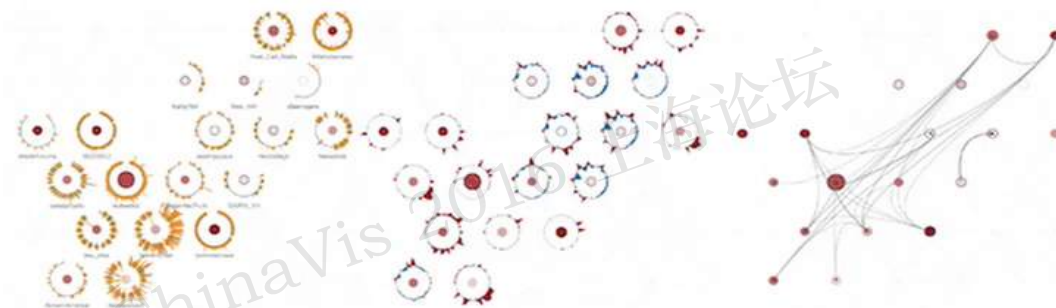


VisSec: When Visualization Meets Security



Nan Cao, NYUSH VisLab
Assistant Professor, NYU ShangHai
Research Assistant Professor, NYU Tandon
<http://nancao.org>

My Research



TargetVue (IEEE VAST 2015)

Graph, Multidimensional Data, Text
InfoVis, Visual Analytics, HCI, Data Mining

InfoSec in Our Daily Life



互联网主机入侵检测



金融欺诈的检测与分析

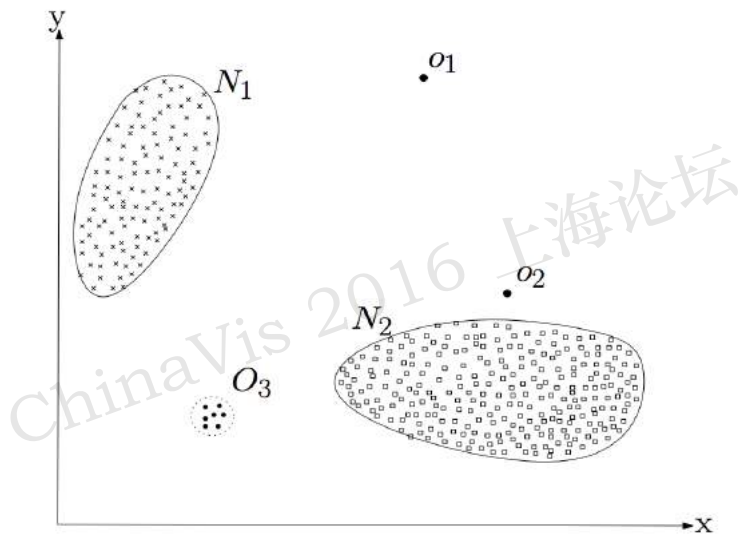


为电商检测潜在的
不良商家或消费者



社交媒体分析潜在的
异常用户行为

Anomaly Detection



Anomaly detection (or outlier detection) is the identification of items, events or observations which do not conform to an expected pattern or other items in a dataset

-- Wikipedia

Key Challenges

- It is difficult to define what is normal or abnormal
- Unavailable of ground truth or labelled data making results validation difficult

**Information visualization can be a
good aid to these challenges**

Do you trust your friends in social media ?

“On the Internet, Nobody Knows You’re a Dog”: A Twitter Case Study of Anonymity in Social Networks

Sai Teja Peddinti*
psaiteja@nyu.edu

*Dept. of Computer Science and Engineering, NYU
Brooklyn, New York, USA

Keith W. Ross**†
keithwross@nyu.edu

Justin Cappos*
jcappos@nyu.edu

†NYU Shanghai
Shanghai, China

(ACM Conference on Online Social Networks, 2014)

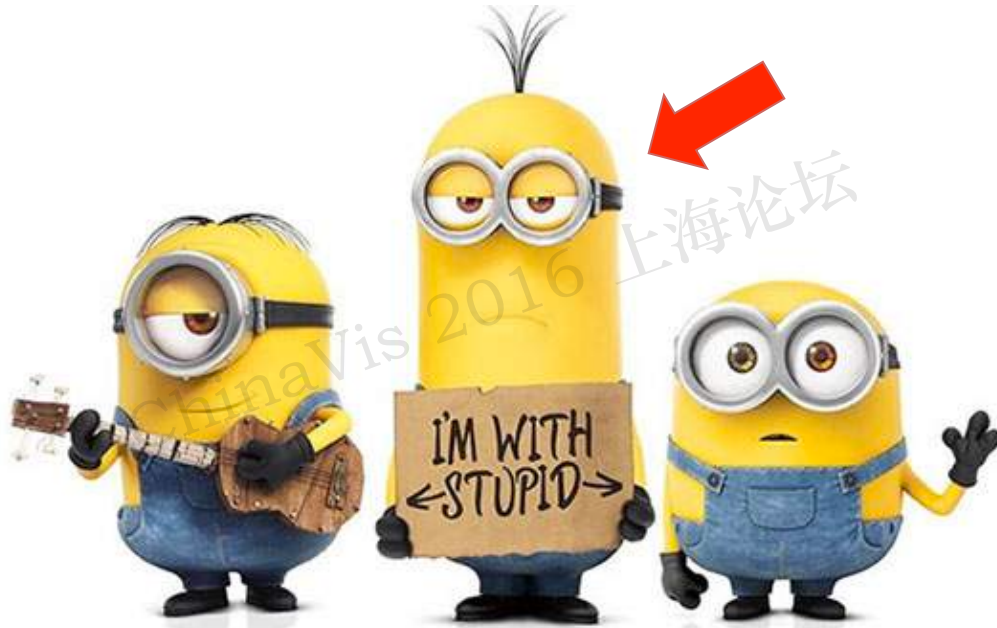


"On the Internet, nobody knows you're a dog."

An adage since 1993

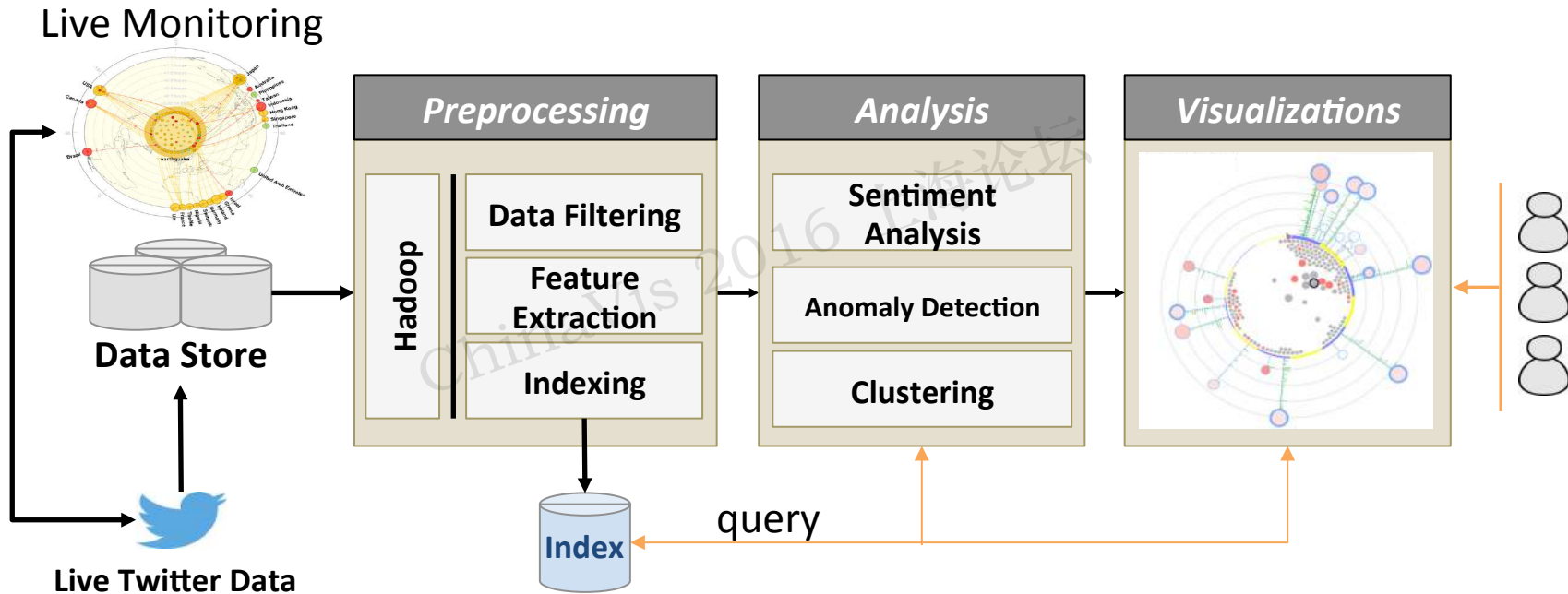
***Anonymous users are potential
threats to the society***

