

Fake Co-visitation Injection Attacks to Recommender Systems

Guolei Yang, Neil Zhenqiang Gong, Ying Cai



Co-visitation Recommender System is Popular

The screenshot shows an Amazon product page for a Sony Alpha Mirrorless camera. On the left, there's a video player with a thumbnail for a cat video and an 'Autoplay' toggle. Below the video, the product title is 'Sony Alpha Mirrorless with 16-50' and it has a 4.5-star rating and a price of \$1,048.00. The main content area features a heading 'Customers Who Viewed This Item Also Viewed' in orange. To the right of this heading are two large logos: 'amazon' on the left and 'ebay' on the right, each next to a grid of four Nike Air Force 1 shoes. The 'amazon' grid includes a red pair, a blue pair, a tan pair, and a maroon pair. The 'ebay' grid also includes a tan pair, a blue pair, a tan pair, and a maroon pair. Below each grid is a row of product details: the first row lists 'NikeLab NIKE AIR FORCE 1 LOW AF1 SHOES GYM...' for \$89.00 with free shipping; the second row lists 'Nike LAB Air Force 1 Low Mens Casual Shoes Sneaker' for \$94.99 plus \$20.00, labeled as 'Popular'; the third row lists 'SZ.9.5 Nike NikeLab Air Force 1 Low 555106-200...' for \$191.48 plus \$10.10; and the fourth row lists 'Nike LAB Air Force 1 Low Night Maroon Mens Casual' for \$99.99 plus \$20.00, also labeled as 'Popular'.

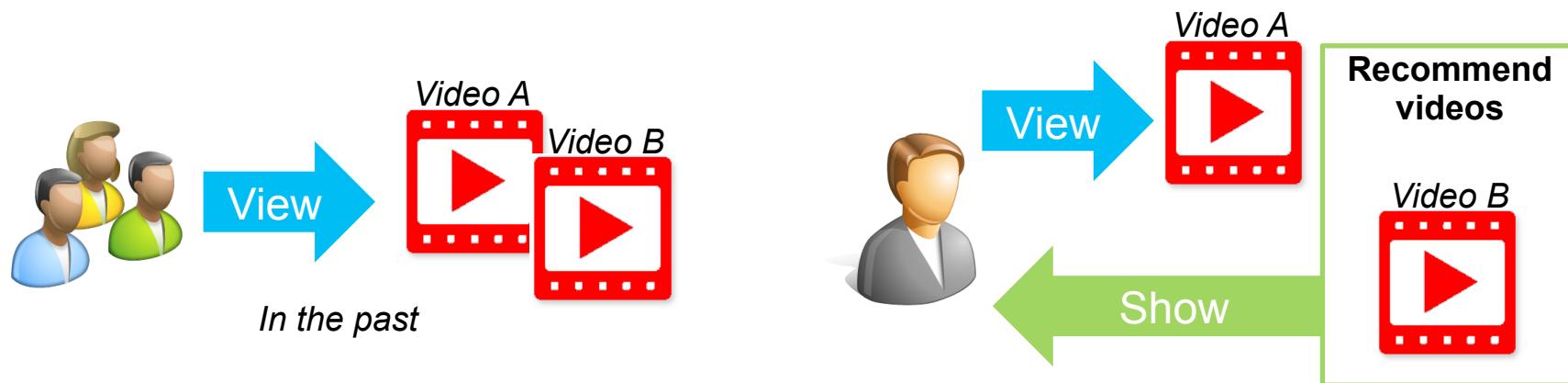
Product	Price	Condition	Shipping
NikeLab NIKE AIR FORCE 1 LOW AF1 SHOES GYM...	\$89.00	New	Free shipping
Nike LAB Air Force 1 Low Mens Casual Shoes Sneaker	\$94.99	New	+ \$20.00 Popular
SZ.9.5 Nike NikeLab Air Force 1 Low 555106-200...	\$191.48	New	+ \$10.10
Nike LAB Air Force 1 Low Night Maroon Mens Casual	\$99.99	New	+ \$20.00 Popular

We show co-visitation recommender systems can be spoofed to recommend items as an attacker desires



Brief Intro to Co-visitation Recommender System

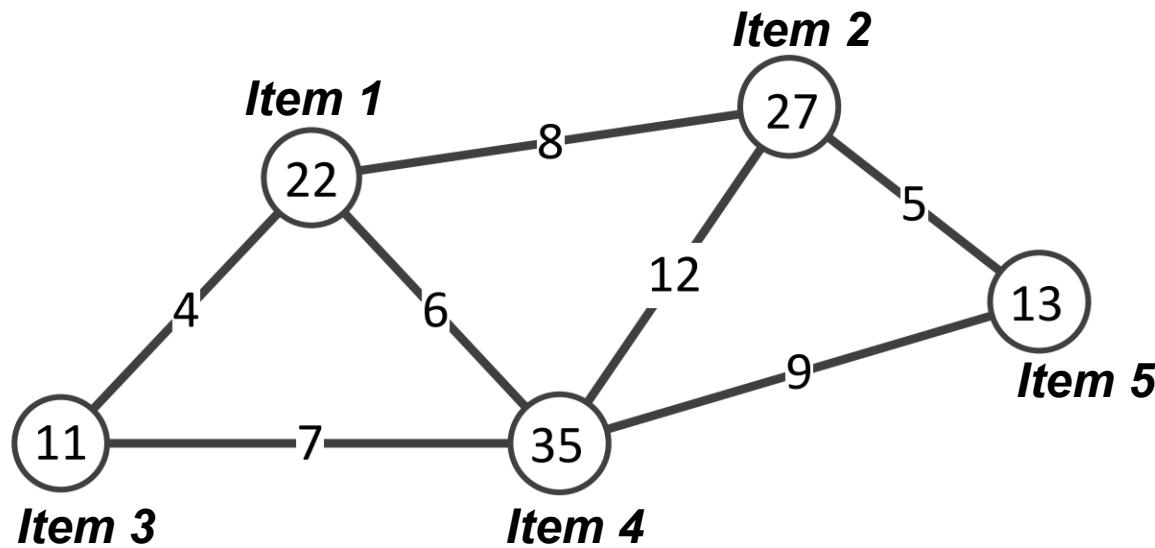
- Key idea: *Items that are frequently visited together in the past are likely to be visited together in the future*





