения проблемы

Представление сети в виде графа $G = (V, E, H)$

Схема дружеских связей

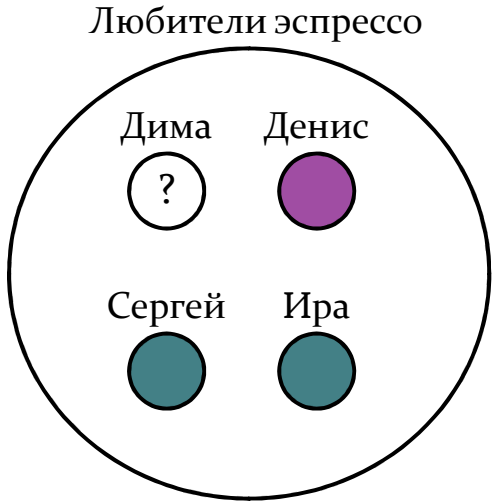


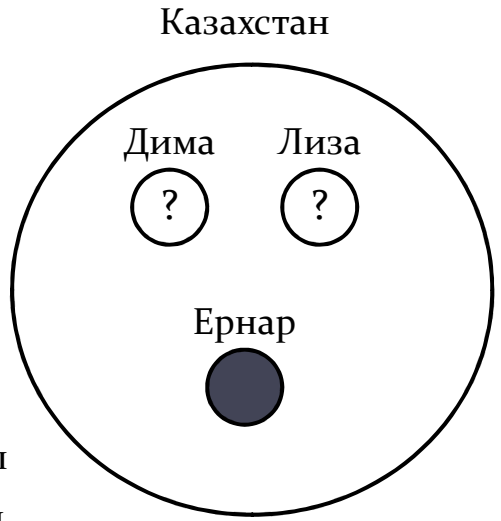
V множество узлов

E множество ребер

H множество групп

Группы в социальных сетях





открытые аккаунты

закрытые аккаунты

Цвет обозначает принадлежность к классу

Основные обозначения

V_s - множество приватных аккаунтов

V_o - множество открытых аккаунтов

$V_s.A$ - скрытые параметры приватных аккаунтов

$$v_s.\hat{a}_M = \underset{a_i}{\operatorname{argmax}} P_M(v_s.a = a_i; G).$$

$P_M(v_s.a = a_i; G)$ - вероятность того, что значение скрытого атрибута приватного аккаунта равно a_i

Методы без использования связей и принадлежности к группам

BASIC

Известны только возможные значения скрытых параметров из открытых профилей

$$P_{BASIC}(v_s.a = a_i; G) = P(v_s.a = a_i | V_o.A) = \frac{|V_o.a_i|}{|V_o|},$$

$|V_o.a_i|$ - число открытых аккаунтов с признаком a_i

$|V_o|$ - общее число открытых аккаунтов

Методы использующие связи

Friend-aggregate model (AGG)

Известны друзья профиля (V_o'). Рассматриваются только открытые профили.

$$P_{AGG}(v_s.a = a_i; G) = P(v_s.a = a_i | V_o.A, E) = \frac{|V_o'.a_i|}{|V_o'|}$$

where $V_o' = \{v_o \in V_o | \exists (v_s, v_o) \in E\}$ and $V_o'.a_i = \{v_o \in V_o' | v_o.a = a_i\}$.

Collective classification model (CC)

Модель использует не только связи между открытыми профилями и рассматриваем. Но также и связи между приватными профилями.

Методы использующие связи

Flat-link model (LINK)

Используется матрица смежности графа. У каждого пользователя в строке записаны бинарные признаки, отвечающие значениям скрытого параметра. Ставится единица, если у пользователя есть друзья с этим.

Blockmodeling attack (BLOCK)

Пользователи делятся на блоки в зависимости от значения скрытого атрибута. Рассматриваем связи между блоками.

$$P_{BLOCK}(v_s.a_i; G) = P(v_s.a_i | V_o.A, E, \lambda) = \frac{1}{Z} sim(\lambda_i, \lambda(v))$$

$sim()$ - функция сходства

λ_i - вектор связей блока с индексом i с другими блоками

$\lambda(v)$ - Вектор связей пользователя с блоками

Методы использующие принадлежность к группам

Groupmate-link model (CLIQUE)

Каждая группа рассматривается как клика друзей. Далее применяется один из методов, основанных на связях.

Group-based classification model (GROUP)

Каждая группа рассматривается как признак для классификатора. Но нужно выделять группы, которые будут действительно полезны.

$$Entropy(h) = -\sum_{i=1}^{m} p(a_i)\log_2 p(a_i) \qquad p(a_i) = \frac{|h.V.a_i|}{|h.V|}$$

Энтропия вводится для измерения однородности группы.

