



# FraudVis: Understanding Unsupervised Fraud Detection Algorithms

Jiao Sun<sup>1</sup>, Qixin Zhu<sup>1</sup>, Zhifei Liu<sup>1</sup>, Xin Liu<sup>1</sup>, Jihae Lee<sup>1</sup>, Lei Shi<sup>2</sup>, Zhigang Su<sup>3</sup>, Ling Huang<sup>1</sup> and Wei Xu<sup>1</sup>

<sup>1</sup> Institute of Interdisciplinary Information Sciences, Tsinghua University

<sup>2</sup> SKLCS, Institute of Software, Chinese Academy of Sciences

<sup>3</sup> JD.com

# Motivation

- Great loss caused by fraud users
  - Various kinds of fraud behavior
- Difficulty in distinguishing fraud users from normal users
  - Camouflage in **individuals**
  - **Collaborative** behavior
- Algorithm itself is hard to interpret
  - Feature selection is a black-box to user
  - The origin of “group” and why a group is abnormal



# What are fraudsters?

		ostype	ip_prefix_22	phone_city	phone_prefix_3	duration_quantized_20	label	id
30	good	android	101.90.252.0	上海	180	0	good	30
40	good	sim	114.95.156.0	上海	131	0	good	40
55	good	android	101.229.16.0	上海	137	0	good	55
63	good	android	1.197.176.0	上海	138	0	good	63
200	good	sim	117.136.8.0	上海	134	0	good	200
299	good	android	180.172.168.0	上海	156	0	good	299
458	bad	android	113.122.4.0	上海	170	0	bad	458
474	bad	android	119.122.96.0	上海	170	0	bad	474
491	bad	android	58.54.220.0	上海	170	0	bad	491
498	bad	android	117.66.192.0	上海	170	0	bad	498
519	bad	android	114.106.224.0	上海	170	0	bad	519
529	bad	android	112.113.60.0	上海	170	0	bad	529
531	bad	android	59.53.140.0	上海	170	0	bad	531
540	bad	android	27.27.172.0	上海	170	0	bad	540
544	bad	android	123.161.152.0	上海	170	0	bad	544
572	bad	android	114.239.0.0	上海	170	0	bad	572
614	bad	android	117.81.116.0	上海	170	0	bad	614
626	bad	android	120.32.128.0	上海	170	0	bad	626
639	bad	android	180.124.44.0	上海	170	0	bad	639
650	bad	android	117.93.140.0	上海	170	0	bad	650
652	bad	android	220.179.212.0	上海	170	0	bad	652
677	bad	android	180.122.20.0	上海	170	0	bad	677