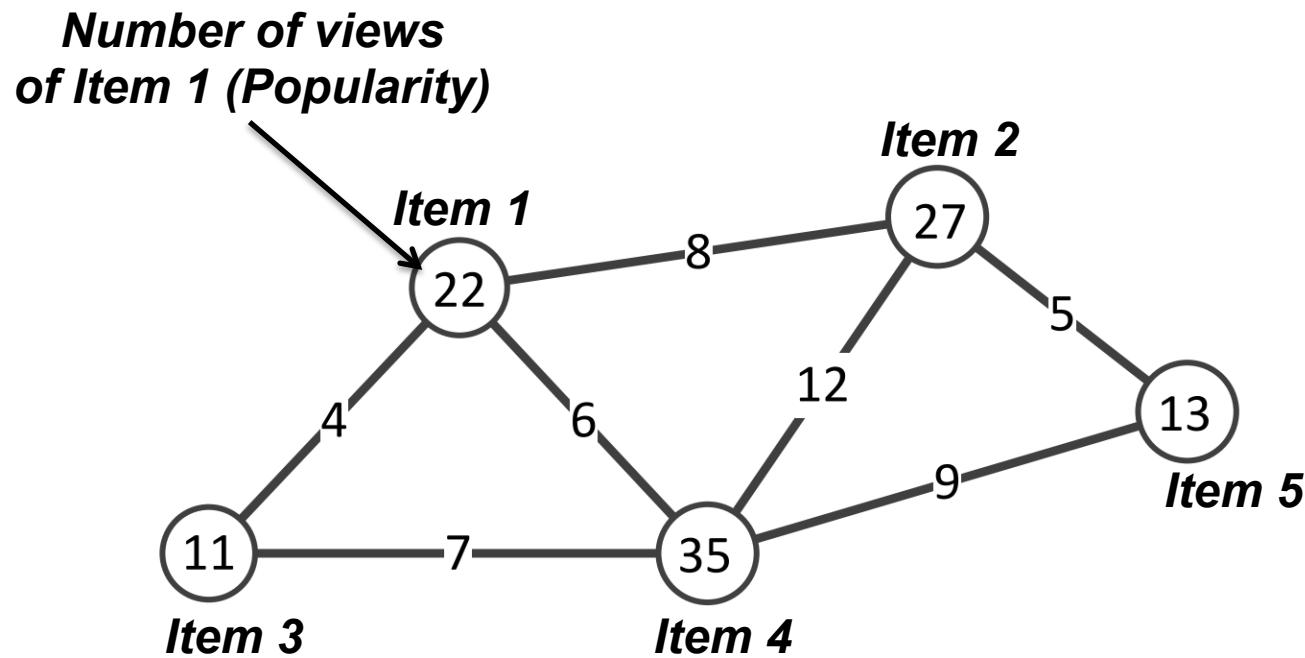
Key Data Structure: Co-visitation Graph

Each vertex represents an item





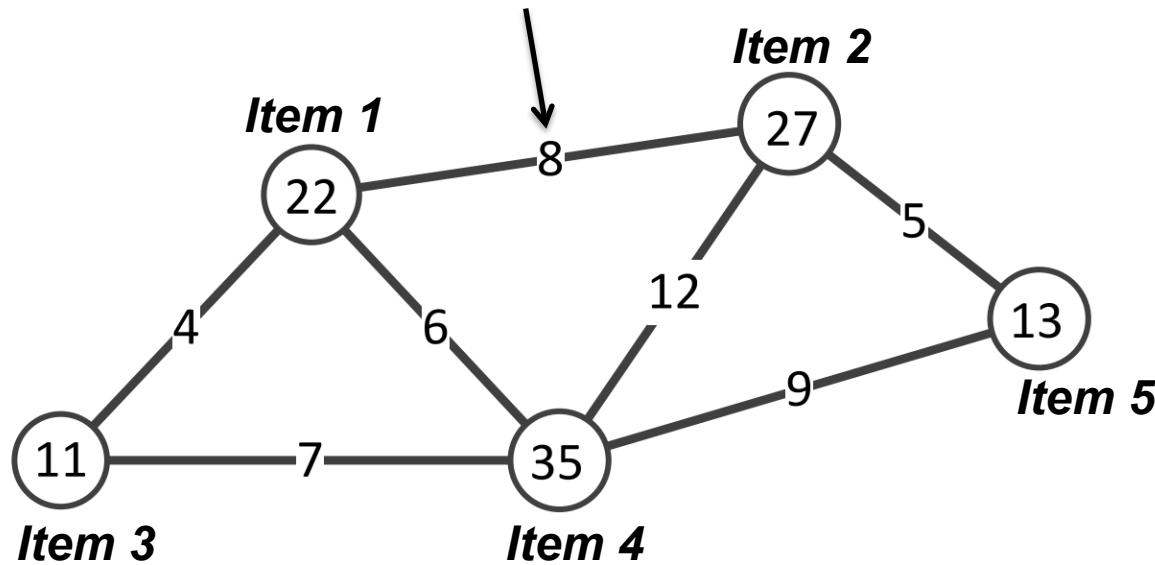
Key Data Structure: Co-visitation Graph





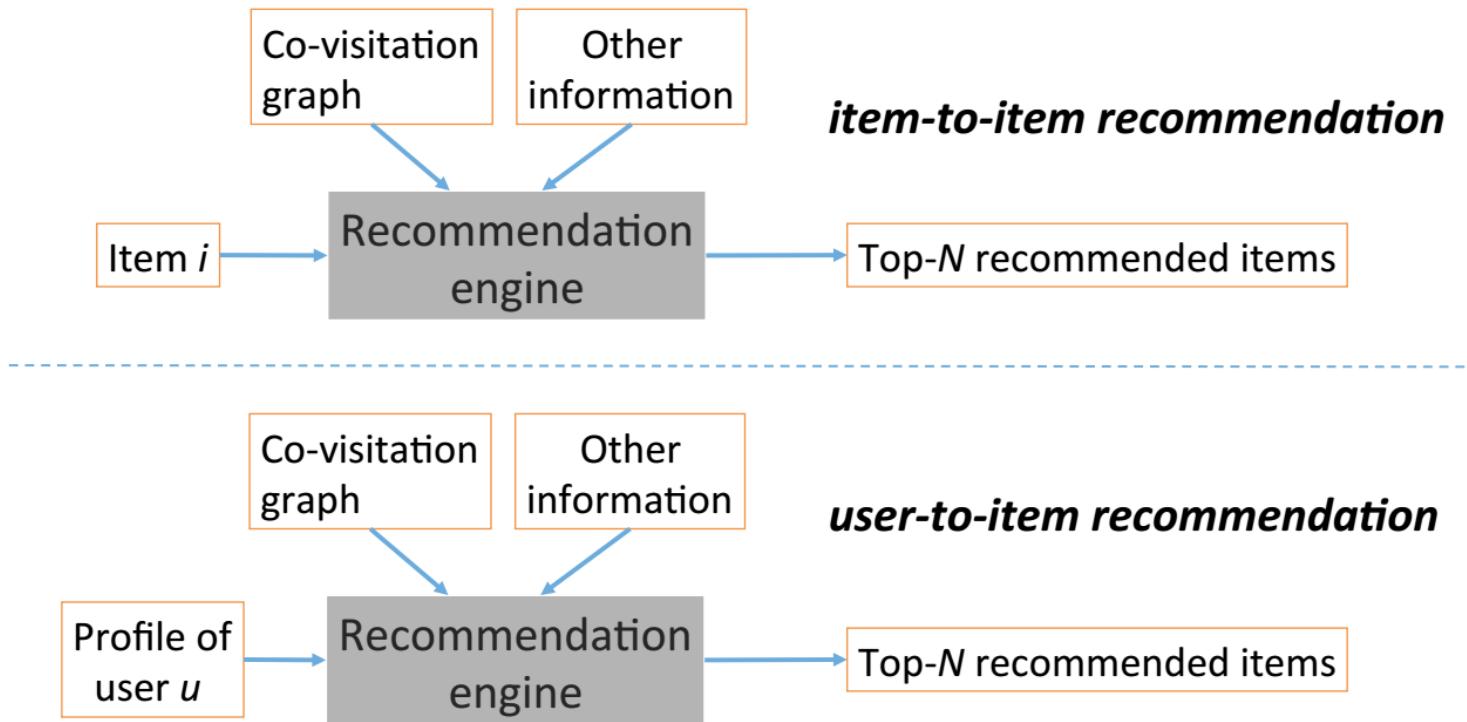
Key Data Structure: Co-visitation Graph

***Number of co-visitations
between Item 1 and 2***



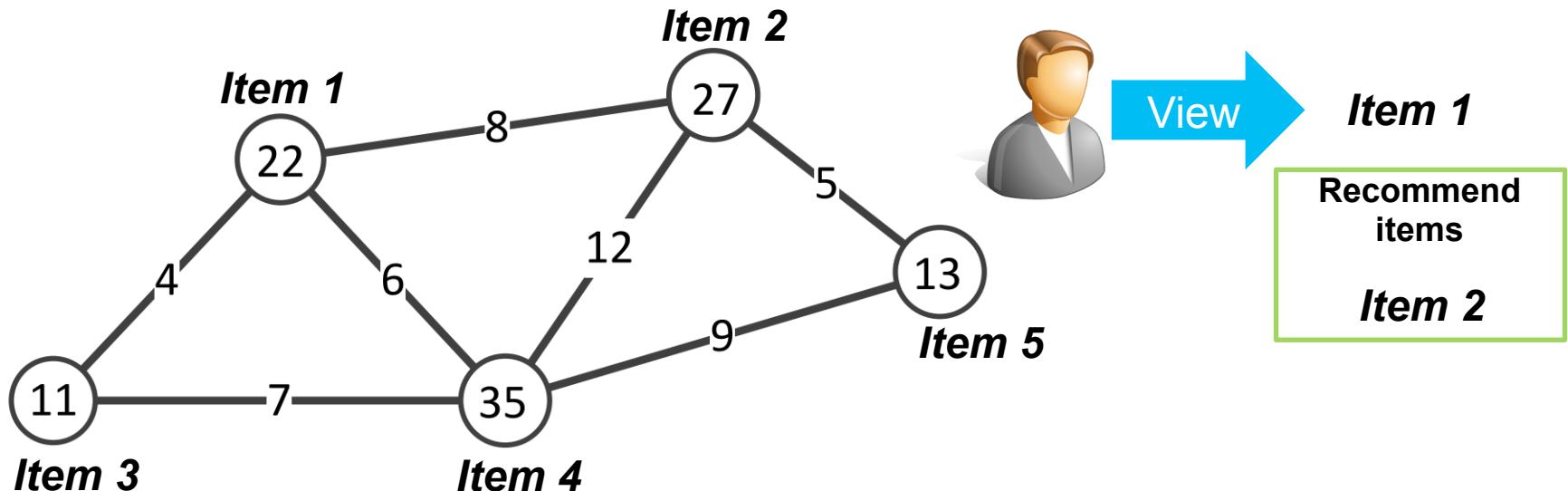
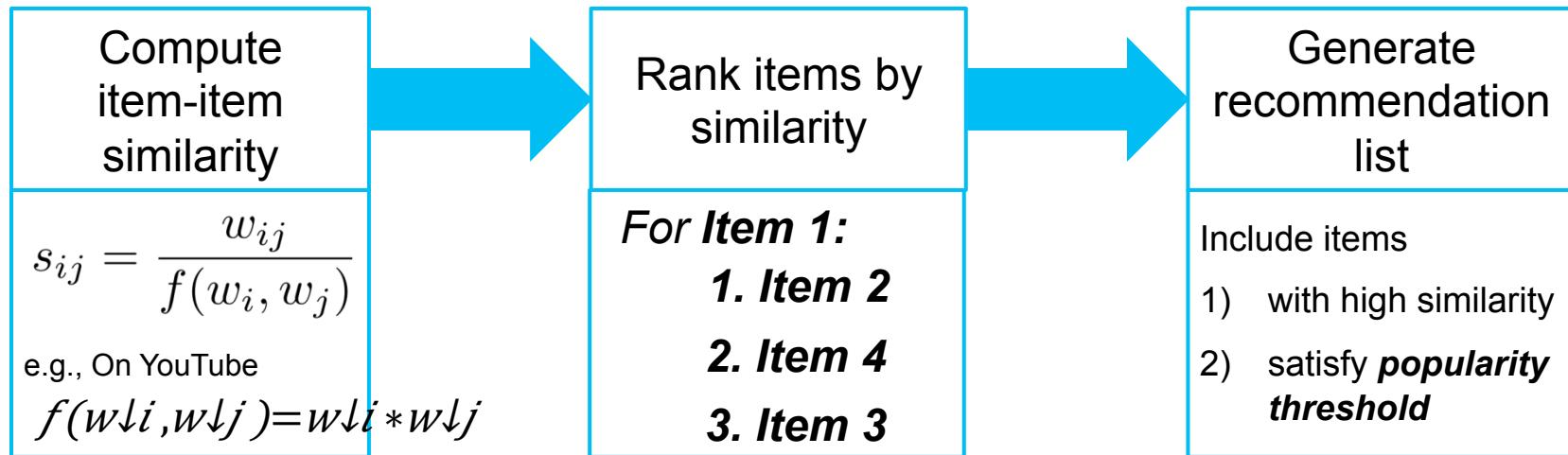


Two Recommendation Tasks





Item-to-Item Recommendation





Related Work

- Xing et al. (USENIX Security'13) proposed *pollution attacks* to the user-to-item recommendation
 - *Relies on Cross-Site Request Forgery (CSRF)*
 - *Not applicable to item-to-item recommendation*
- *Profile injection (Shilling) attacks* to recommender systems via user-item rating matrices
 - Not applicable to co-visitation recommender systems which do not rely on user-item rating matrix.
- Relationship to adversarial machine learning
 - Our attack is data poisoning attack to recommender systems



Roadmap

- Threat model
- Proposed attacks
- Evaluations on synthetic data
- Evaluations on real-world recommender systems
- Countermeasures



Threat Model

- Attacker's background knowledge

	High knowledge	Medium knowledge	Low knowledge
Knowledge	<i>Co-visitation Graph</i>	<i>Recommendation Lists</i>	<i>Recommendation Lists</i>
Scenario	<i>Insider</i>	<i>YouTube ...</i>	<i>Amazon, eBay...</i>

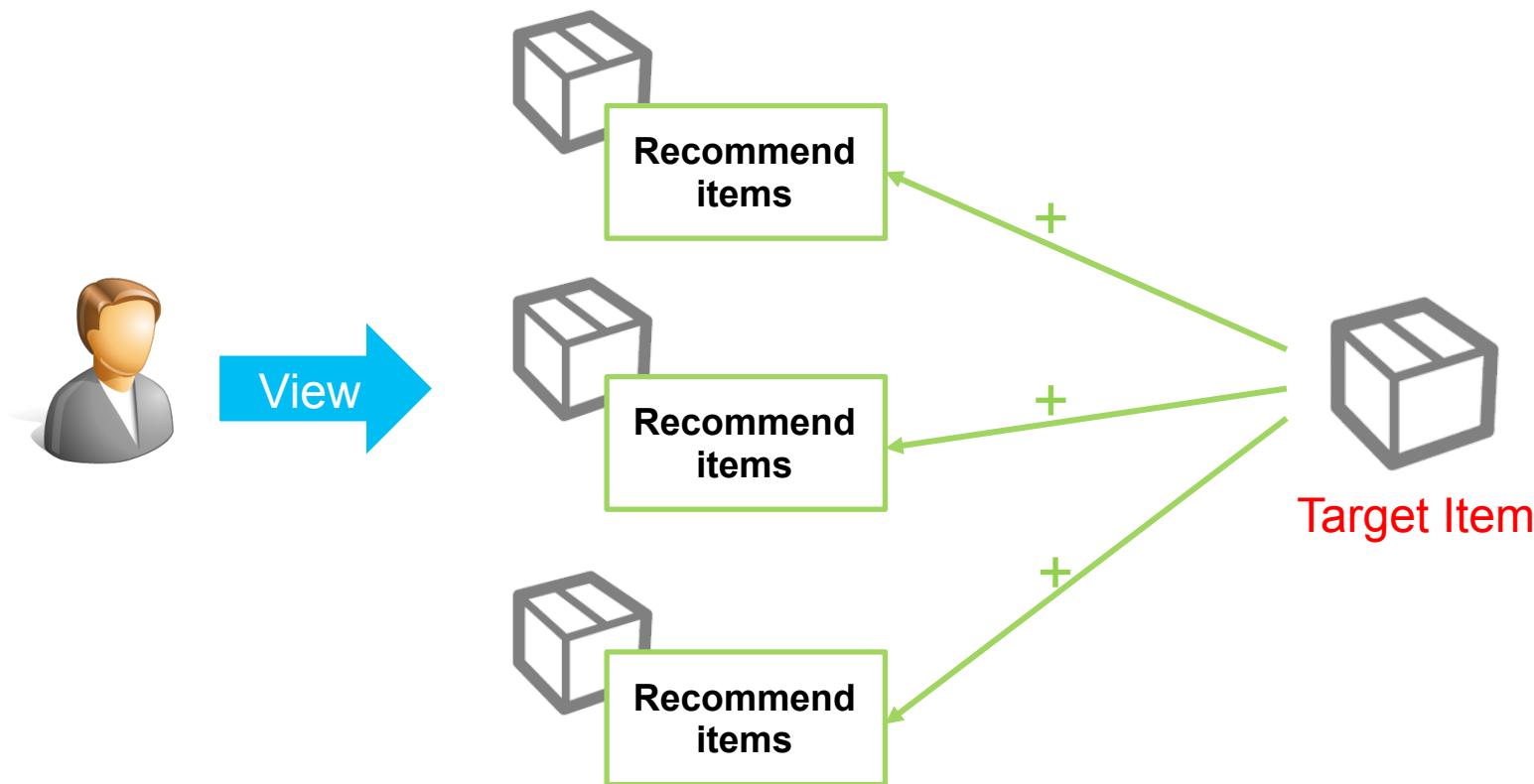
- Attacker's goal

- User Impression (**UI**) : The probability that a random visitor will see the item
- Increase UI of a target item
- Decrease UI of a target item