Этот метод состоит из трех шагов:

1. Выделяются значимые группы
2. Классификатор обучается на открытых аккаунтах
3. Определяются значения скрытых параметров для приватных аккаунтов

LINK-GROUP

Смешанный метод. Использует связи и группы как признаки.

Результаты эксперимента

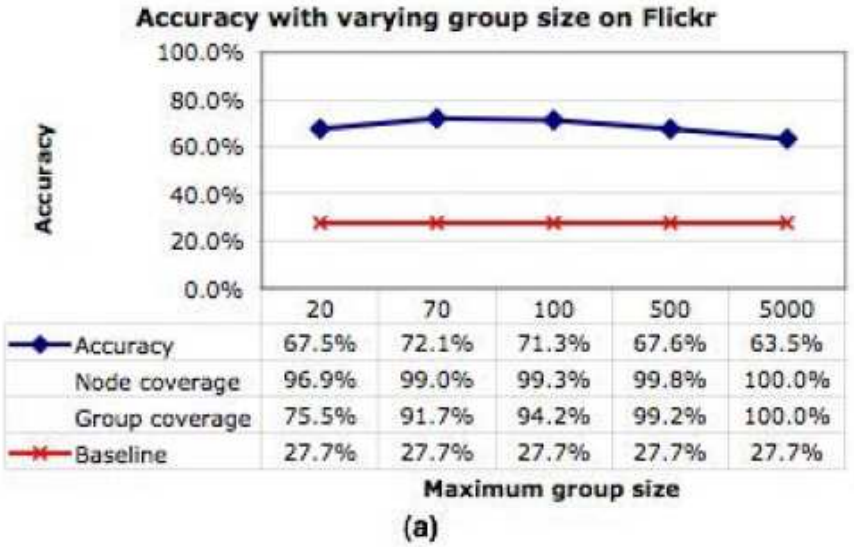
Table 1: Properties of the four datasets.

PROPERTY	FLICKR	FACEBOOK	DOGSTER	BIBSONOMY
Number of users	9,179	1,598/965	2,632	31,715
Number of links	941,677	86,007/33,597	4,482	N/A
Number of groups	47,754	2,932/2,497	1,042	132,554
Average in-sample degree	142	108/70	1	N/A
Average number of groups per user	162	24/25	1	98
Average group size	31	10/9	3	9
Largest group size	4,527	290/221	118	7,182
Percent links between nodes with the same label	23.5%	49.9%/40.3%	-	N/A
Number of possible labels	55	2/6	7	2
Sensitive attribute	*location*	*gender/polviews*	*breed category*	*spammer*

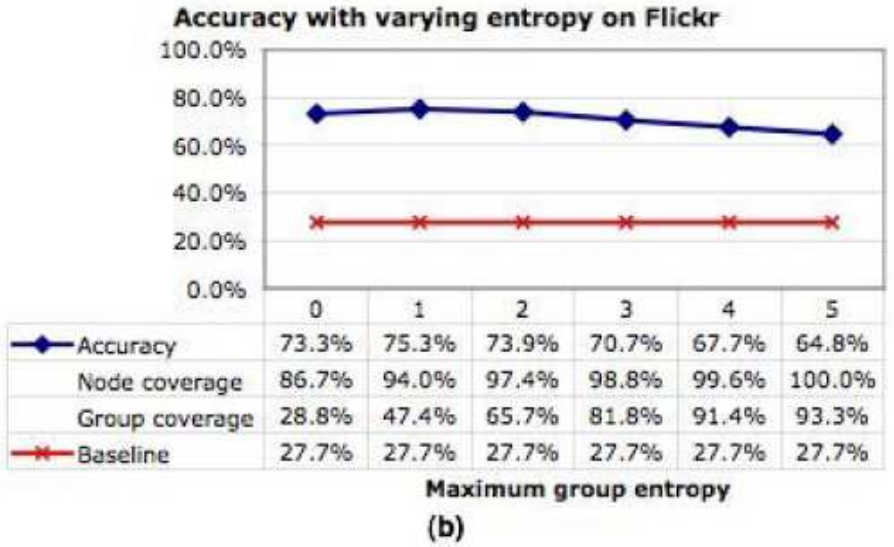
Table 2: Attack accuracy assuming 50% private profiles. The successful attacks are shown in bold.

