Heterogeneous Graph Neural Networks for Malicious Account Detection

Ziqi Liu et al.

Ant Financial Service, Georgia Tech

27^{th} *ACM International Conference on Information and Knowledge Management (CIKM'18)*
Industry and Case Study Paper

Presenter: Weilin Xu
https://qdata.github.io/deep2Read

Outline

Fraud Detection

Malicious Account Detection:

To determine if an account is owned by adversary or normal user.

Fraud Detection

Malicious Account Detection:

To determine if an account is owned by adversary or normal user.

Proposed solution:

Graph **E**mbeddings for **M**alicious accounts (GEM)

Intuition

Patterns observed from malicious accounts.

- Device aggregation

  Adversary logins to many accounts on one device.

Device Aggregation

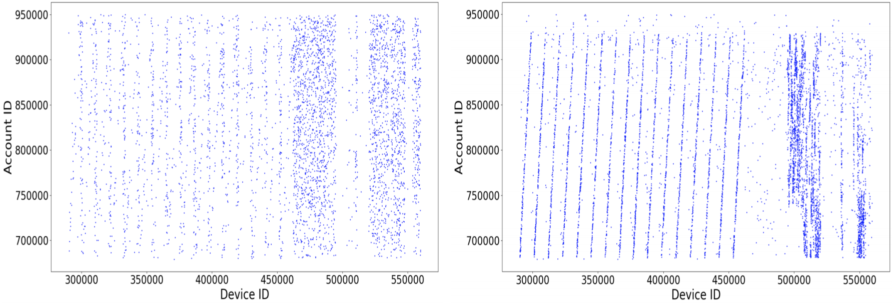

Figure: Left: Normal; Right: Malicious.

Intuition

Patterns observed from malicious accounts.

- Device aggregation
  Adversary logins to many accounts on one device.
- Activity aggregation
  Adversary's accounts behave in batches.

Activity Aggregation

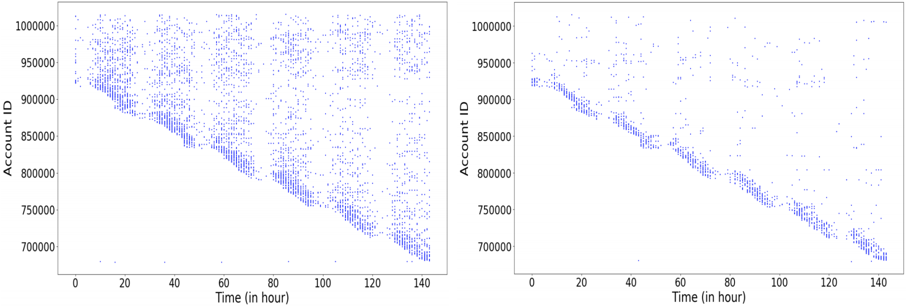

Figure: Left: Normal; Right: Malicious.

Heterogeneous Graph Construction

- **Vertices**: 1) Account vertices; 2) Device vertices.
- **Edges**: Account is active on Device.

Represented as **adjacency matrix** $A \in \{0, 1\}^{N,N}$.

$A_{i,j} = 1$: account i active on device j

$A^{(d)}$: subgraph ignoring edges to non-type-d devices.

Features of Vertices: $X \in \mathbb{R}^{N,p+|\mathcal{D}|+200}$

Account vertices only: p time slots, with activity counts;

$p = 7 \times 24 = 168$ slots, with activity counts.

Device vertices only: one hot $|\mathbb{D}|$.

6 types of devices.

Account vertices only: 200 demographics features.

Broad Device Concept

Six device types.

- Four Hardware ID.
  - Phone number
  - WiFi MAC address
  - International Mobile Subscriber Identity (IMSI)
  - TID

    Random number generated with IMSI and IMEI.
- Two Proprietary Composite Fingerprint
  - User Machine ID (UMID)

    Unclear
  - Alipay Device ID (APDID)

    Consider IMEI, IMSI, CPU, Bluetooth ADDR, ROM.