Research Goal

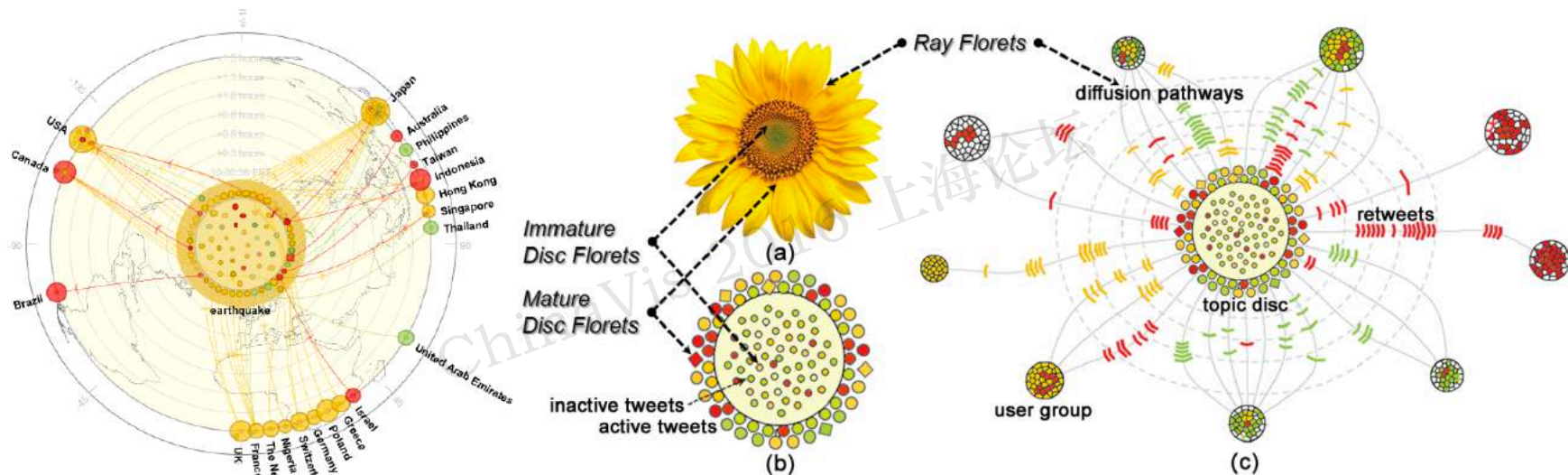


**Finding users with anomalous behaviors
on social media (e.g. Twitter)**

System Overview



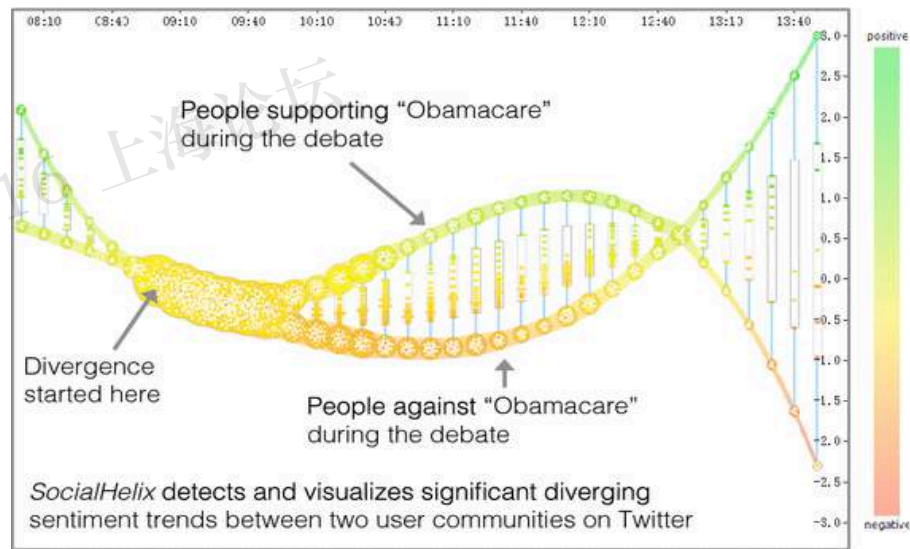
Whisper (2012)



"Whisper: Tracing the Spatiotemporal Process of *Information Diffusion* in Real Time",
IEEE Transactions on Visualization and Computer Graphics. TVCG, InfoVis 2012.

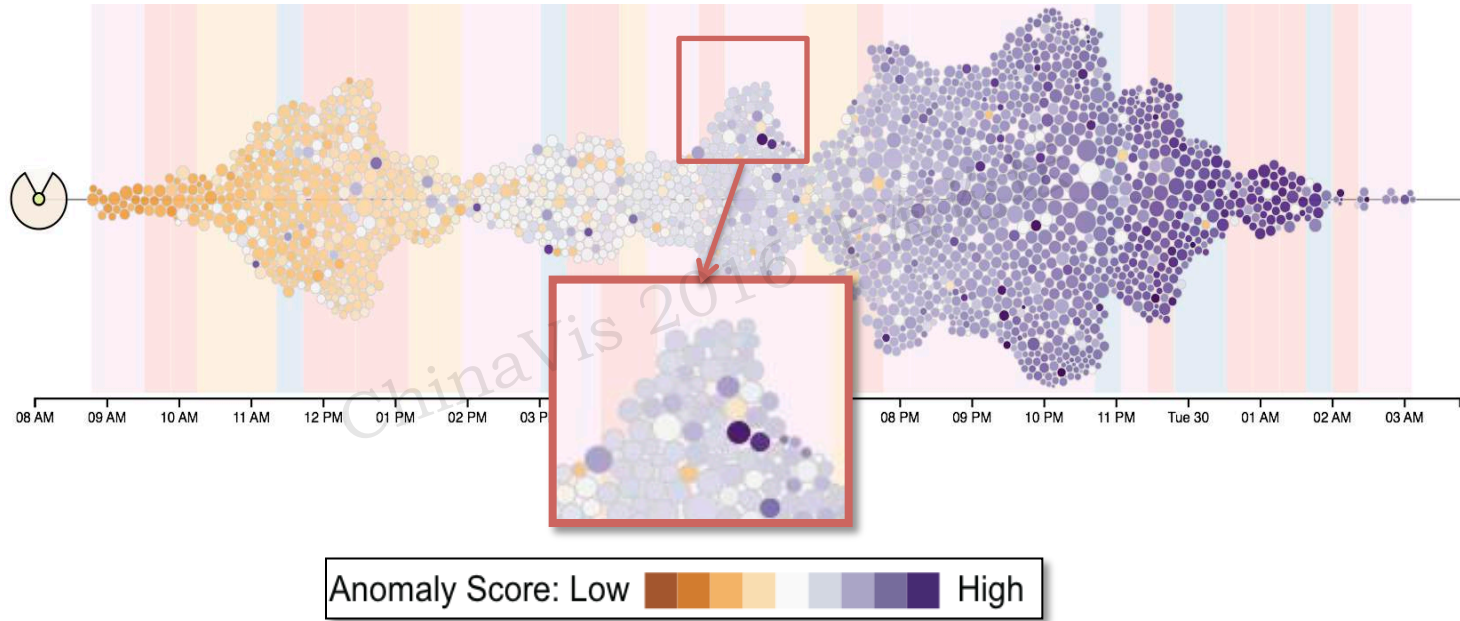
SocialHelix (2013)

Divergence of sentiments about "Obamacare" during the 2012 US presidential debate (October 3, 2012)