# Challenges

- High-dimensional datasets
  - Various kinds of fraud behavior
  - High-dimensional data for each log
- Selection of features and algorithms
  - Hard to evaluate which ones are useful
  - Heavily depends on the scenario
- No labels
  - No label for evaluation
  - High cost for false positive

```
channel,device_id,duration_more_than_26,duration_quantized_19,duration_quantized_26,duration_quantized_5,duration_quantized_59,email,email_email_prefix,email_email_provider,event
_time,event_type,gid,ip,ip_ip_city,ip_ip_country,ip_is_from_datacenter,ip_prefix_22,is_same_country,knownbad,label,latitude,longitude,ostype,phone,phone_city,phone_country,phone_
postcode,phone_prefix_3,source,success,terminaltype,time_stamp_date,time_stamp_hour,uid
2,-5.41976403153e+18,false,10,0,10,0,,,,,2017-04-18 18:59:20,register,4,183.152.44.196,<E0><88><9F><E5><E1><B1><E5><B8><82>,<E4><B8><AD><E5><9B><BD>,false,183.152.44.0,true,: fals
e,bad,0,0,sim,1581867,<E6><B7><B1><E5><9C><B3>,China/<E4><B8><AD><E5><9B><BD>,518000,158,1,1,2,2017-04-18,2017-04-18 18:09:00,-4385323533386907648
1,8.04009947254e+18,true,37140,37140,37145,37100,45215983146ab18e09a987eb21bd8391,,,,,2017-04-20 15:43:59,register,"30857,34909,34910",1.180.215.93,Baolou,<F4><B8><AD><F5><9B><BD>,
false,1.180.212.0,true,: false,bad,0,0,,1473037,<E7><9F><E3><E5><AE><B6><E5><BA><B4>,China/<E4><B8><AD><E5><9B><BD>,050000,147,2,1,,2017-04-20,2017-04-20 15:00:00,-32793984784363
68383
1,,true,23880,23880,23880,23850,,,,,2017-04-18 10:33:42,register,"54650,163,54651,4242,19636",182.37.254.175,<F4><B8><B4><F6><B2><82><F5><B8><82>,<F4><B8><AD><F5><9B><BD>,false,18
2.37.252.0,true,: false,bad,0,0,,1703237,<E6><88><9C><E9><B3><BD>,China/<E4><B8><AD><E5><9B><BD>,610000,170,1,1,,2017-04-18,2017-04-18 10:00:00,-1798754768289197397
2,5.18130815457e+18,false,10,0,10,0,,,,,2017-04-19 17:43:01,register,18041,125.115.77.74,<E5><AE><B1><E5><B3><A2><E5><DB><B2>,<E4><DB><AD><E5><9B><BD>,false,125.115.76.0,true,: fa
lse,bad,0,0,sim,1570073,<E9><95><BF><F6><B2><99>,China/<F4><B8><AD><F5><9B><BD>,410000,157,1,1,2,2017-04-19,2017-04-19 17:00:00,2021256085410152452
1,,true,50920,50920,50920,50900,,,,,2017-04-19 13:41:34,register,"41963,3783",171.211.101.31,<E5><BE><B7><E9><98><D3><E5><B8><82>,<E4><DB><AD><E5><9B><BD>,false,171.211.100.0,true
,: false,bad,0,0,,1719451,<E5><93><B8><E5><B0><94><E6><BB><AB>,China/<E4><B8><AD><E5><9B><BD>,150000,171,1,1,,2017-04-19,2017-04-19 13:00:00,-4477480007556573856
2,6.70855316048e+18,false,0,0,5,0,,,,,2017-04-20 08:49:18,register,"6831,16608",218.63.66.182,<E7><8E><B9><E6><BA><AA><E5><B8><82>,<E4><B8><AD><E5><9B><BD>,false,218.63.64.0,true,
: false,bad,0,0,sim,1554472,<E9><82><AF><E9><B3><B0>,China/<E4><B8><AD><E5><9B><BD>,050000,155,1,1,2,2017-04-20,2017-04-20 08:00:00,-325003769452953593
1,,true,23710,23700,23710,23700,,,,,2017-04-17 14:07:16,register,"11,12,13,14",144.52.130.158,<E4><B8><B4><F6><B2><82><F5><B8><82>,<F4><B8><AD><F5><9B><BD>,false,144.52.128.0,true
,: false,bad,0,0,,1351776,<E7><99><BE><E8><B9><B2>,China/<E4><B8><AD><E5><9B><BD>,533000,135,1,1,,2017-04-17,2017-04-17 14:00:00,2775022301951819784
2,-8.50030767799e+18,false,10,0,10,0,,,,,2017-04-20 15:14:10,register,4035,102.41.111.17,<E6><B5><B8><E5><AE><B1><E5><DB><B2>,<E4><DB><AD><E5><9B><BD>,false,102.41.108.0,true,: fa
lse,bad,0,0,sim,1706510,<E6><B5><B7><E5><BF><A3>,China/<E4><B8><AD><E5><9B><BD>,571000,170,1,1,2,2017-04-20,2017-04-20 15:00:00,4612993339438399497
```



# Works for both algorithm experts and domain experts

- Why do users belong to the same group?
- What are the important features?
- What did they do as a fraud group?
- Do they have some correlations?
- Is the user good or not?



domain experts

- What causes the form of a fraud group?
- What are the distributions of the important features?
- Do users in the same group share the same pattern?
- Will members in one group build a strange network?
- Did I make a mistake for this user?



algorithm experts

# Works for both algorithm experts and domain experts

- Why do users belong to the same group?
- **What are the important features?**
- What did they do as a fraud group?
- Do they have some correlations?
- Is the user good or not?



domain experts

- What causes the form of a fraud group?
- **What are the distributions of the important features?**
- Do users in the same group share the same pattern?
- Will members in one group build a strange network?
- Did I make a mistake for this user?



algorithm experts

# Works for both algorithm experts and domain experts

- Why do users belong to the same group?
- **What are the important features?**
- What did they do as a fraud group?
- **Do they have some correlations?**
- Is the user good or not?