Proposed Attacks

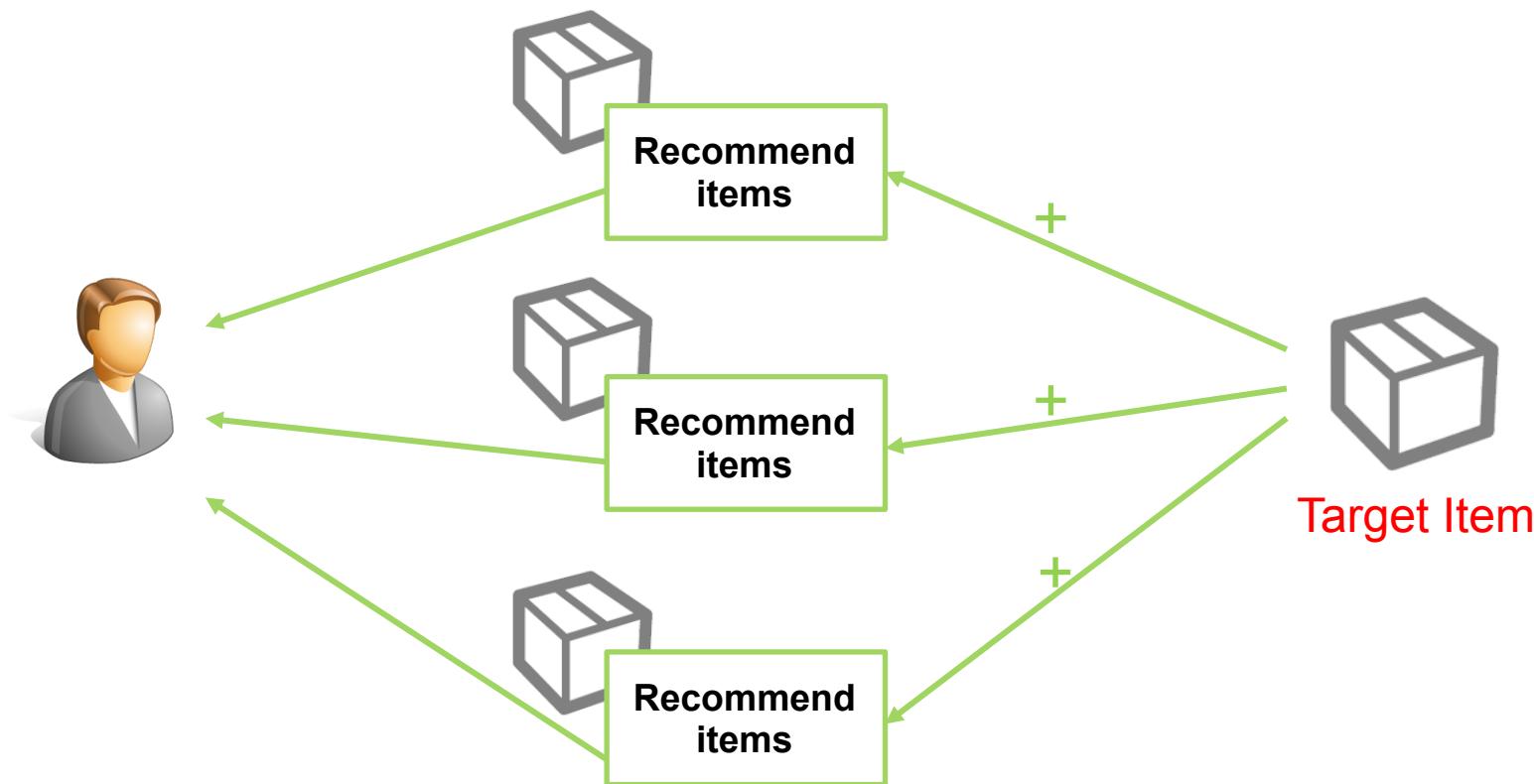
- Promotion attack
 - Goal: Increase UI of a **Target Item**
 - Make the target item appear in the recommendation lists of as many items as possible





Proposed Attacks

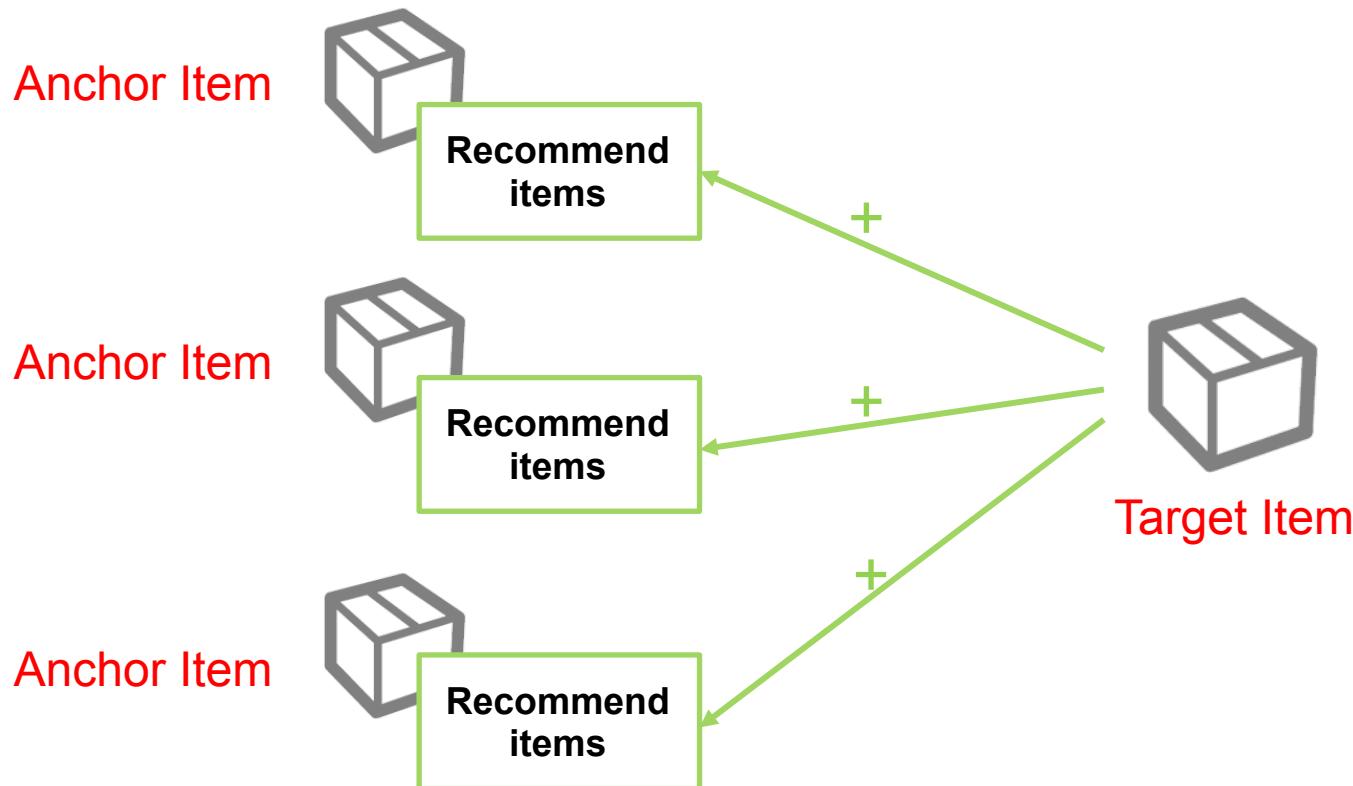
- Promotion attack
 - Goal: Increase UI of a **Target Item**
 - Make the target item appear in the recommendation lists of as many items as possible





Proposed Attacks

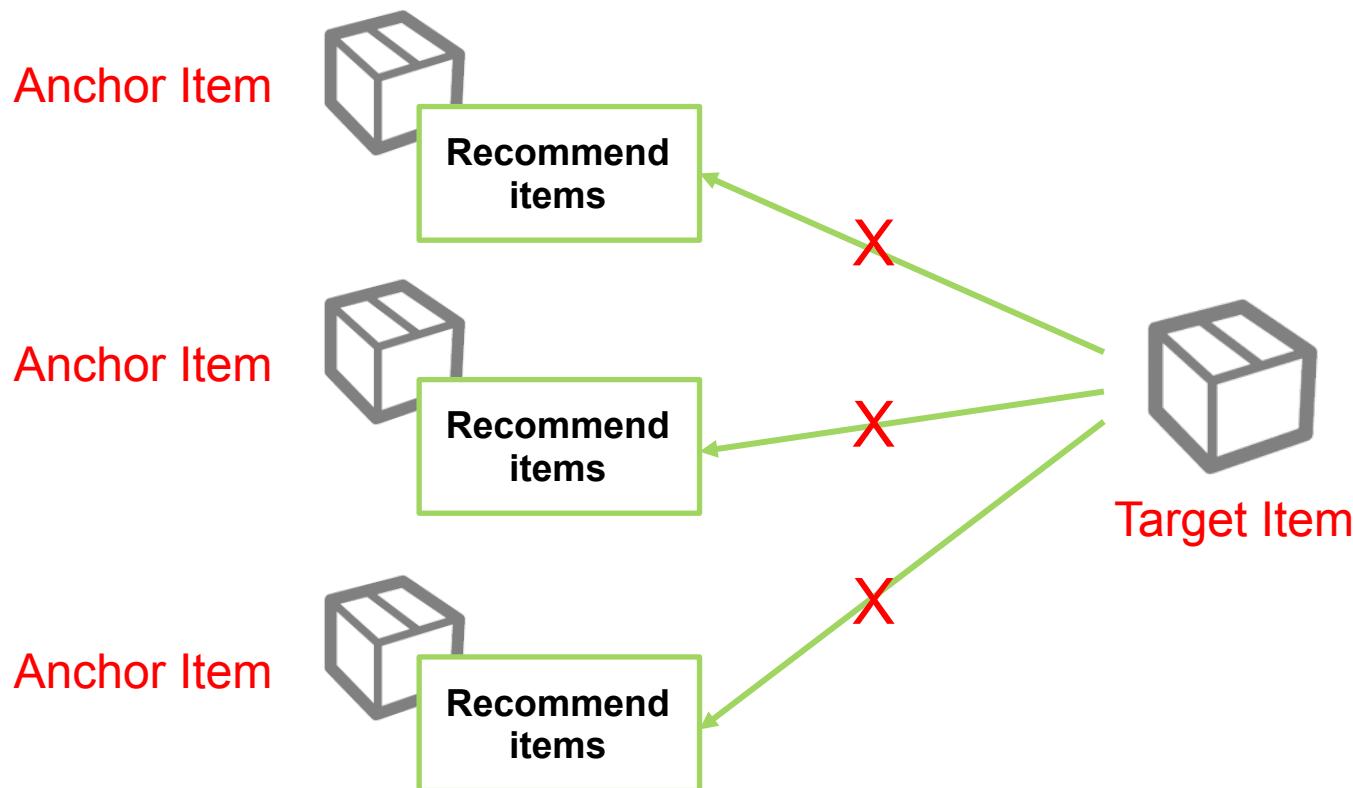
- Promotion attack
 - Goal: Increase UI of a **Target Item**
 - Make the target item appear in the recommendation lists of as many items as possible





Proposed Attacks

- Demotion attack
 - Goal: Decrease UI of a **Target Item**
 - Remove the target item from the recommendation lists of as many items as possible





Key Challenge

- Given a target item and a limited number fake co-visitations
 - *How to select the anchor item(s) to attack?*
 - *How many fake co-visitations to insert for each anchor item?*



Key Challenge

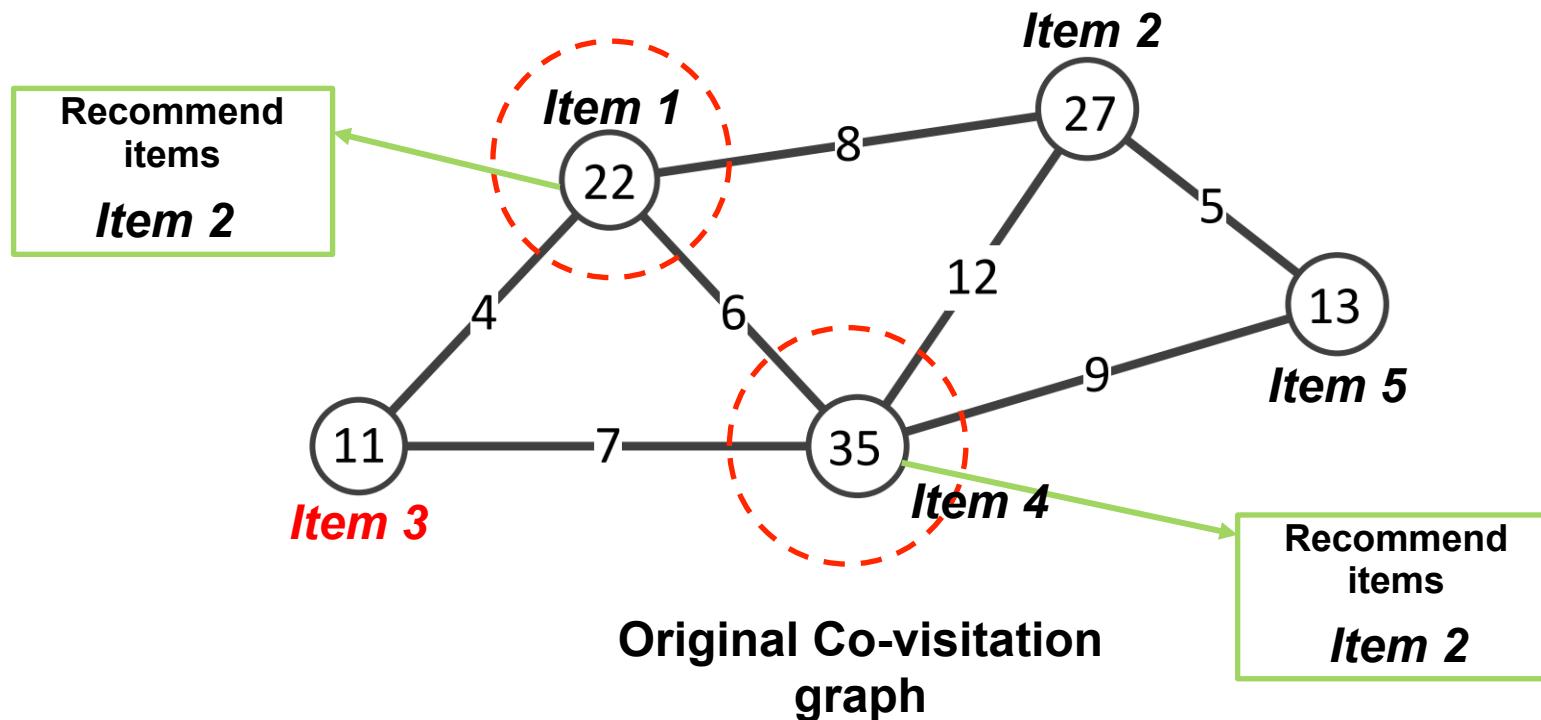
- Given a target item
 - *How to select the anchor item(s) to attack?*
 - *How many fake co-visitations to insert for each anchor item?*
- Solution: Formulate the attack as an optimization problem
 - *Select the best anchor items to attack*
 - *Determine how many fake co-visitation is needed to attack each anchor*