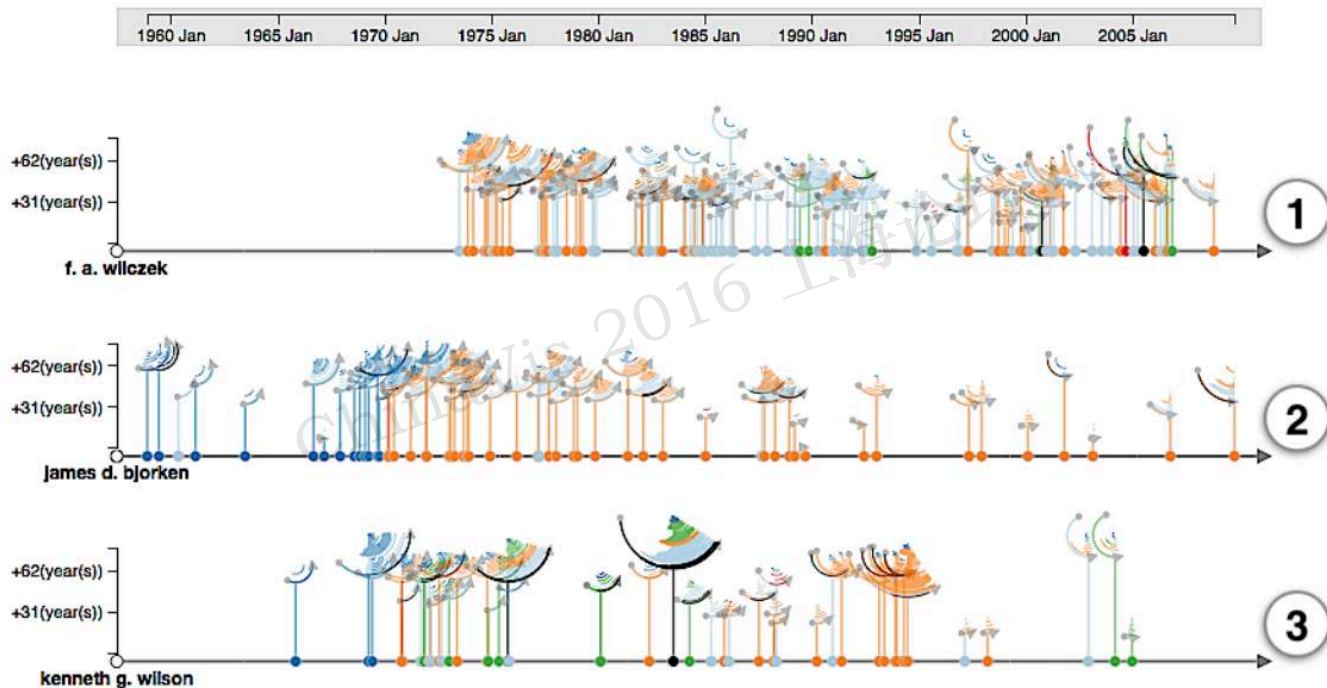
"SocialHelix: Visual Analysis of *Sentiment Divergence* in Social Media",
Journal of Visualization, May 2015, Volume 18, Issue 2, pp 221-235

FluxFlow (2014)



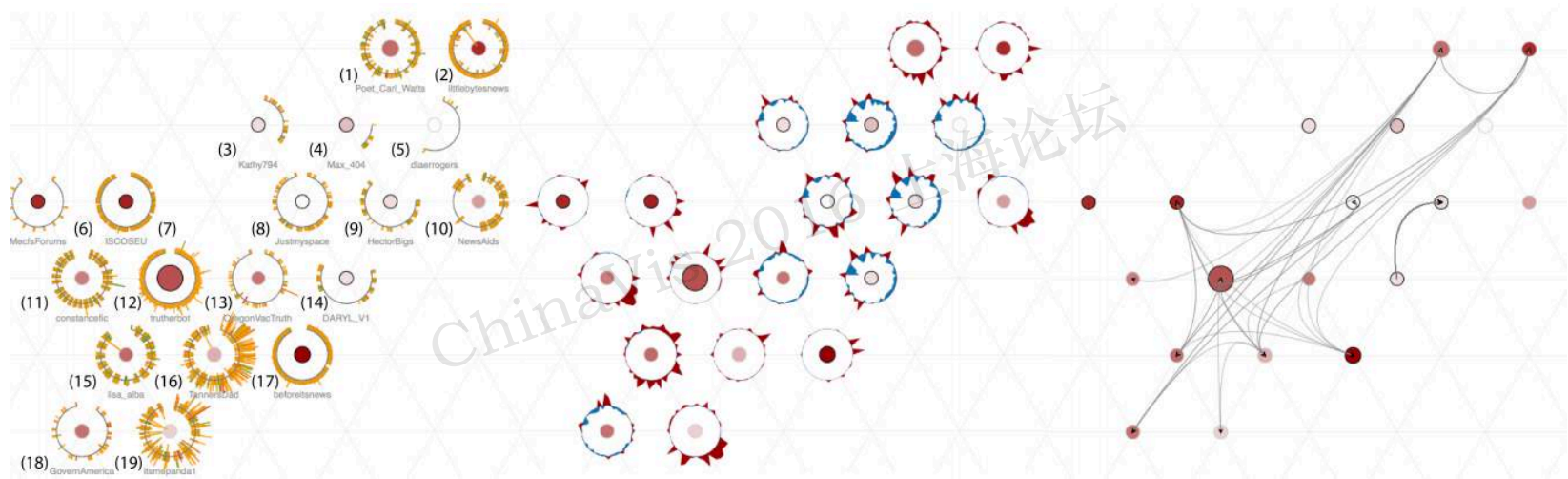
#FluxFlow: Visual Analysis of **Anomalous Information Spreading** on Social Media, TVCG, IEEE VAST 2014 (**Honorable Mention**)

Episogram (2014)



"Episogram: Visual Summarization of *Egocentric Social Interactions*"
IEEE Computer Graphics and Applications

TargetVue (VAST 2015)

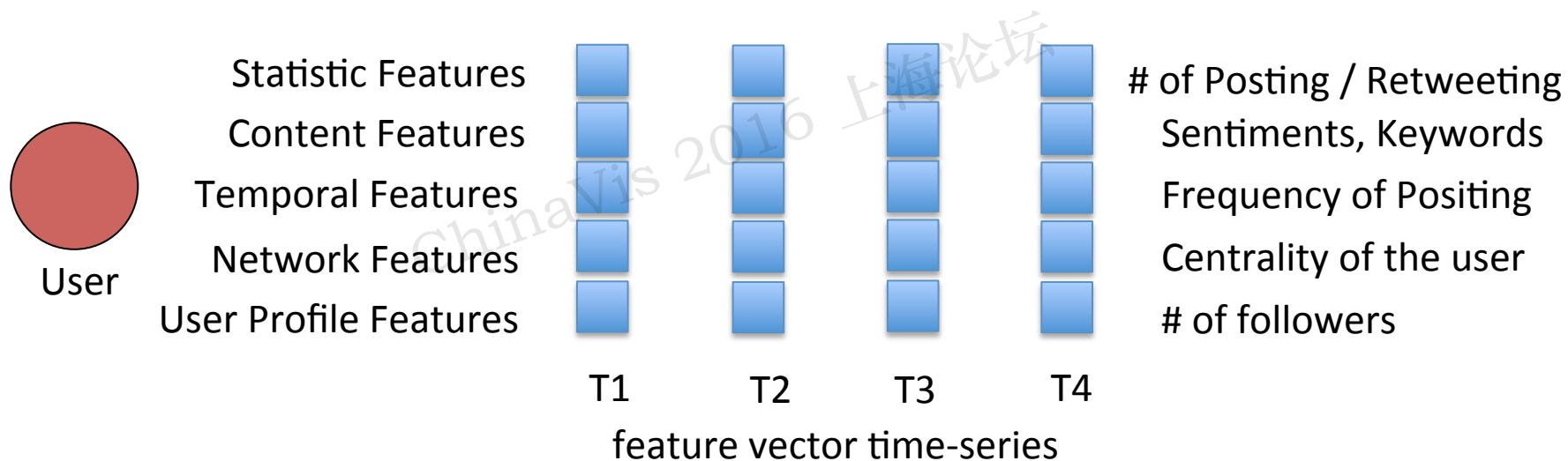


TargetVue: Visual Analysis of *Anomalous User Behaviors* in Online Communication Systems, TVCG 2016

User Behaviors

- Posting (Tweeting)
 - Create a message and post it to others
- Responding (Replying / Retweeting)
 - Spread the messages posted by others

Capturing User Behaviors via Features



Anomaly Detection

TLOF: Temporal Local Outlier Factor

$$s(X) = \alpha \cdot Z_1(X) + (1 - \alpha) \cdot Z_2(X)$$

$$Z_1(X) = LOF(x_T) - \sum_{t=T-W}^{t=T-1} LOF(x_t) / W$$

$$Z_2(X) = 1 - P_N(LOF(x_T), \mu, \sigma)$$

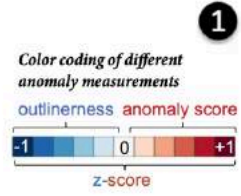
The TLOF gives an anomaly measurement for every users by identifying the features that are significantly different from other users in the test data and the past history of his own

Breunig, Markus M., et al. "LOF: identifying density-based local outliers." ACM sigMOD record. Vol. 29. No. 2. ACM, 2000.