Broad Device Concept : Attention Coefficients

Six device types.

- Four Hardware ID.
  - Phone number
  - WiFi MAC address
  - International Mobile Subscriber Identity (IMSI)
  - TID

    Random number generated with IMSI and IMEI.
- Two Proprietary Composite Fingerprint
  - User Machine ID (UMID) 0.4412 <Secret Weapon>

    Unclear
  - Alipay Device ID (APDID)

    Consider IMEI, IMSI, CPU, Bluetooth ADDR, ROM.

Broad Device Concept : Attention Coefficients

Six device types.

- Four Hardware ID.
  - Phone number 0.2952
  - WiFi MAC address
  - International Mobile Subscriber Identity (IMSI)
  - TID

    Random number generated with IMSI and IMEI.
- Two Proprietary Composite Fingerprint
  - User Machine ID (UMID) 0.4412 <Secret Weapon>

    Unclear
  - Alipay Device ID (APDID)

    Consider IMEI, IMSI, CPU, Bluetooth ADDR, ROM.

Broad Device Concept : Attention Coefficients

Six device types.

- Four Hardware ID.
  - Phone number 0.2952
  - WiFi MAC address 0.13
  - International Mobile Subscriber Identity (IMSI)
  - TID
    Random number generated with IMSI and IMEI.
- Two Proprietary Composite Fingerprint
  - User Machine ID (UMID) 0.4412 <Secret Weapon>
    Unclear
  - Alipay Device ID (APDID)
    Consider IMEI, IMSI, CPU, Bluetooth ADDR, ROM.

Broad Device Concept : Attention Coefficients

Six device types.

- Four Hardware ID.
  - Phone number 0.2952
  - WiFi MAC address 0.13
  - International Mobile Subscriber Identity (IMSI)
  - TID

    Random number generated with IMSI and IMEI.
- Two Proprietary Composite Fingerprint
  - User Machine ID (UMID) 0.4412 <Secret Weapon>

    Unclear
  - Alipay Device ID (APDID) 0.0142

    Consider IMEI, IMSI, CPU, Bluetooth ADDR, ROM.

Broad Device Concept : Attention Coefficients

Six device types.

- Four Hardware ID.
  - Phone number 0.2952
  - WiFi MAC address 0.13
  - International Mobile Subscriber Identity (IMSI)
  - TID 0.0125

    Random number generated with IMSI and IMEI.
- Two Proprietary Composite Fingerprint
  - User Machine ID (UMID) 0.4412 <Secret Weapon>

    Unclear
  - Alipay Device ID (APDID) 0.0142

    Consider IMEI, IMSI, CPU, Bluetooth ADDR, ROM.

Models

Goal: learn embedding matrix H (i^{th} row is h_i of vertex i)

$$H^{(0)} \leftarrow \mathbf{0}$$

$$\text{for} \quad t = 1, ..., T$$

$$H^{(t)} \leftarrow \sigma(X \cdot W + \frac{1}{|\mathcal{D}|} \sum_{d=1}^{|\mathcal{D}|} A^{(d)} \cdot H^{(t-1)} \cdot V_d)$$

Embeddings at t^{th} layer: $H^{(t)} \in \mathbb{R}^{N,k}$
Features: $X \in \mathbb{R}^{N,p+|\mathcal{D}|}$, fed into each layer, ResNet alike.
Trainable parameters: $\{V_d\} \in \mathbb{R}^{k \times k}$;
$W \in \mathbb{R}^{P \times k} (P = p + |\mathcal{D}|)$, shared among subgraphs.
Adjacency matrix: $A \in \{0, 1\}^{N,N}$
Hyper-parameters: Embedding size k;
#hidden layers T (#hops a vertex needs to look at)

Attention Mechanism

$$\alpha = [\alpha_1, ..., \alpha_{|\mathbb{D}|}]^T \in \mathbb{R}^{|\mathbb{D}|}$$

$$softmax(\alpha_d) = \frac{exp\alpha_d}{\sum_i exp\alpha_i}$$

$$H^{(t)} \leftarrow \sigma(X \cdot W + \sum_{d \in \mathbb{D}} softmax(\alpha_d) \cdot A^{(d)} \cdot H^{(t-1)} \cdot V_d)$$