Promotion Attack – High Knowledge Attacker

Attacker's Goal: Promote *Item 3*

Select anchor items

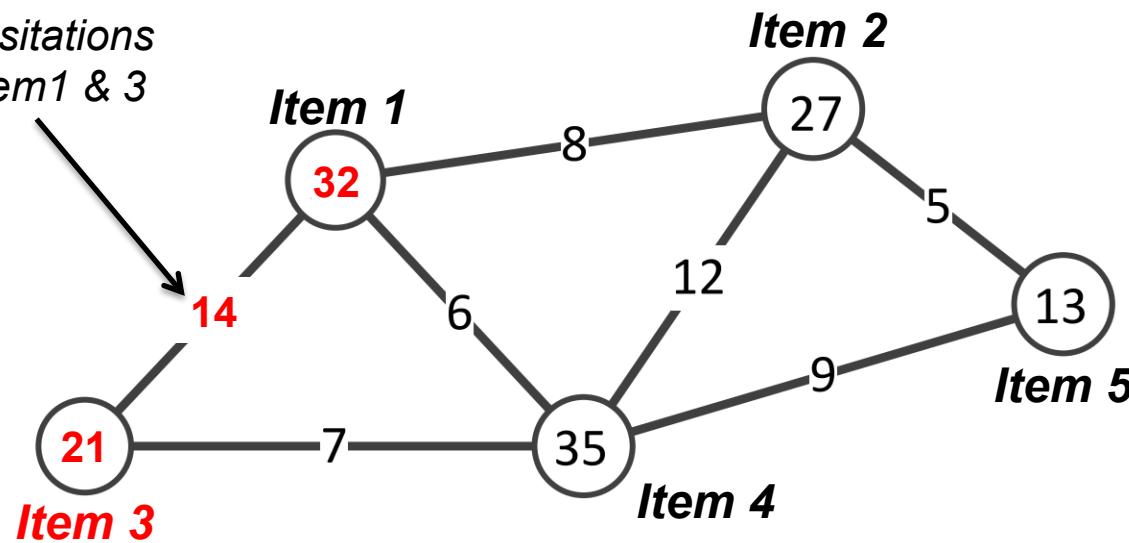




Promotion Attack – High Knowledge Attacker

Attacker's Goal: Promote *Item 3*

*Insert 10 fake
co-visitations
of Item 1 & 3*

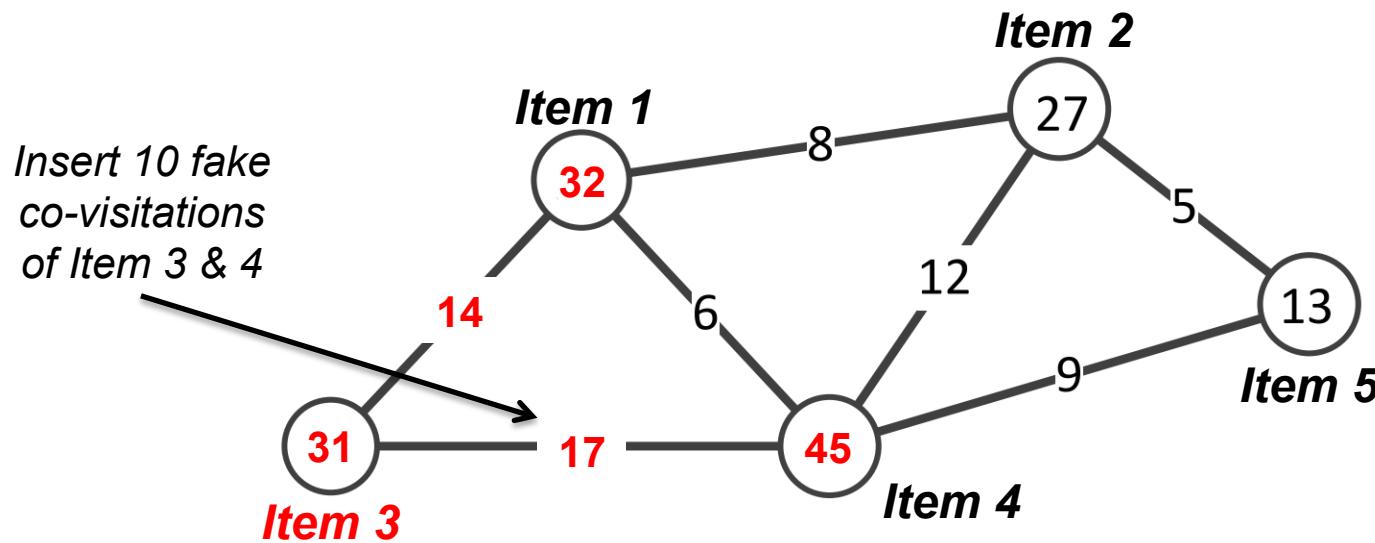


**Attacked Co-visitation
graph**



Promotion Attack – High Knowledge Attacker

Attacker's Goal: Promote *Item 3*

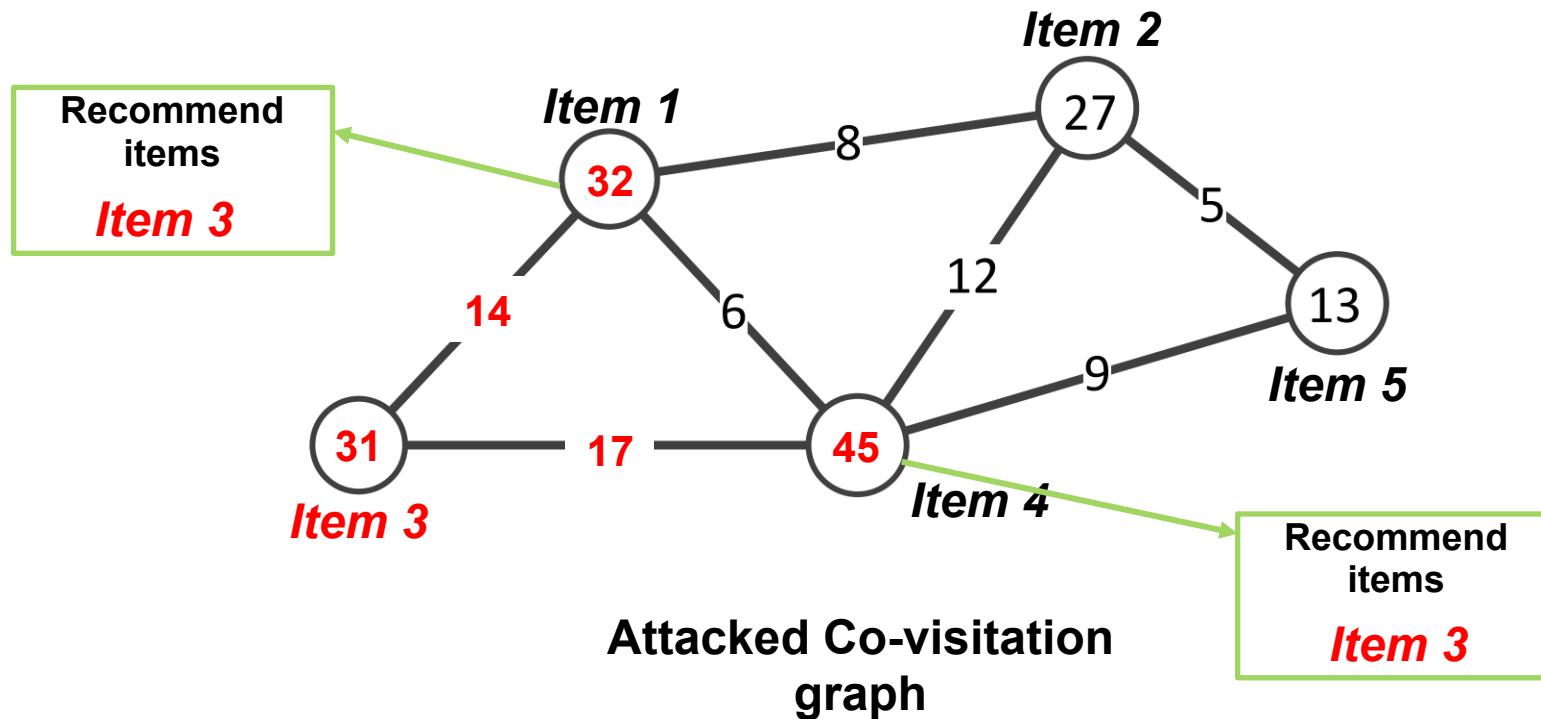


Attacked Co-visitation graph



Promotion Attack – High Knowledge Attacker

Attacker's Goal: Promote *Item 3*





Promotion Attack – High Knowledge Attacker

Attacker's Goal: Promote *Item 3*

Recomm
item
Item 3

- Medium knowledge attacker can be converted into high knowledge attacker by *estimating edge weight*
- Low knowledge attacker can be converted into medium knowledge attacker by *estimating vertex weight*