ChinaVis 2016 上海论坛

Introduction
Visualization Design
Evaluation

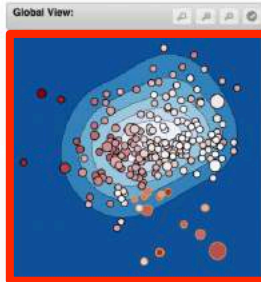
User Interface



2

Users Tweets

	ID: 12996172 Name: lilsibylnews Anomaly: 0.62 Sentiment: 0.02 Followers: 23404 Impact: 253 Posts: 4311 Activity: 2015-02-17 00:08:43 2015-03-04 00:19:54
	ID: 72552866 Name: USRealityCheck Anomaly: 0.72 Sentiment: 0.02 Followers: 86263 Impact: 44 Posts: 1875 Activity: 2015-02-17 00:19:52 2015-03-04 07:48:48
	ID: 477583514 Name: Intubot Anomaly: 0.67 Sentiment: 0.01 Followers: 238831 Impact: 1700 Posts: 1995 Activity: 2015-02-17 00:08:43



3

Users Tweets

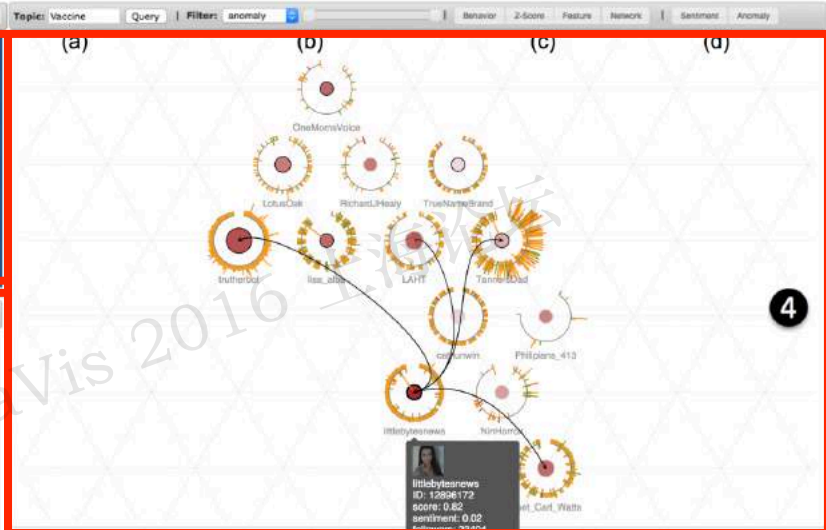
news

tcot

lilsibylnews
Israel: Foot #foot Technical Difficulties in Jerusalem Fire Hotline
<http://t.co/ny7aOgC01>
2015-02-17 00:08:43 Retweet Beak Favorite

lilsibylnews
Breitbart: Louisiana's Next Senator, Bill Cassidy: GOP is Party for the Working Person
<http://t.co/cArW0xb>
2015-02-17 00:08:45 Retweet Beak Favorite

lilsibylnews
USPolitics: Protest of chokehold death turns violent in California
<http://t.co/y77KdL3k>



5

Propagation: 0.00 Feature Variance

lilsibylnews

Intubot

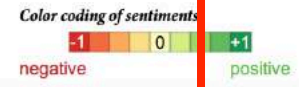
USRealityCheck

lilsibylnews

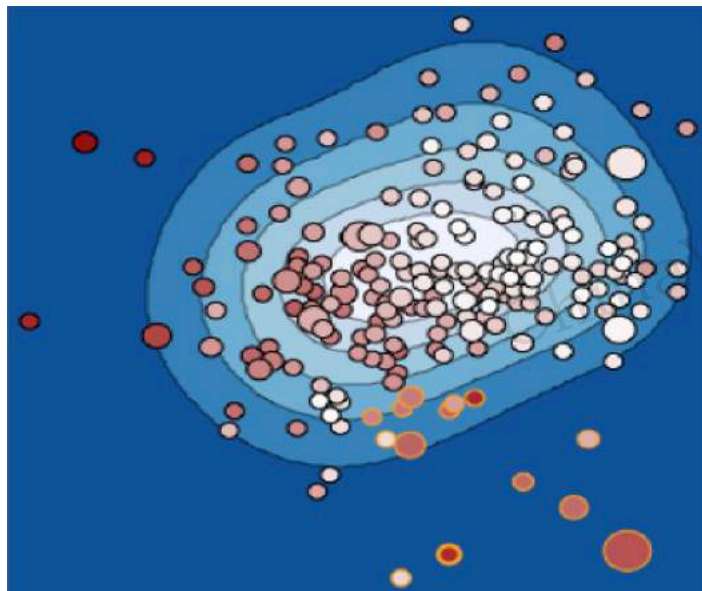
USPolitics: Protest of chokehold death turns violent in California
<http://t.co/y77KdL3k>

lilsibylnews
ID: 12996172
Anomaly: 0.62
Sentiment: 0.02
Followers: 23404
Impact: 253
Posts: 4311
Activity: 2015-02-17 00:08:43
2015-03-04 00:19:54

6



The Overview



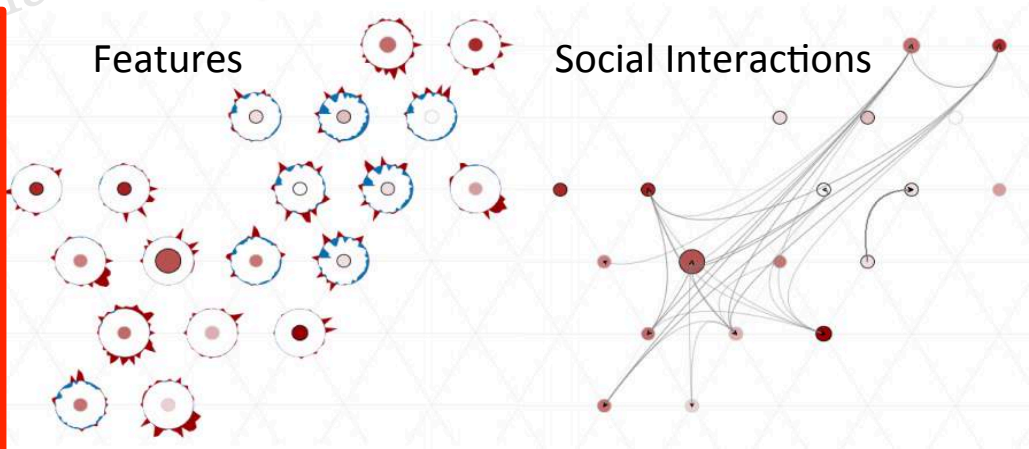
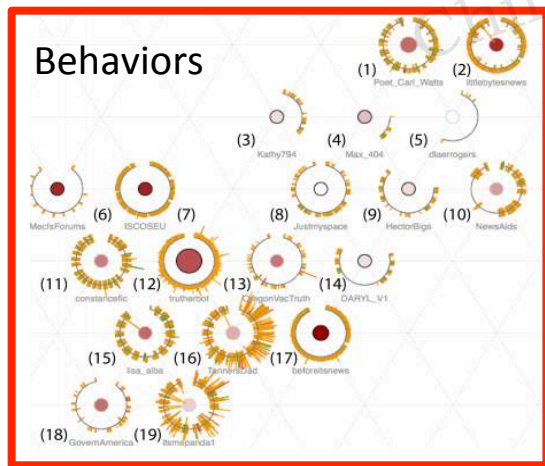
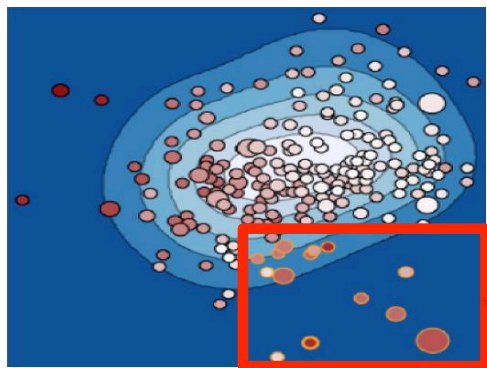
Multidimensional Scaling

$$\min_{\mathbf{x}_1, \dots, \mathbf{x}_J} \sum_{i < j} (\underbrace{\|\mathbf{x}_i - \mathbf{x}_j\|}_{\text{Screen Distance}} - \underbrace{\delta_{i,j}}_{\text{Distance in feature space}})^2.$$