domain experts

- What causes the form of a fraud group?
- **What are the distributions of the important features?**
- Do users in the same group share the same pattern?
- **Will members in one group build a strange network?**
- Did I make a mistake for this user?



algorithm experts

# Works for both algorithm experts and domain experts

- Why do users belong to the same group?
- **What are the important features?**
- What did they do as a fraud group?
- **Do they have some correlations?**
- **Is the user good or not?**



domain experts

- What causes the form of a fraud group?
- **What are the distributions of the important features?**
- Do users in the same group share the same pattern?
- **Will members in one group build a strange network?**
- **Did I make a mistake for this user?**



algorithm experts

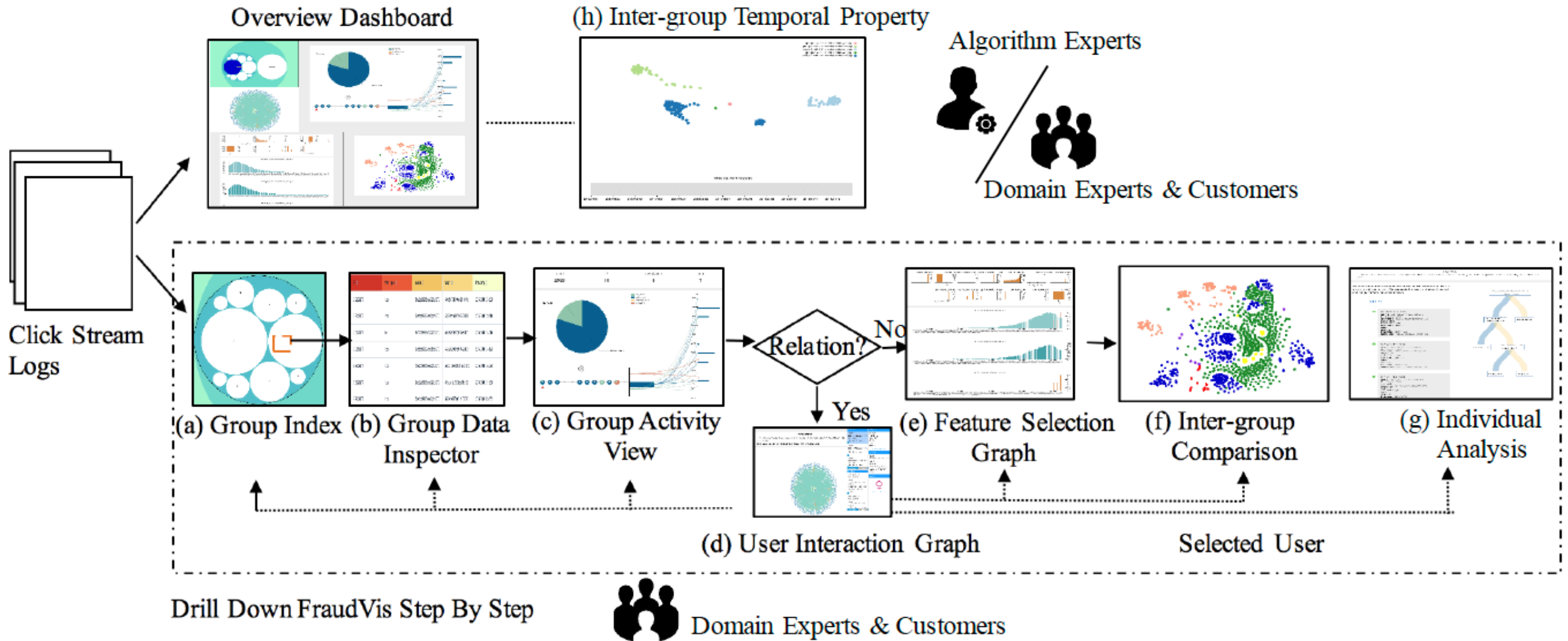


We need  