Item 3

Item 7

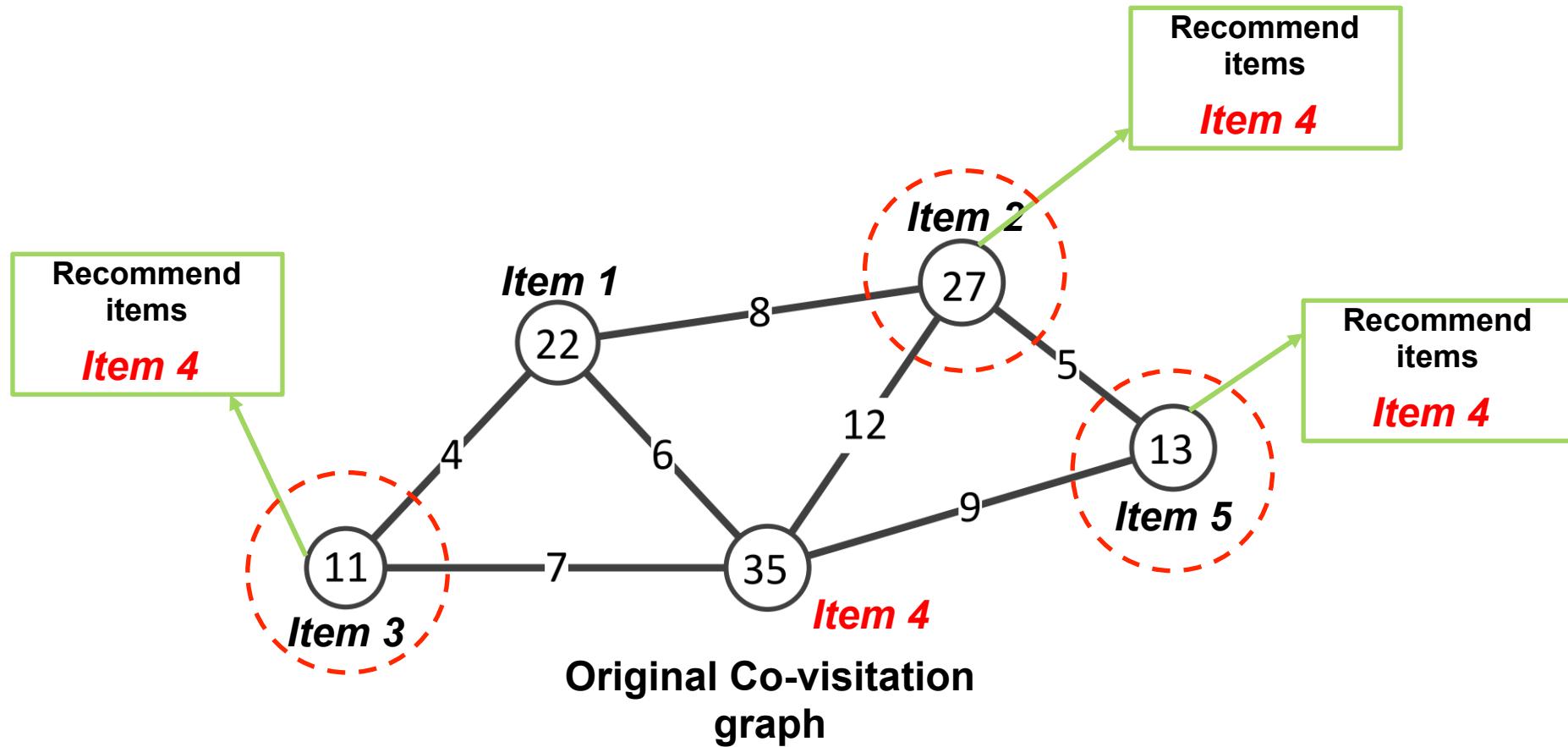
Recommend
items
Item 3

**Attacked Co-visitation
graph**



Demotion Attack – High Knowledge Attacker

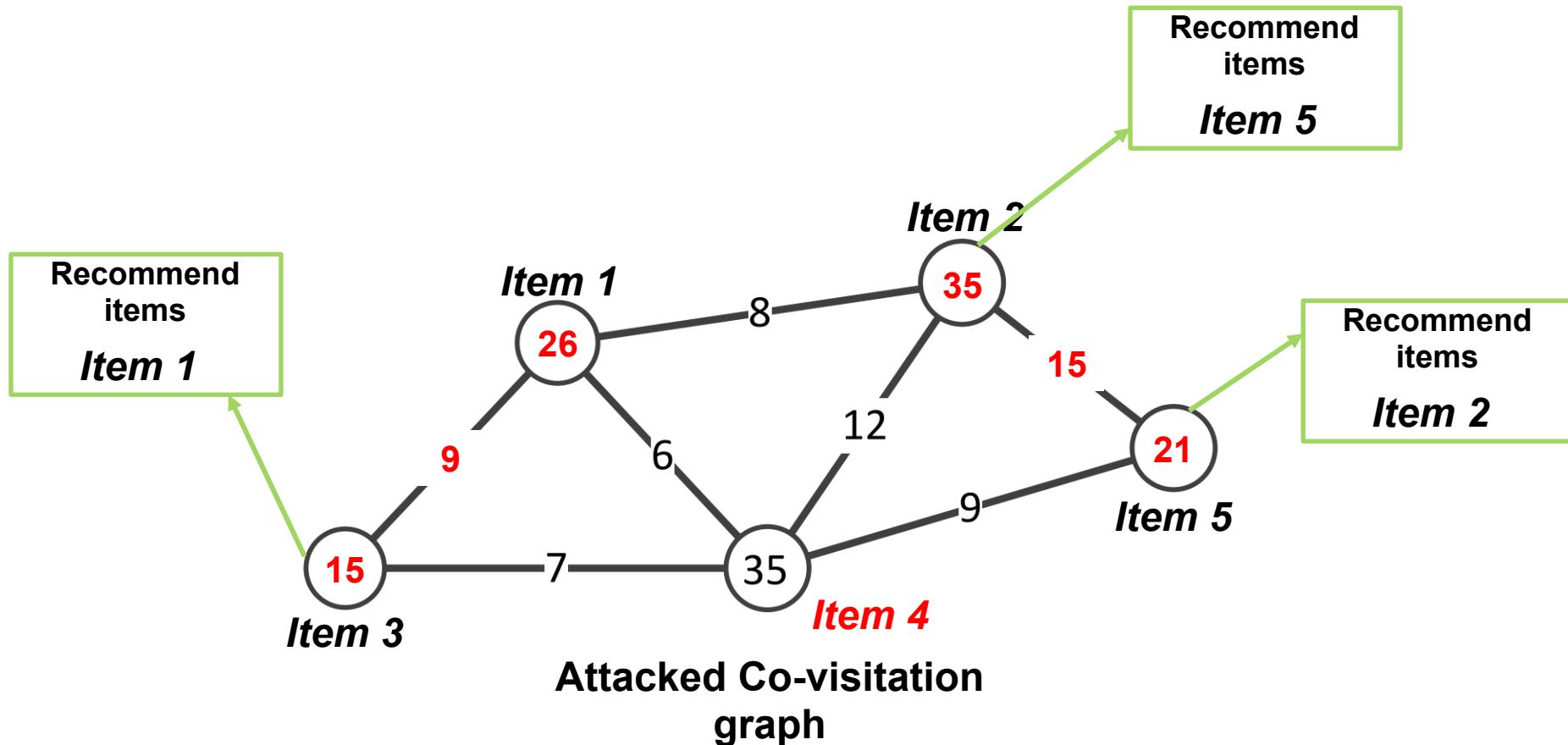
Attacker's Goal: Demote *Item 4*





Demotion Attack – High Knowledge Attacker

Attacker's Goal: Demote *Item 4*



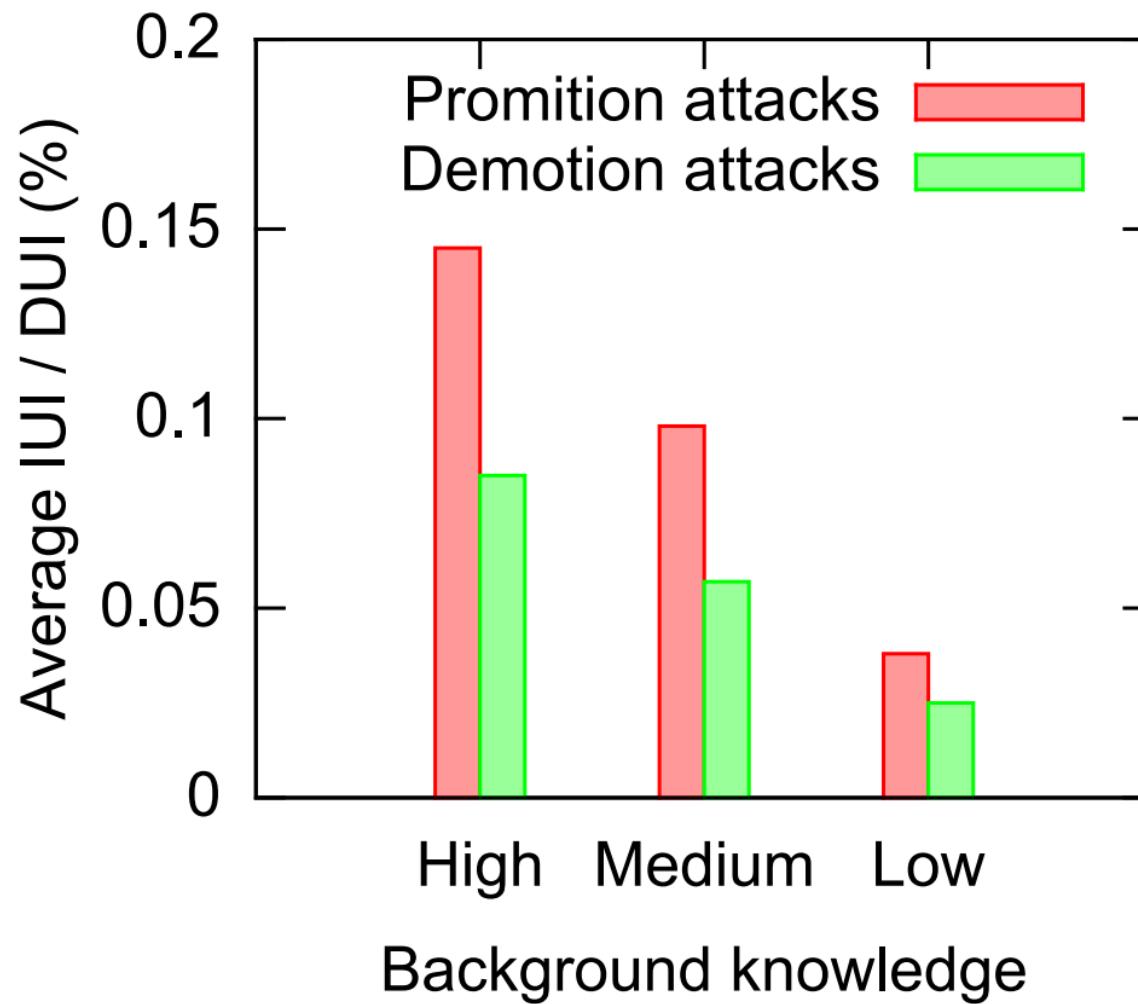


Evaluation on Synthetic Data

- Question we aim to answer
 - How does attacker's background knowledge impact our attacks
 - How does the co-visitation graph structure impact our attacks?
 - How does the number of inserted fake co-visitations impact our attacks?