ATTACK MODEL	FLICKR	FACEBOOK (GENDER)	FACEBOOK (POLVIEWS)	DOGSTER	BIBSONOMY
BASIC	27.7%	50.0%	56.5%	28.6%	92.2%
Random guess	1.8%	50.0%	16.7%	14.3%	50%
BLOCK	8.8%	49.1%	6.1%	-	-
AGG	28.4%	50.2%	57.6%	-	-
CC	28.6%	50.4%	56.3%	-	-
LINK	**56.5%**	**68.6%**	58.1%	-	-
CLIQUE-LINK	**46.3%**	51.8%	57.1%	**60.2%**	-
GROUP	**63.5%**	**73.4%**	45.2%	**65.5%**	**94.0%**
GROUP (50% node coverage)	**83.6%**	**77.2%**	46.6%	**82.0%**	**96.0%**
LINK-GROUP	**64.8%**	**72.5%**	57.8%	-	-

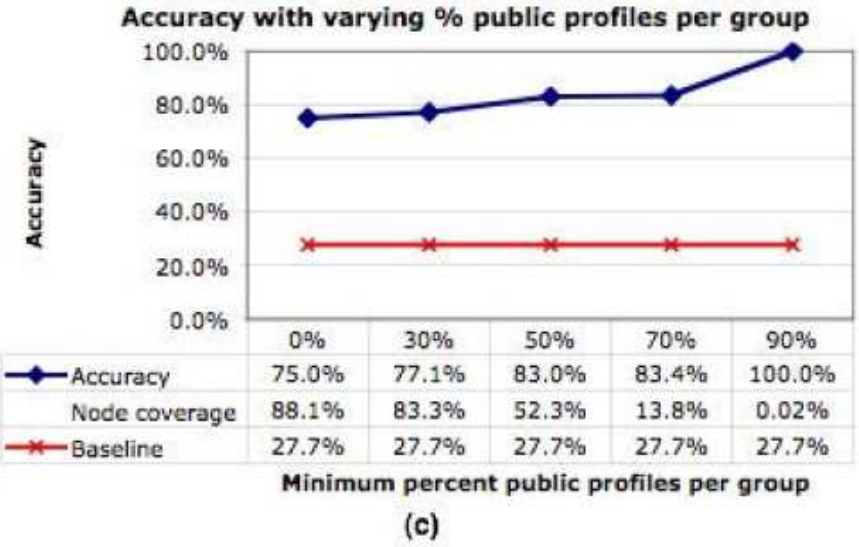
Результаты эксперимента



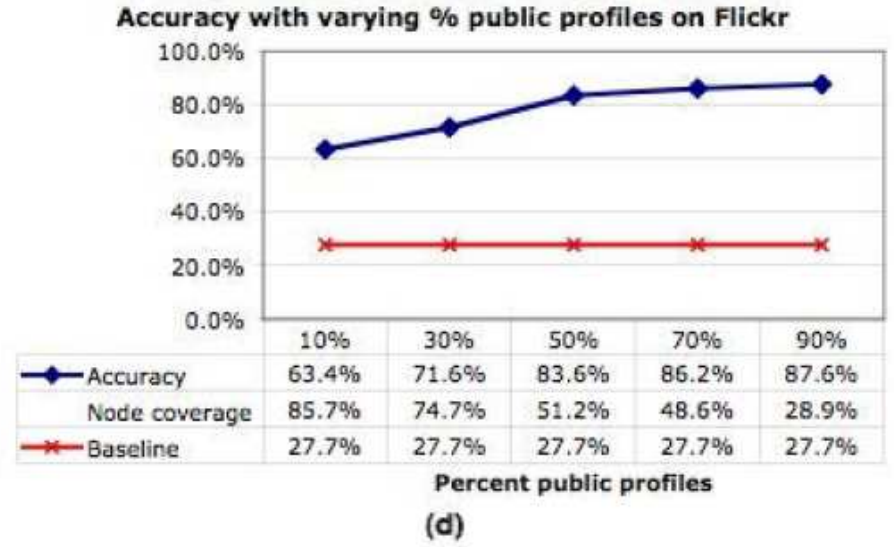
	20	70	100	500	5000
Accuracy	67.5%	72.1%	71.3%	67.6%	63.5%
Node coverage	96.9%	99.0%	99.3%	99.8%	100.0%
Group coverage	75.5%	91.7%	94.2%	99.2%	100.0%
Baseline	27.7%	27.7%	27.7%	27.7%	27.7%



	0	1	2	3	4	5
Accuracy	73.3%	75.3%	73.9%	70.7%	67.7%	64.8%
Node coverage	86.7%	94.0%	97.4%	98.8%	99.6%	100.0%
Group coverage	28.8%	47.4%	65.7%	81.8%	91.4%	93.3%
Baseline	27.7%	27.7%	27.7%	27.7%	27.7%	27.7%