**VISUALIZATION!**

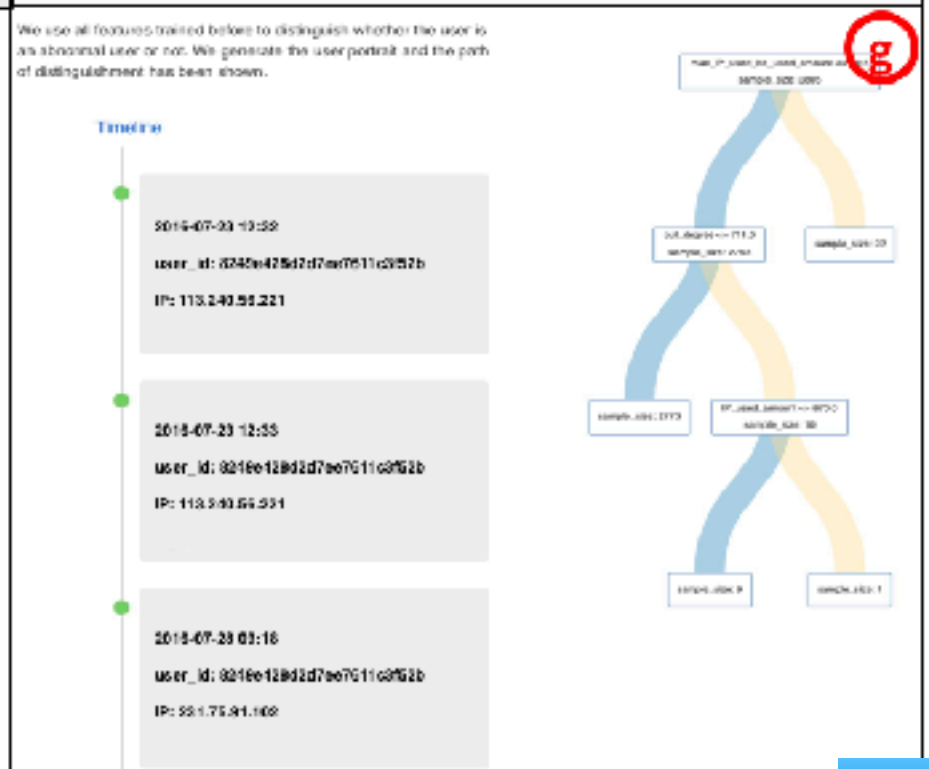
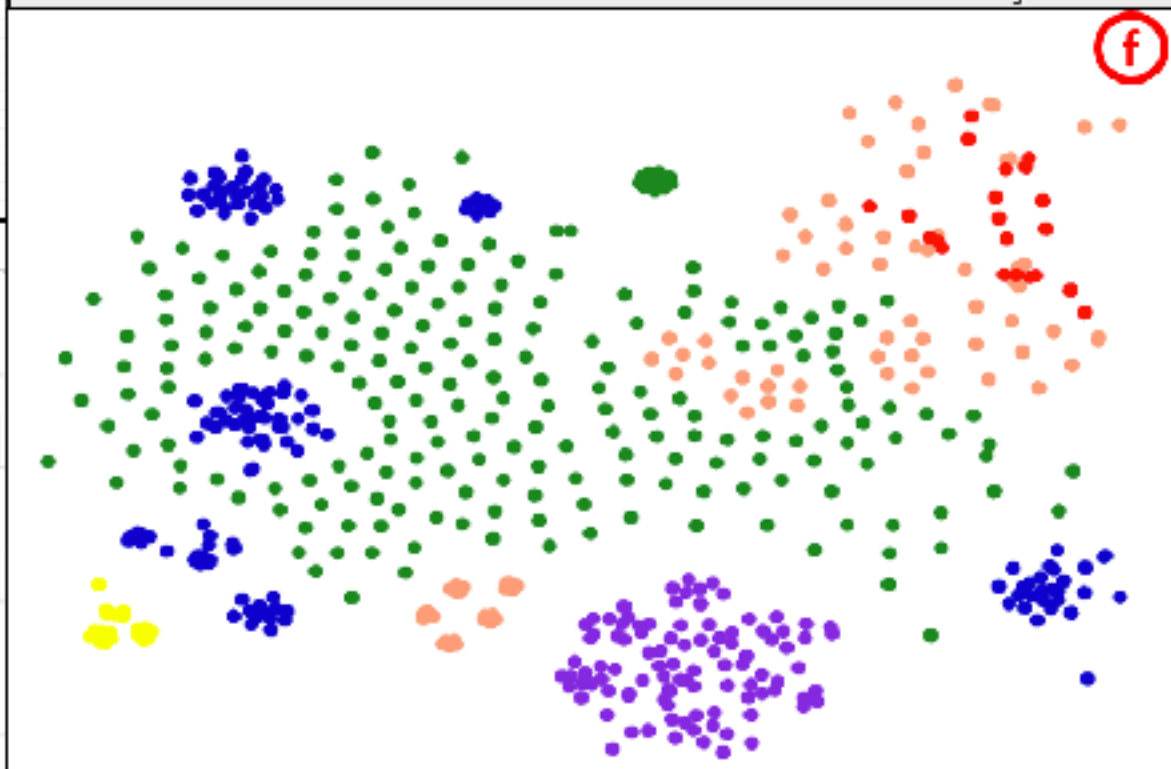
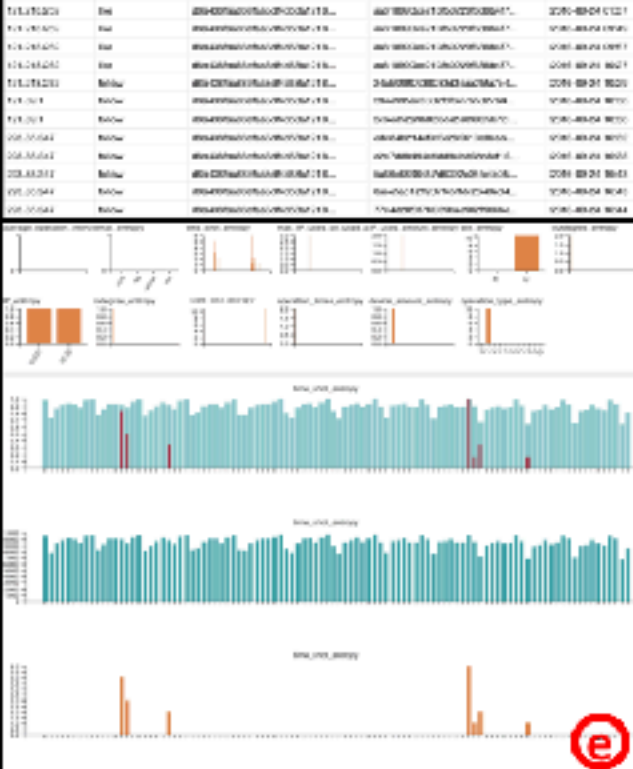
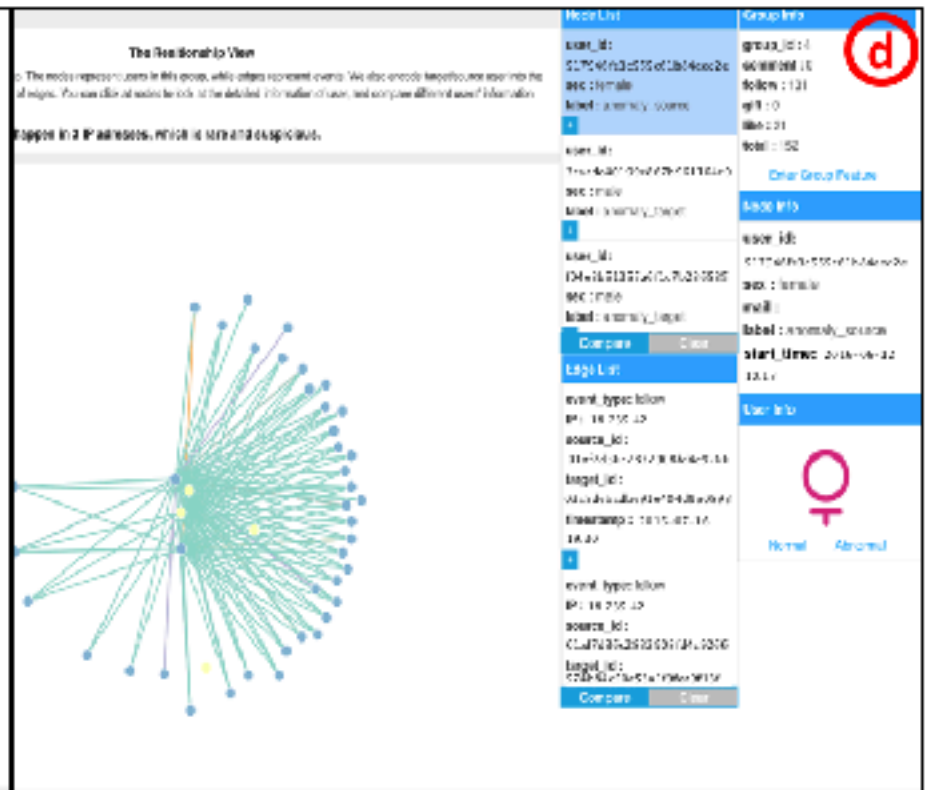
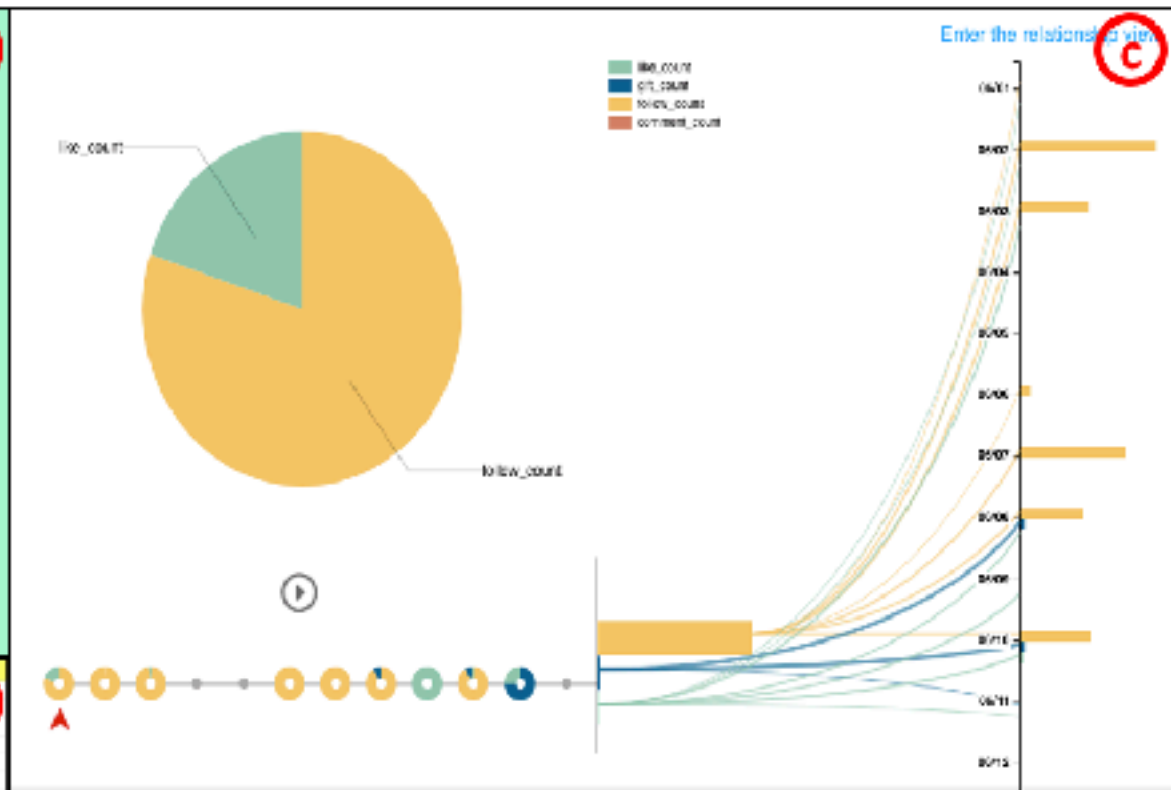
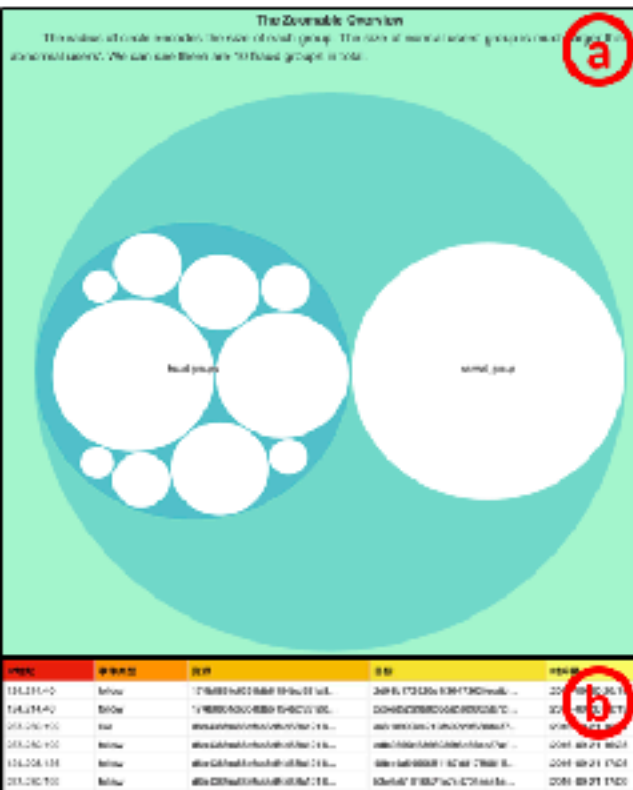
# Main contributions