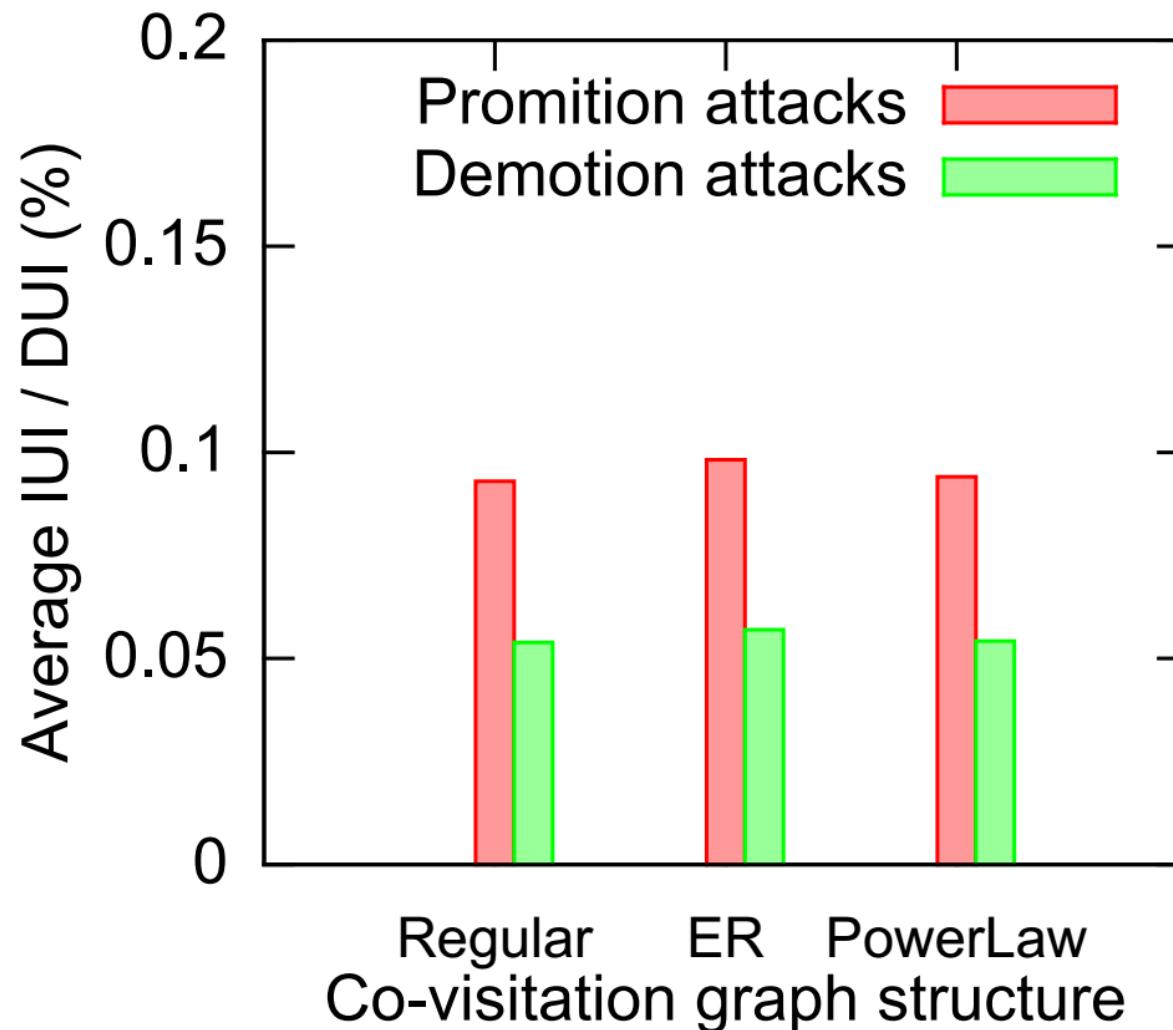


Impact of Attacker's Background Knowledge



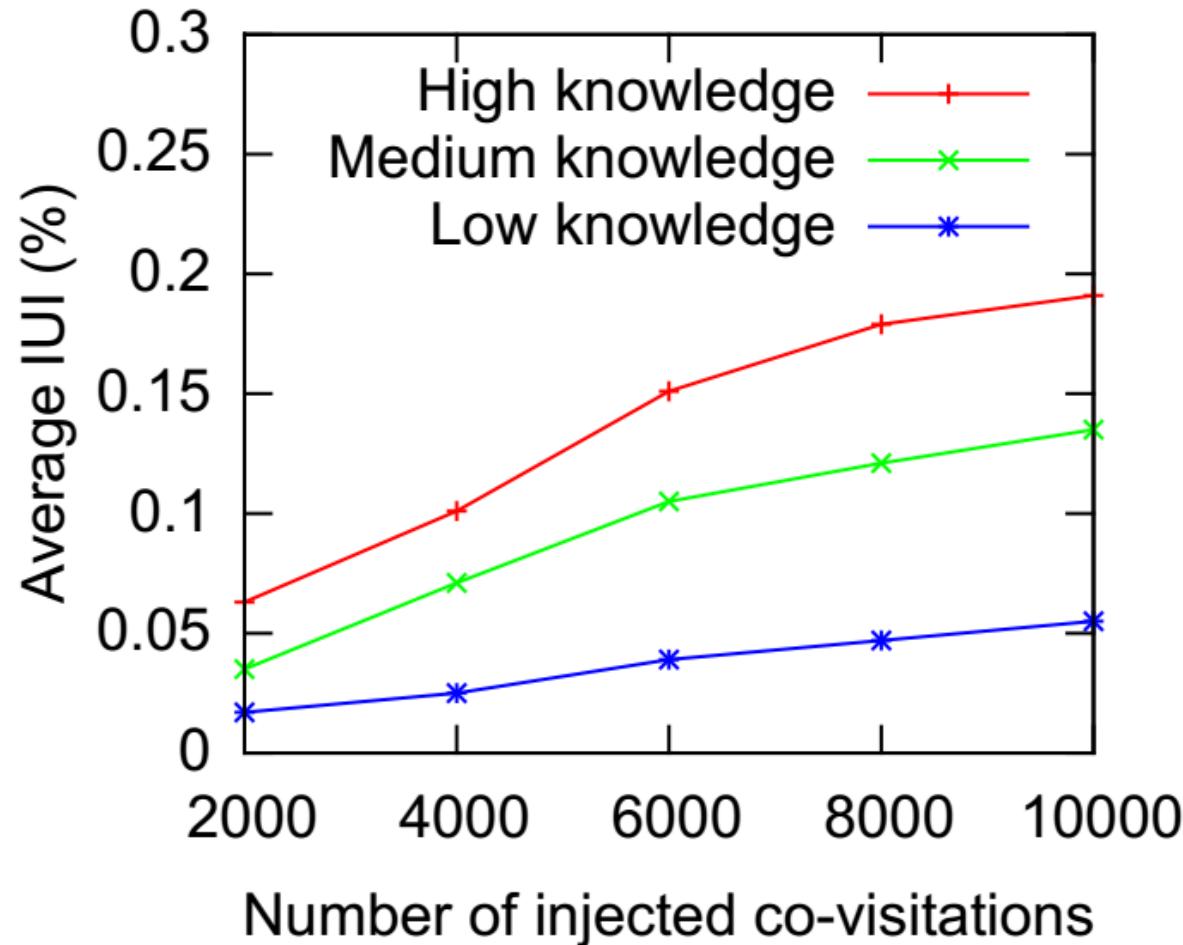


Impact of Co-visitation Graph Structure



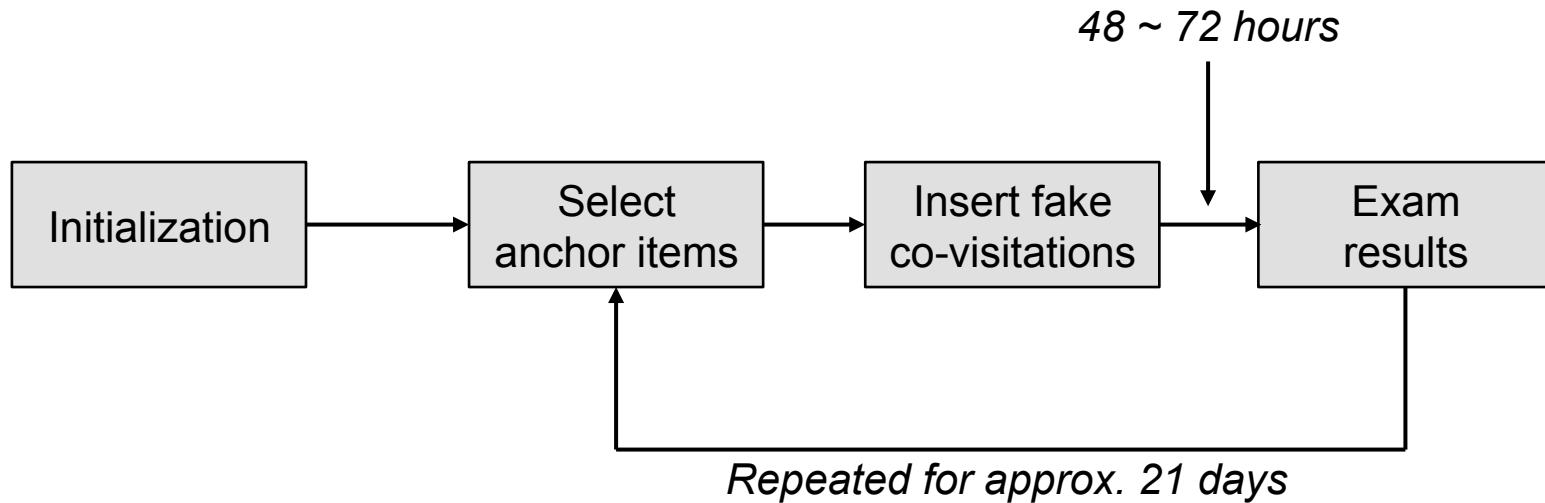


Impact of Number of Fake Co-visitations



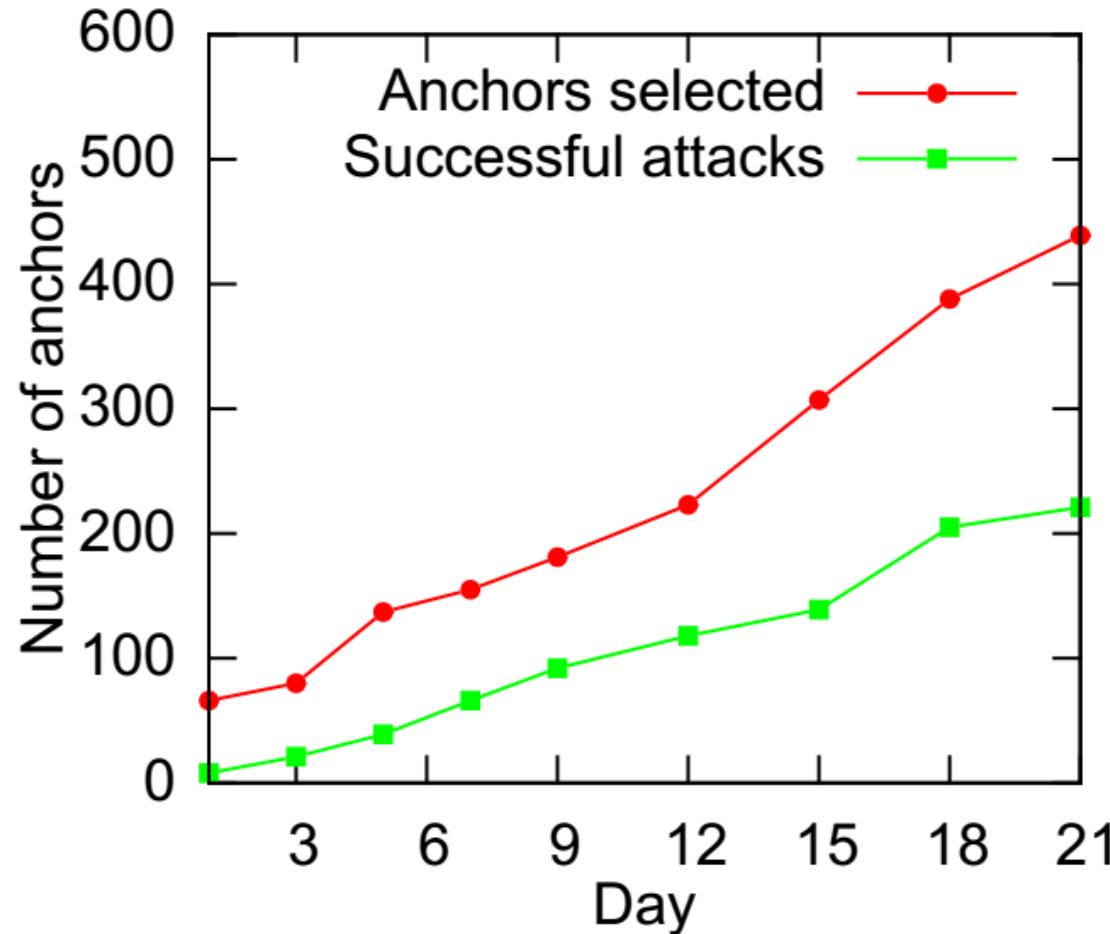


Evaluation on Real-World Recommender Systems



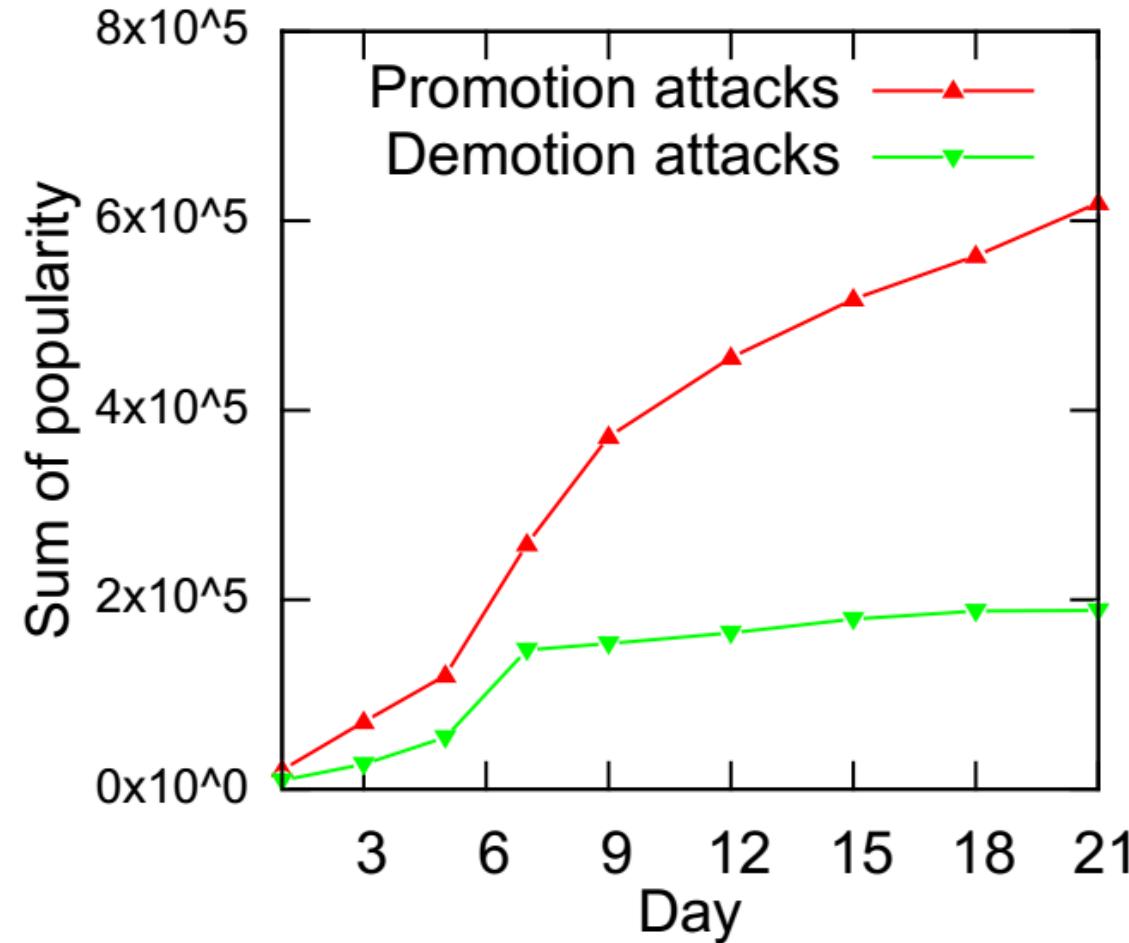


Results on YouTube





Results on YouTube





Countermeasures

- Limiting background knowledge
 - The website can *discretize item popularities*