Logistic Regression Classifier

$$\min_{W,\{V_d\},u} \mathbb{L}(W,\{V_d\},u) = -\sum_{i}^{N_0} log\sigma(y_i \cdot (u^\top h_i)) \tag{1}$$

where $\sigma = \frac{1}{1+exp(-x)}$, $u \in \mathbb{R}^k$

Expectation Maximization style

e-step: compute embeddings based on $W, \{V_d\}$.

m-step: optimize u, while freezing embeddings.

Datasets

4 consecutive weeks of data from Alipay.

- 8M vertices, 10M edges
- 1.7M train labels, 0.2M test labels (#account vertices?)
- 374 features

374 features for each vertex:

- [Account Only] $p = 7 \times 24 = 168$ slots, with activity counts.
- [Device Only] 6 types of devices.
- [Account Only] 200 demographics features (yet another secret weapon?)

Train with first 6 days; test with the last day.
4 isolated experiments.

Comparison Methods

Baseline

- Connected Subgraph
- GBDT + Graph
- GBDT + Node2Vec
- Graph Convolutional Network

Variants of this work

- **G**raph **E**mbeddings for **M**alicious accounts (GEM)
- GEM-attention

Result - F-1 Score

	week 1	week 2	week 3	week 4
Connected Subgraphs	0.5033	0.5567	0.58	0.5421
GBDT+Graph	0.7423	0.7598	0.7693	0.6639
GBDT+Node2Vec	0.741	0.7571	0.769	0.6626
GCN	0.7729	0.7757	0.7957	0.6919
GEM (Ours)	0.7992	0.8066	0.8191	0.718
GEM-attention (Ours)	**0.8165**	**0.8133**	**0.8244**	**0.7344**

Figure: F-1 Score

Result - AUC

	week 1	week 2	week 3	week 4
Connected Subgraphs	0.6689	0.6692	0.665	0.6938
GBDT+Graph	0.8878	0.8835	0.8707	0.8778
GBDT+Node2Vec	0.8884	0.883	0.8711	0.8773
GCN	0.8995	0.8932	0.8922	0.881
GEM (Ours)	0.9159	0.9238	0.9193	0.9082
GEM-attention (Ours)	**0.9364**	**0.9293**	**0.9259**	**0.9155**

Figure: AUC

Online Result

98% precision over 89% of rule-based system.
Recall unknown.

Precision-Recall Curves on Week 4

[Guess: Recall at 98% precision is about 0.5%.]

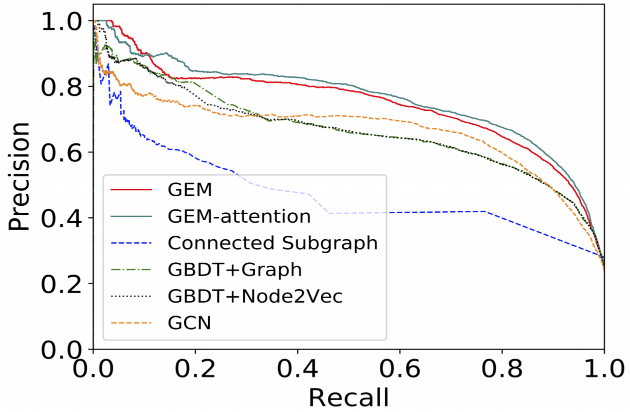

Figure: Precision-Recall Curves on Week 4.

Conclusion

- Novel graph neural network model for heterogeneous graph.
- Exploit two weaknesses of adversary:
  Device aggregation & Activity aggregation.
- Detect 10K malicious accounts daily at Alipay.
- Future work: beyond adjacency matrix.

Discussions

- Not reproducible.
  No open dataset or open source code.
  Lack details of secret weapons.
- Adaptive adversary.
  Fake Hardware ID by hijacking system APIs on rooted devices.
  Malicious account can be more active.