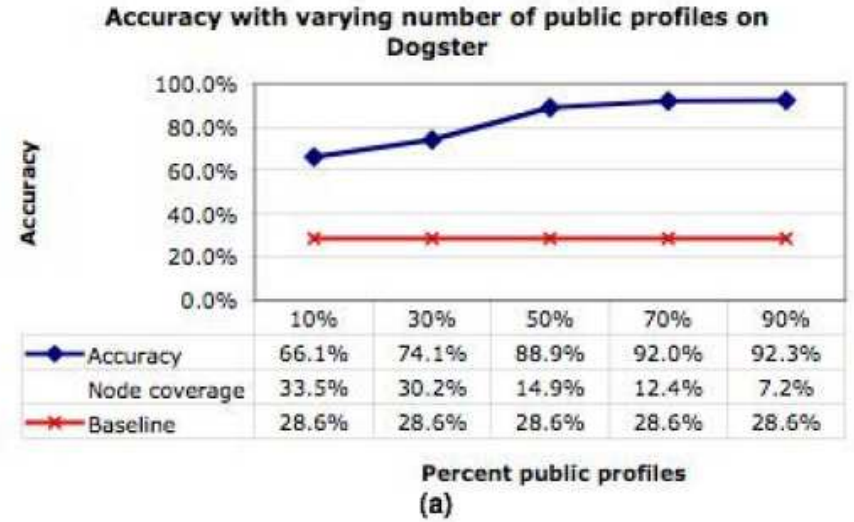
	0%	30%	50%	70%	90%
Accuracy	75.0%	77.1%	83.0%	83.4%	100.0%
Node coverage	88.1%	83.3%	52.3%	13.8%	0.02%
Baseline	27.7%	27.7%	27.7%	27.7%	27.7%



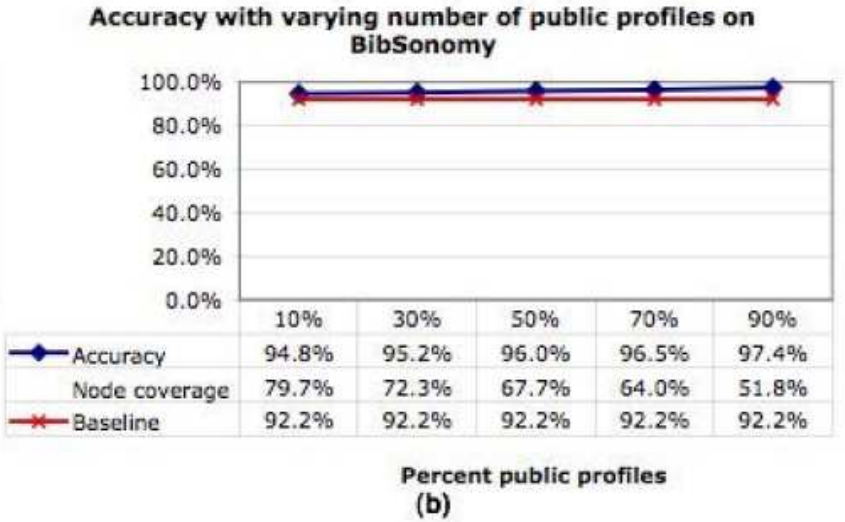
	10%	30%	50%	70%	90%
Accuracy	63.4%	71.6%	83.6%	86.2%	87.6%
Node coverage	85.7%	74.7%	51.2%	48.6%	28.9%
Baseline	27.7%	27.7%	27.7%	27.7%	27.7%

Результаты эксперимента

	0	1	2	3	4	5
Accuracy	65.2%	57.7%	50.4%	40.0%	20.3%	0.0%
Node coverage	100.0%	99.8%	99.5%	99.1%	96.8%	0.0%
Group coverage	92.9%	56.6%	29.6%	11.9%	1.6%	0.0%
Baseline	27.7%	27.7%	27.7%	27.7%	27.7%	27.7%



	10%	30%	50%	70%	90%
Accuracy	66.1%	74.1%	88.9%	92.0%	92.3%
Node coverage	33.5%	30.2%	14.9%	12.4%	7.2%
Baseline	28.6%	28.6%	28.6%	28.6%	28.6%



	10%	30%	50%	70%	90%
Accuracy	94.8%	95.2%	96.0%	96.5%	97.4%
Node coverage	79.7%	72.3%	67.7%	64.0%	51.8%
Baseline	92.2%	92.2%	92.2%	92.2%	92.2%

Выводы

- Рассмотрена проблема приватности
- Показано, что методы, основанных на информации принадлежности к группам, имеют более высокую точность
- Получен способ повышения защищенности приватной информации аккаунта

Спасибо за внимание