Shows exact
popularity



Discretize Granularity
= 500

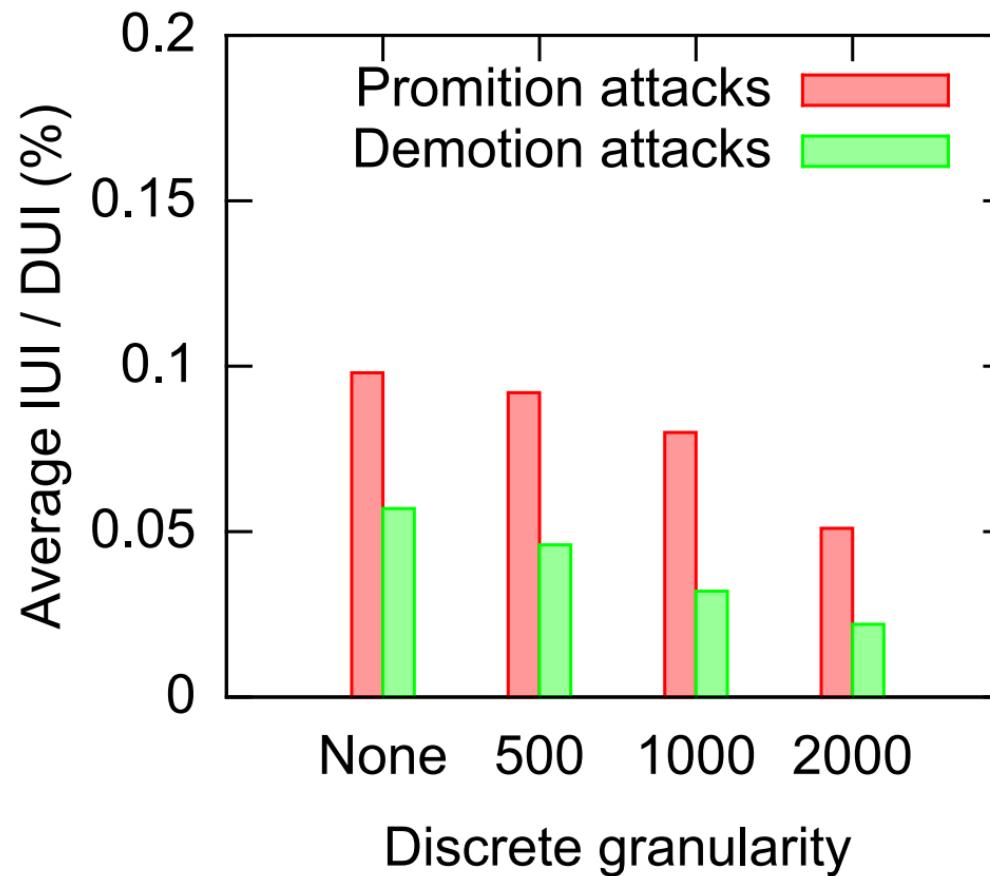


Discretize Granularity
= 2000



Countermeasures

- Limiting background knowledge
 - The website can *discretize item popularities*





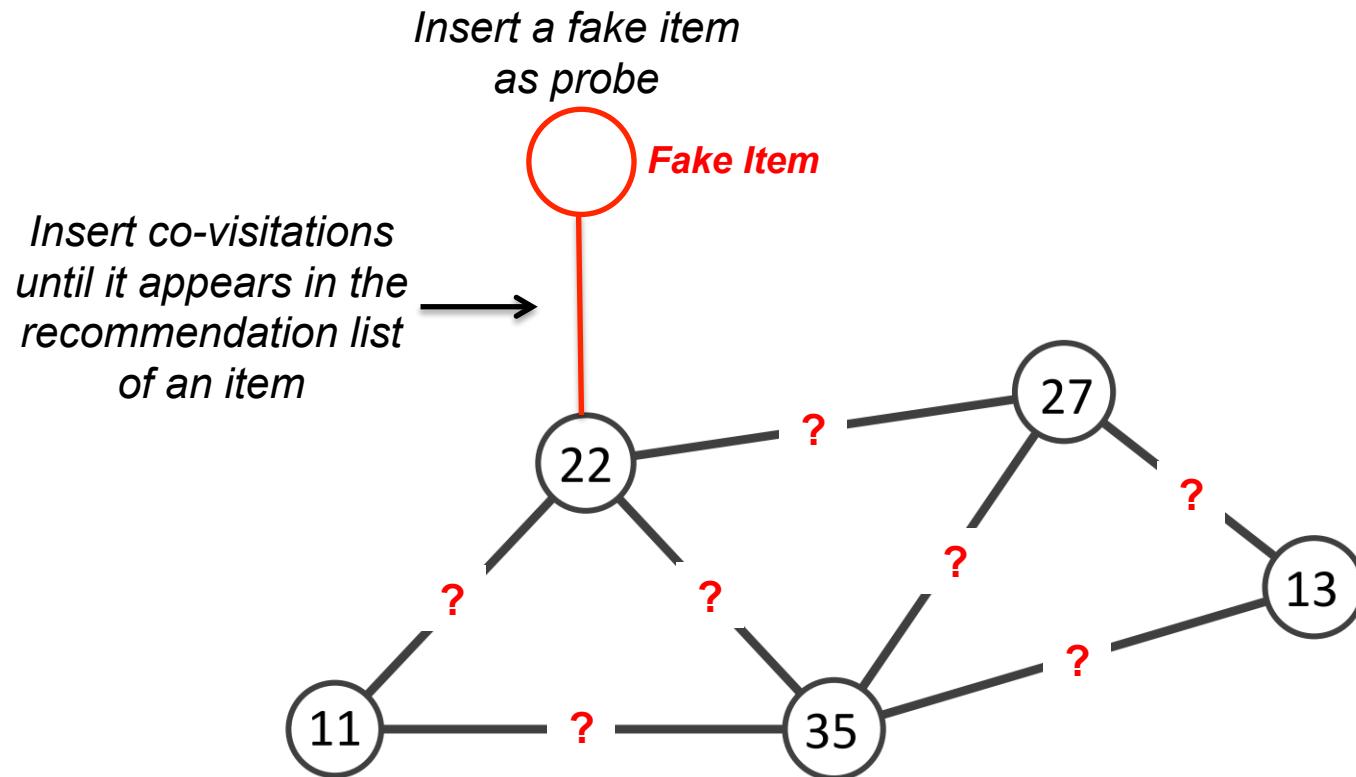
Conclusion

- Recommender systems are vulnerable to *Fake Co-visitation Injection Attacks*
- An attacker can use our attacks to spoof a recommender system to make recommendations as the attacker desires.



Parameter Estimation

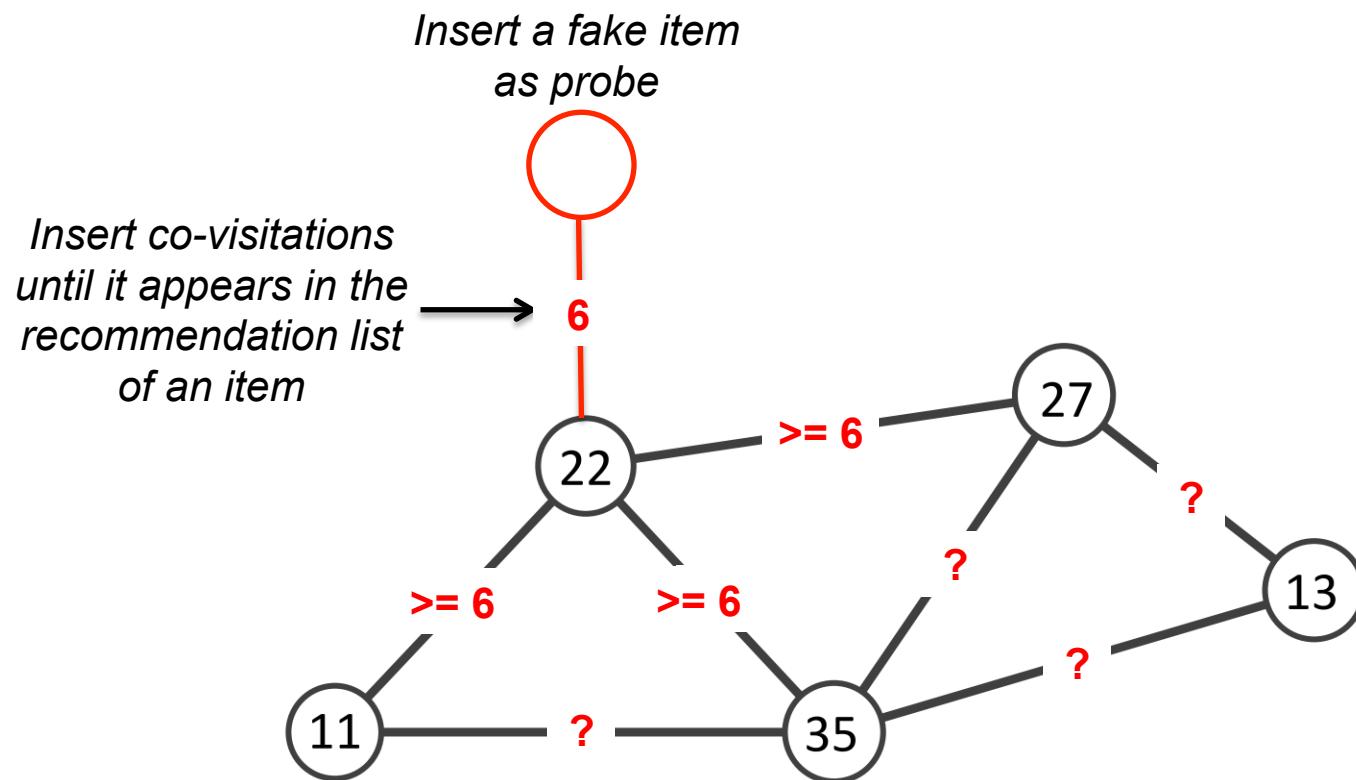
- Convert *medium/low knowledge attackers* into *high knowledge attacker*
 - The missing knowledge is estimated based on publically available information





Parameter Estimation

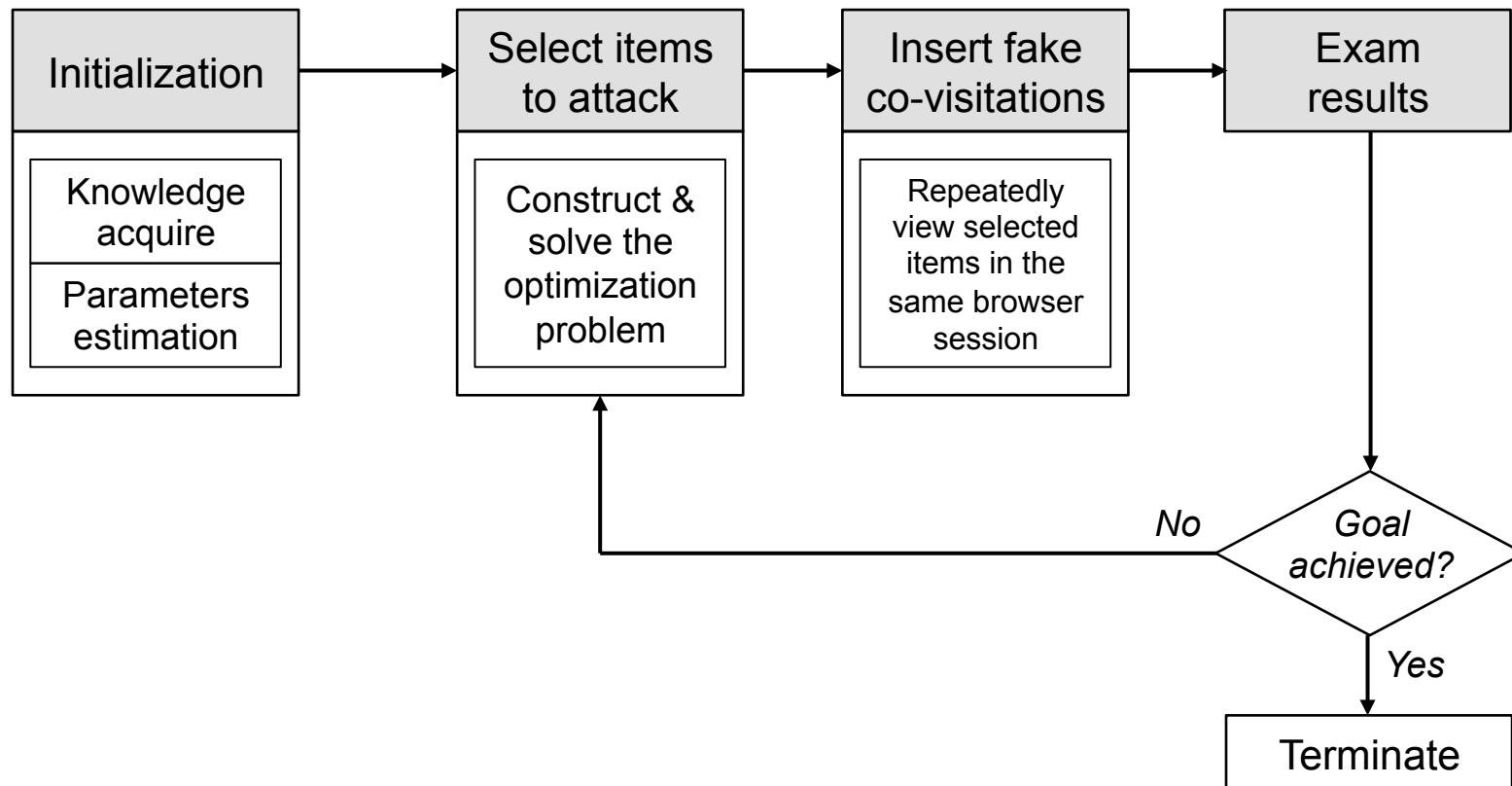
- Convert *medium/low knowledge attackers* into *high knowledge attacker*
 - The missing knowledge is estimated based on publically available information