Screen Distance

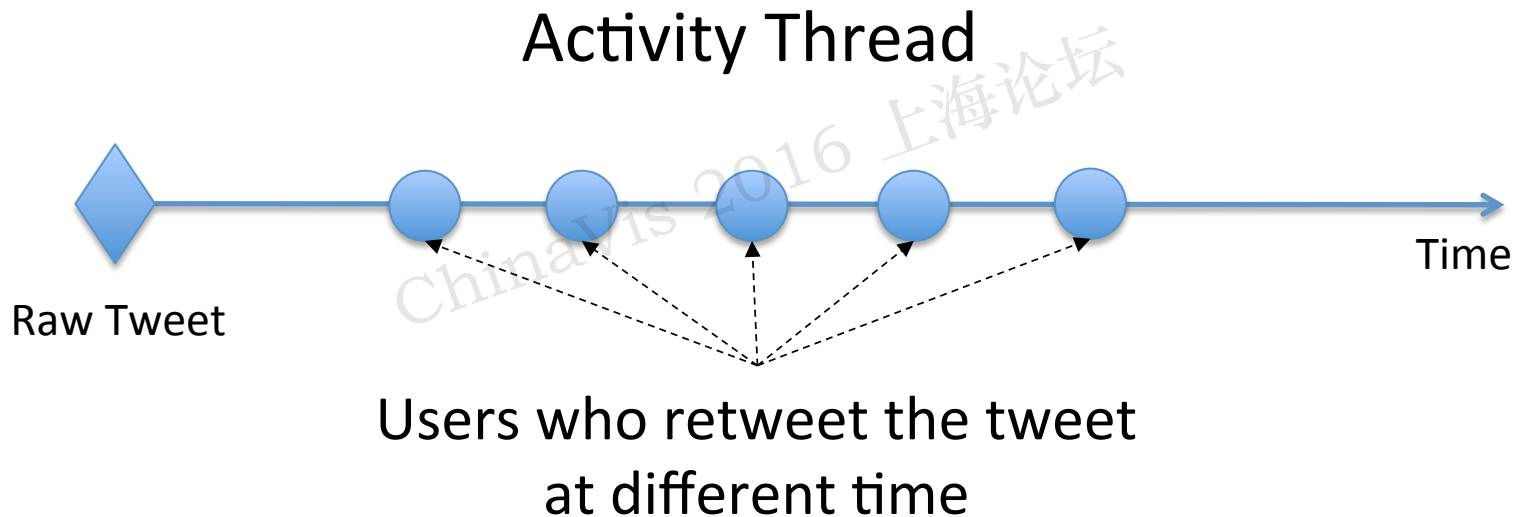
Distance in
feature space

The Inspection View

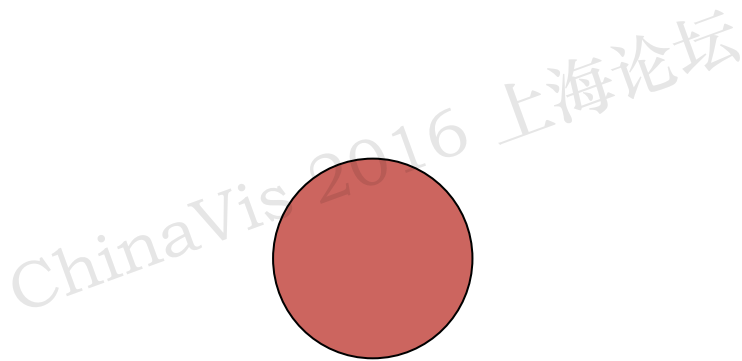


VisVis 2016 上海论坛

Showing Posting and Retweeting Activities

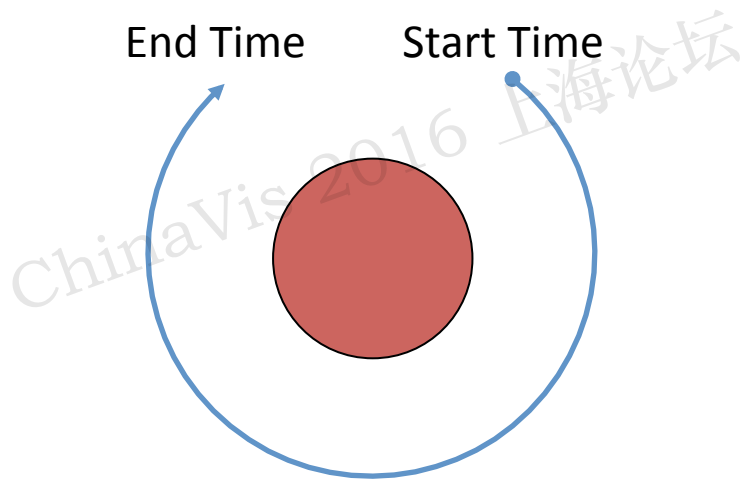


Showing Posting and Retweeting Activities



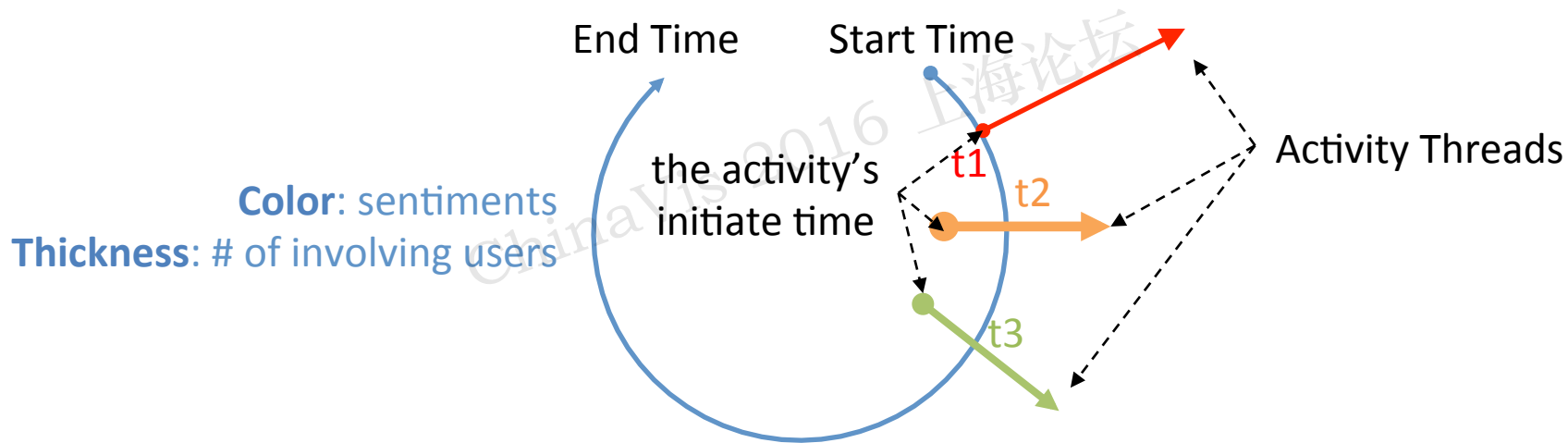
A user is visualized as circle sized by their importance and colored by their anomaly score