- Comprehensive analysis
  - Inter-group, intra-group, individual
  - Correlation, temporal, spatial
- Visualization interpretation of algorithm result through customized interactions
  - Instructions
  - Different dashboards
- Evaluation through real-world data sets and algorithms

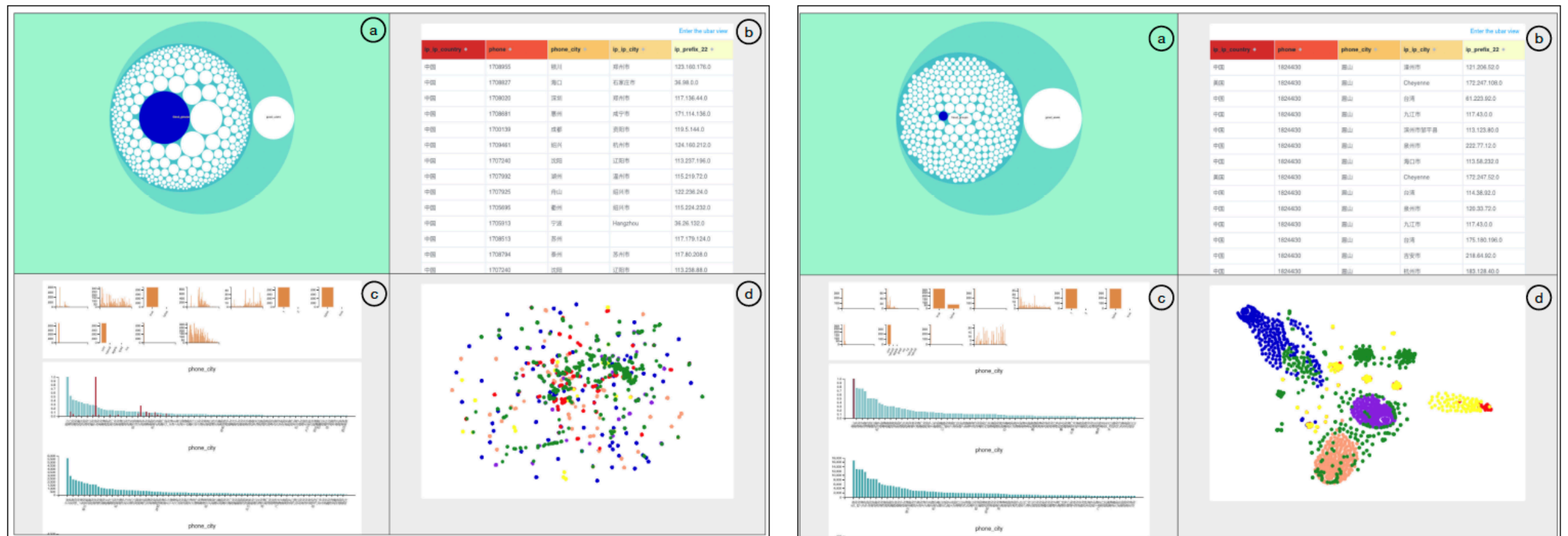
# Workflow



# Overview Dashboard



# Case study 2: E-commerce Website



(a) stock k-means

(b) improved

- The distribution of the most important feature hardly differ from the overall distribution
- Members from different groups are mixed together and hard to separate
- Large fraud group containing many users that are not similar



# Conclusion

- We solve two main problems
  - How to explain the fraud behavior to domain users with little technology background?
  - How to test the result of various fraud detection algorithms and discover the fundamental features?
- A fresh view and a working system to display high-dimensional fraud behaviors
- Visually interpret and compare the result of unsupervised fraud detection algorithms

# The future of Fraud Detection

Good detection algorithms



**VISUALIZATION**



# Thanks & QA



Jiao Sun - <https://sunjiao123sun.github.io>

Email: j-sun16@mails.tsinghua.edu.cn

All kinds of collaboration are welcomed! 😊