Proposed Attack Algorithm

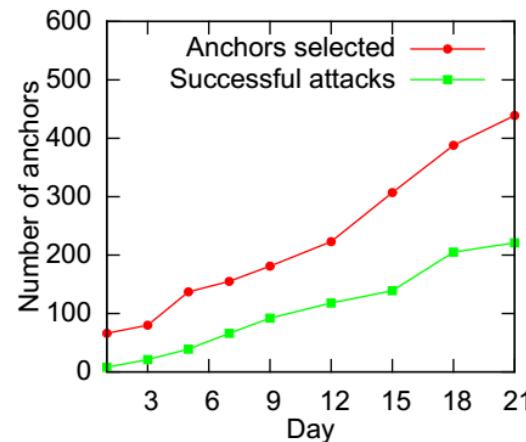
- General steps



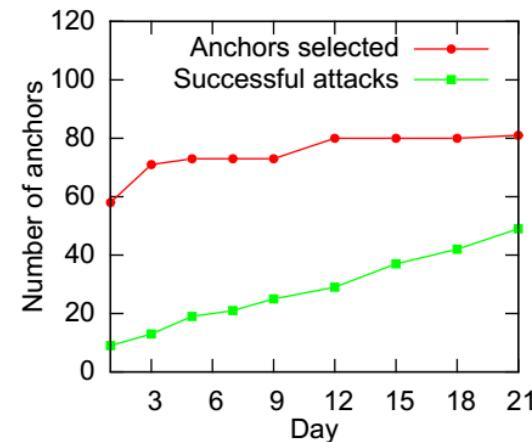


Experiments on Real-world Recommender Systems

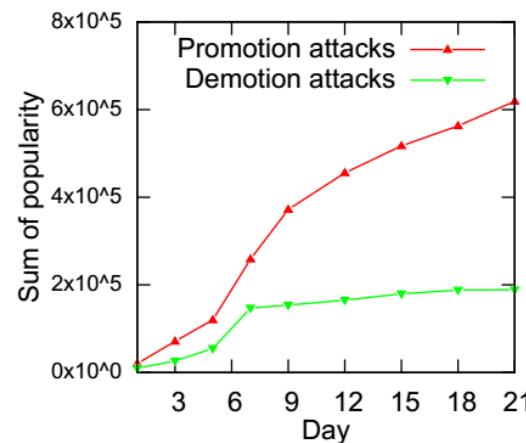
- Results on YouTube



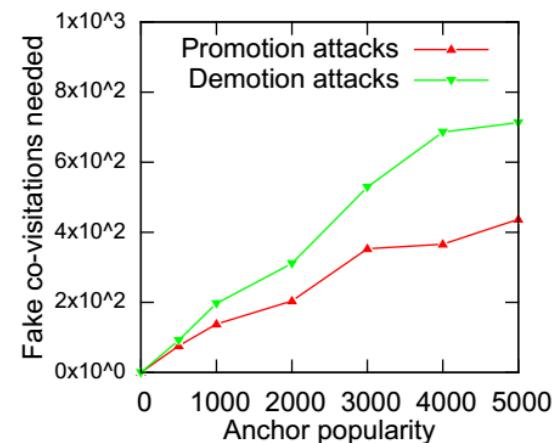
(a) Promotion attacks



(b) Demotion attacks



(c) Popularity of successfully attacked anchors

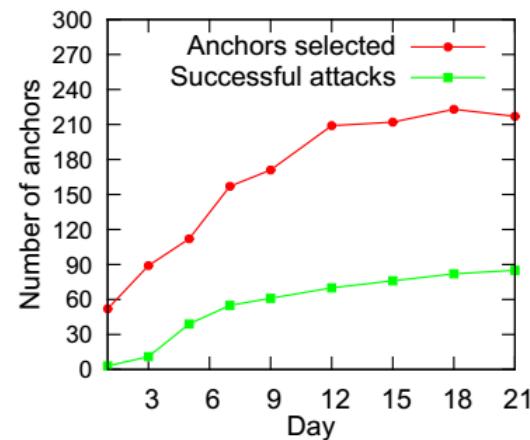


(d) Cost vs. anchor popularity

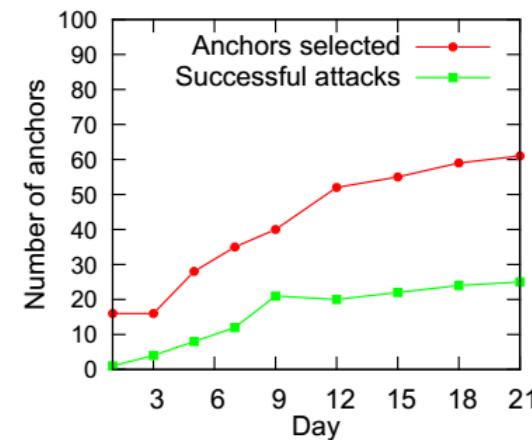


Experiments on Real-world Recommender Systems

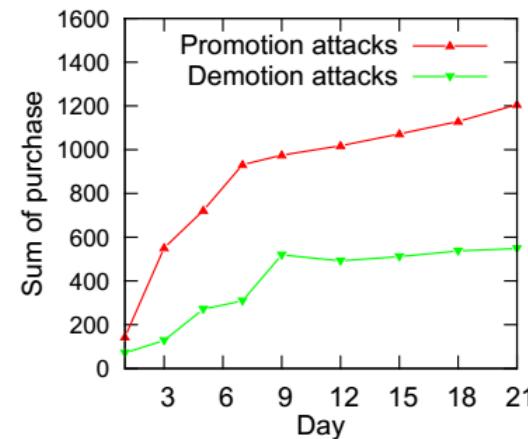
- Results on eBay



(a) Promotion attack



(b) Demotion attacks

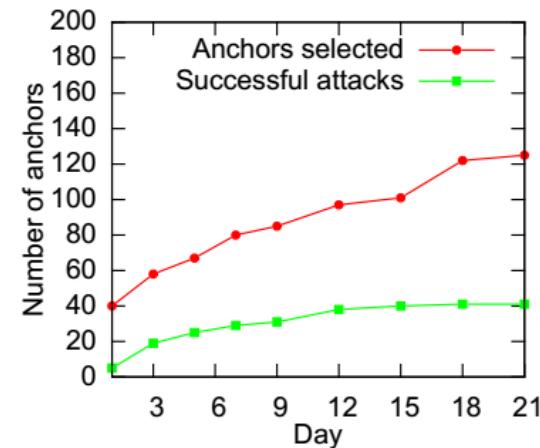


(c) Purchases of successfully attacked anchors

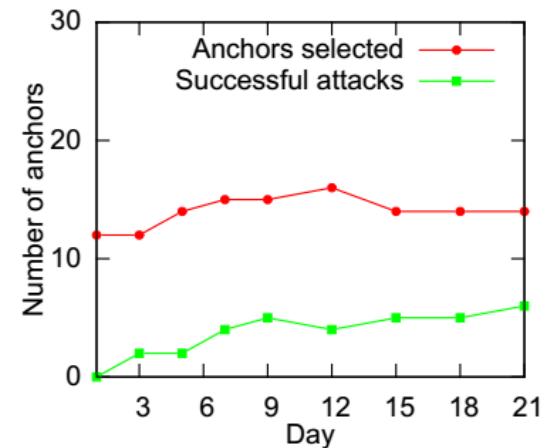


Experiments on Real-world Recommender Systems

- Results on *Amazon*

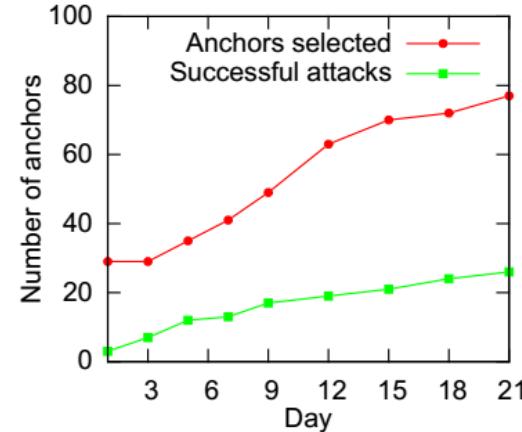


(a) Promotion attacks

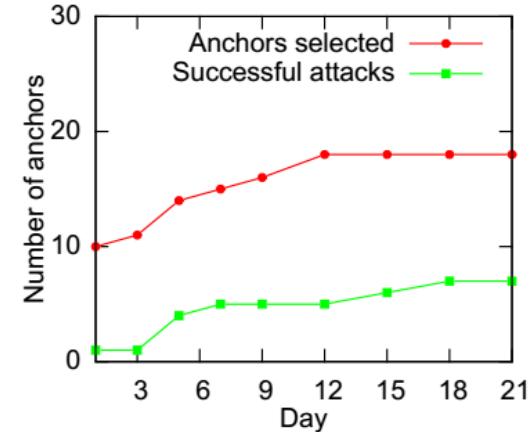


(b) Demotion attacks

- Results on *Yelp*



(a) Promotion attacks

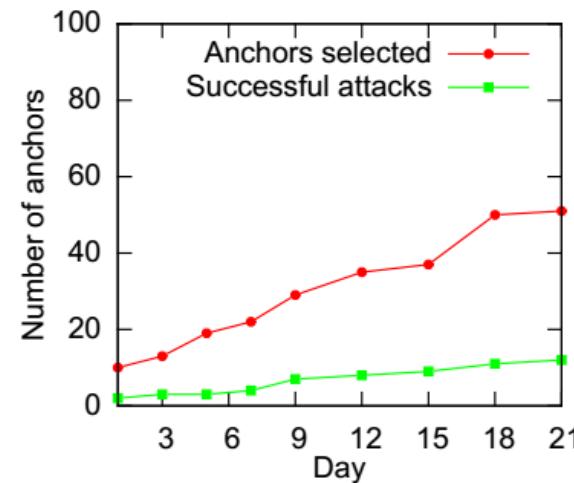


(b) Demotion attacks

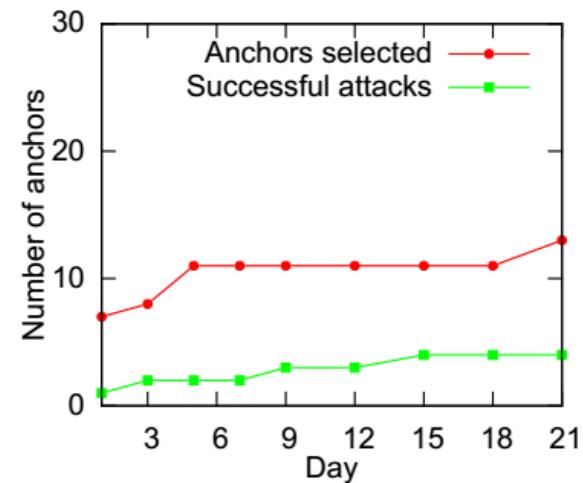


Experiments on Real-world Recommender Systems

- Results on *LinkedIn*



(a) Promotion attacks

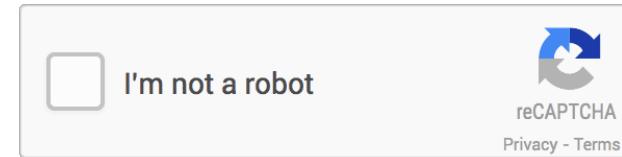


(b) Demotion attacks



Countermeasures

- Limiting fake co-visitations
 - Use CAPTCHA



- Fake co-visitation detection
- Using co-visitations from registered users only