Showing Posting and Retweeting Activities

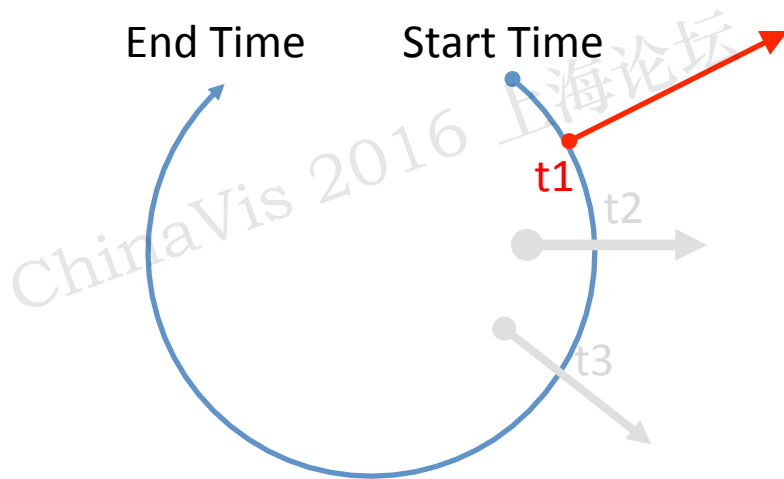


The centric user's activity history is recorded in a circular timeline

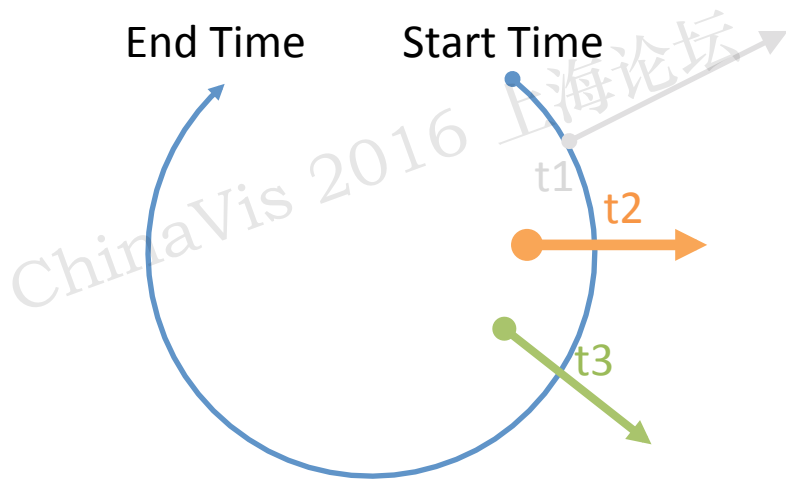
Showing Posting and Retweeting Activities



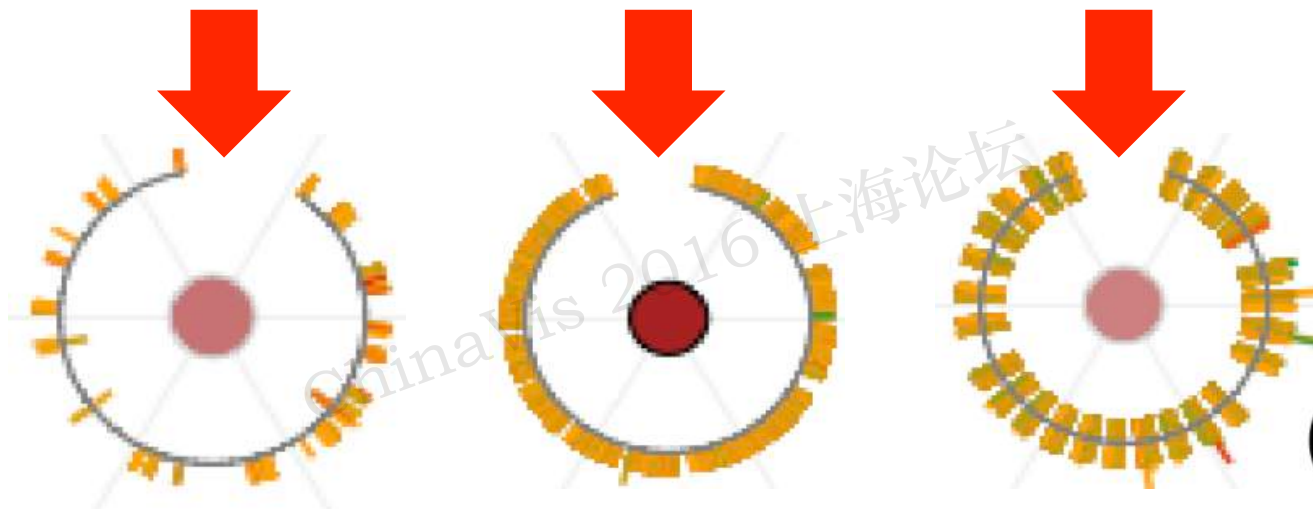
Showing Posting and Retweeting Activities



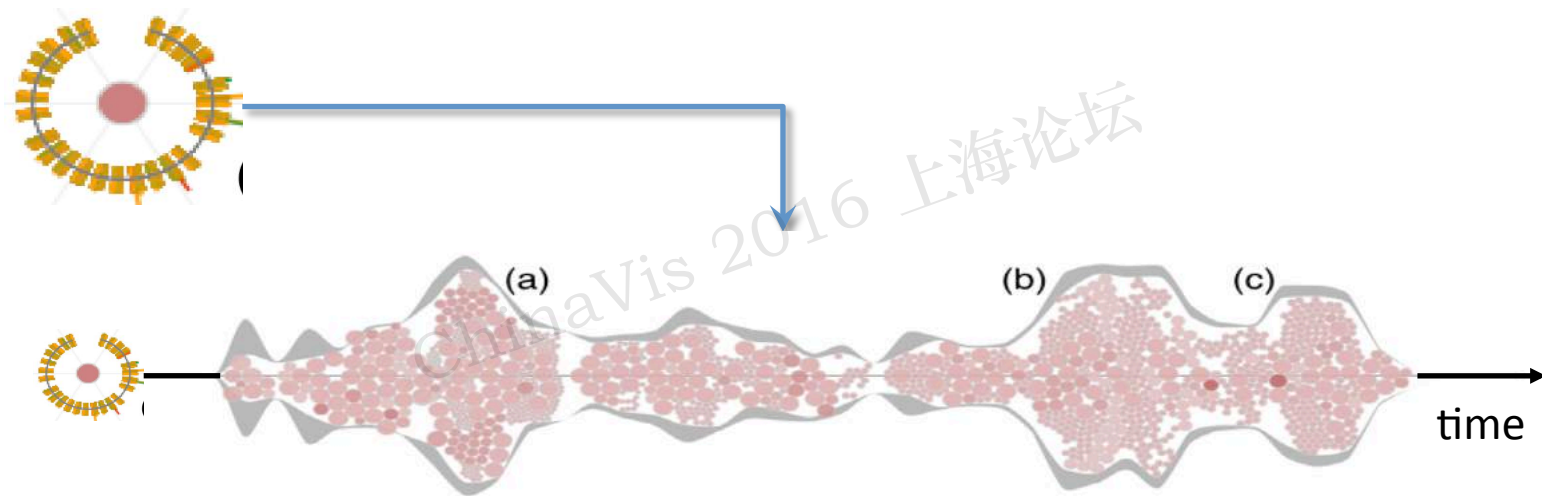
Showing Posting and Retweeting Activities



Who is the normal user?

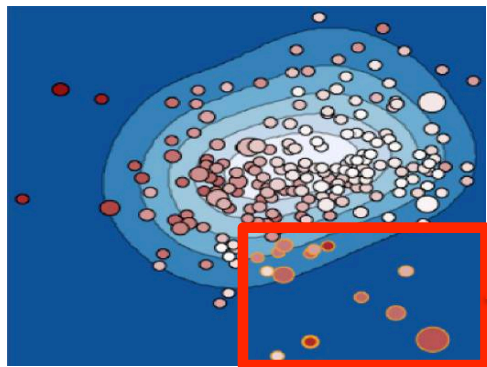


Context View 1: Showing Activity Dynamics

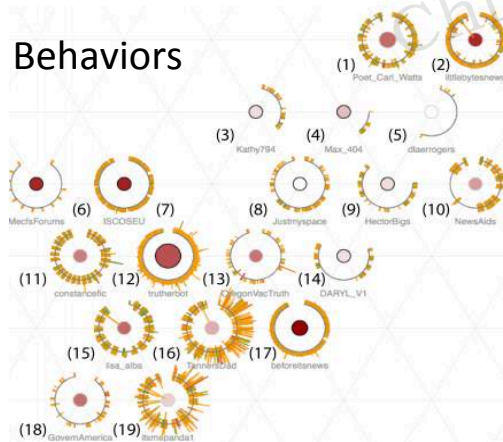


Aggregate all the activity threads and align all the involving users together along a timeline

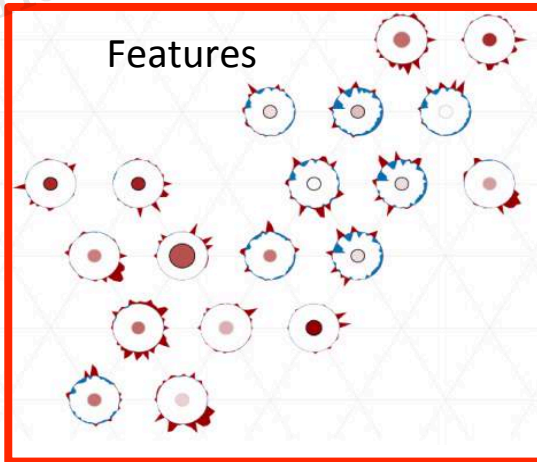
The Inspection View



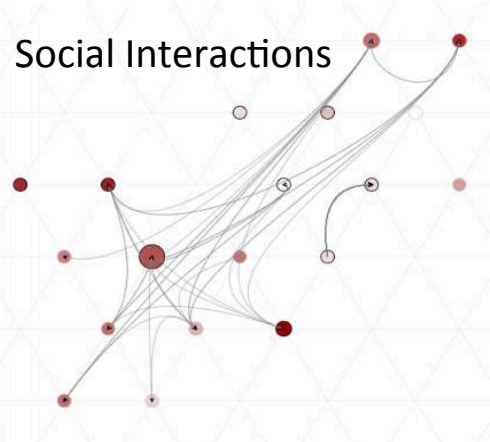
Behaviors



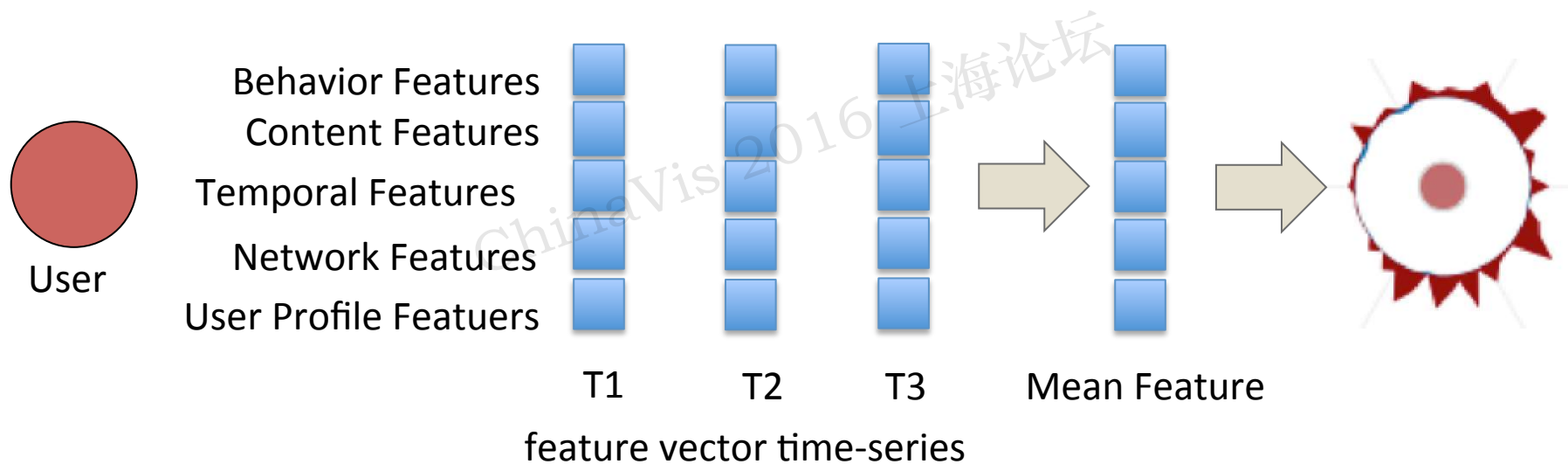
Features



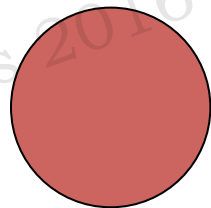
Social Interactions



Showing a User's Features

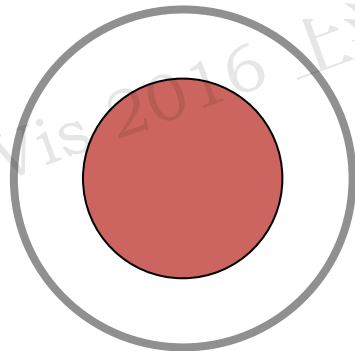


Visualizing a User's Features



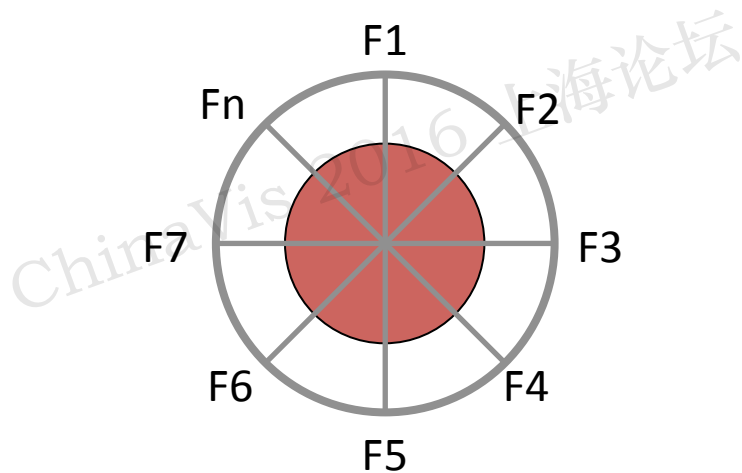
A user is visualized as circle sized by their importance and colored by their anomaly score

Visualizing a User's Features



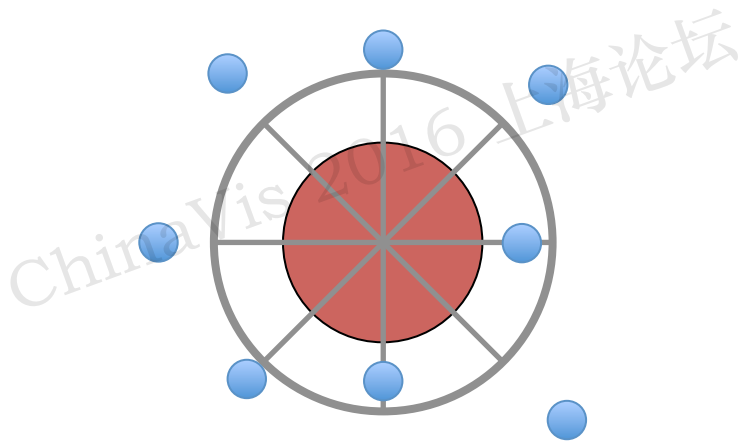
Using a baseline circle to indicate the mean feature values over all the users

Visualizing a User's Features



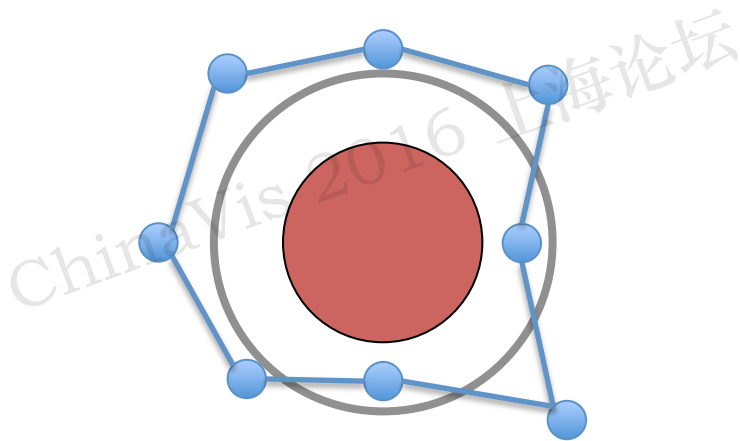
Feature axes are radially arranged

Visualizing a User's Features



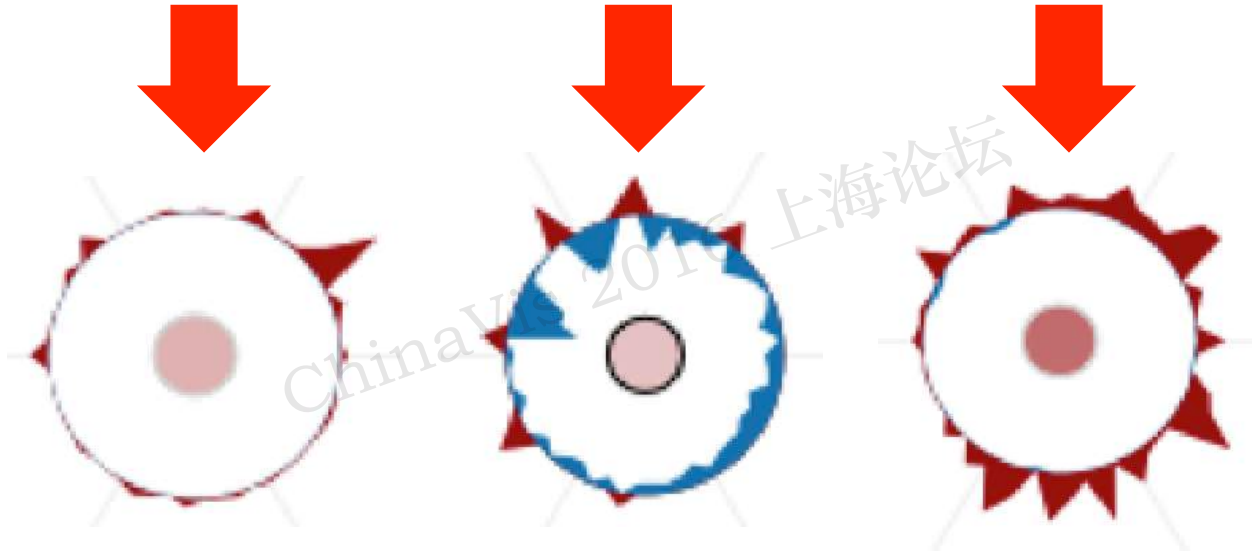
Plot the user's feature values along the feature axes surrounding the baseline

Visualizing a User's Features

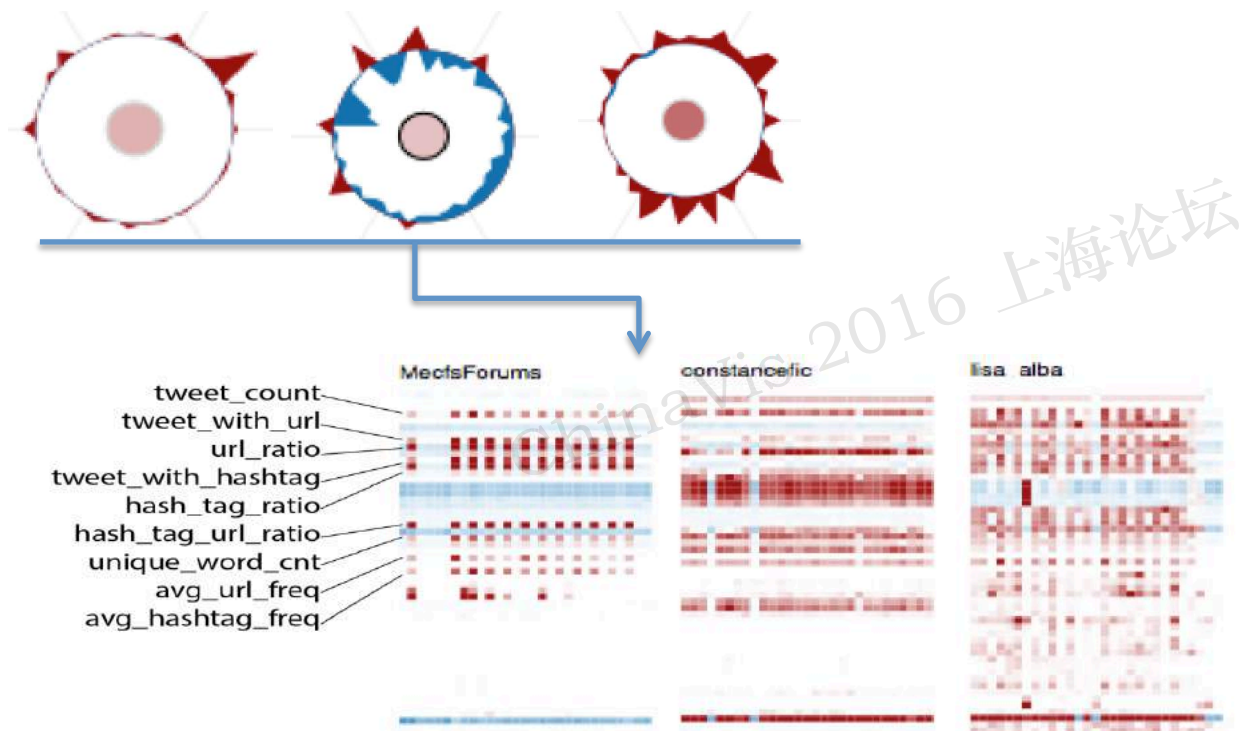


Connecting the data points to produce the feature glyph

Who is the normal user?



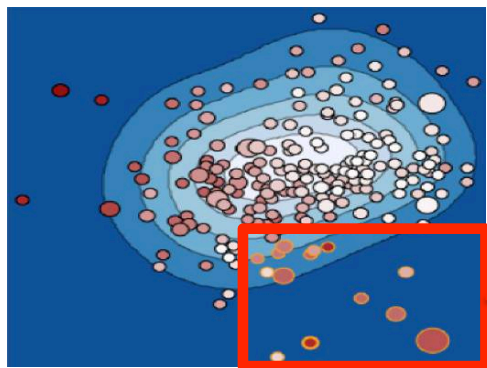
Context View 2: Showing Feature Dynamics



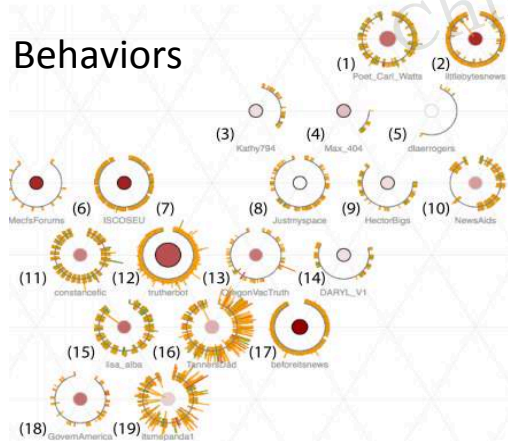
- Each user is shown as a heatmap
- **Row:** different features
- **Column:** different timestamp
- **Cell Color:** feature values (red: larger than mean, blue: smaller than mean)

Showing the change of users' features over time in a heatmap

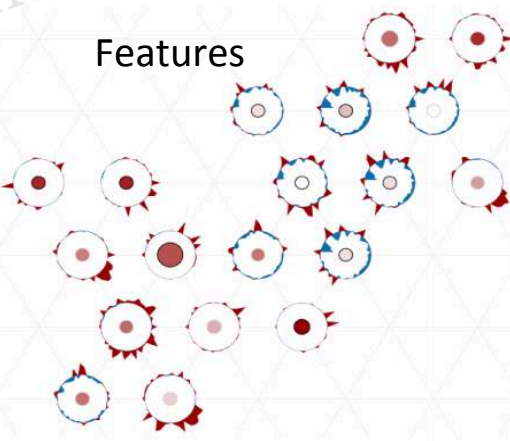
The Inspection View



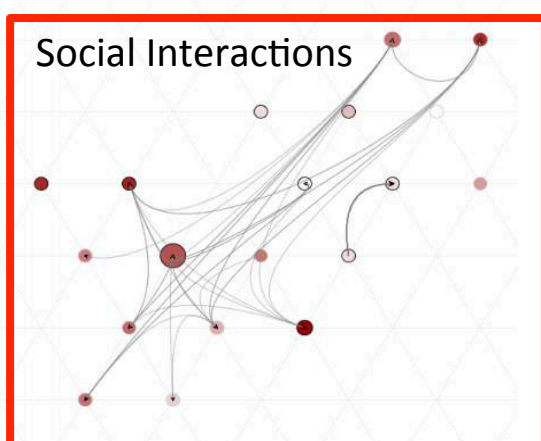
Behaviors



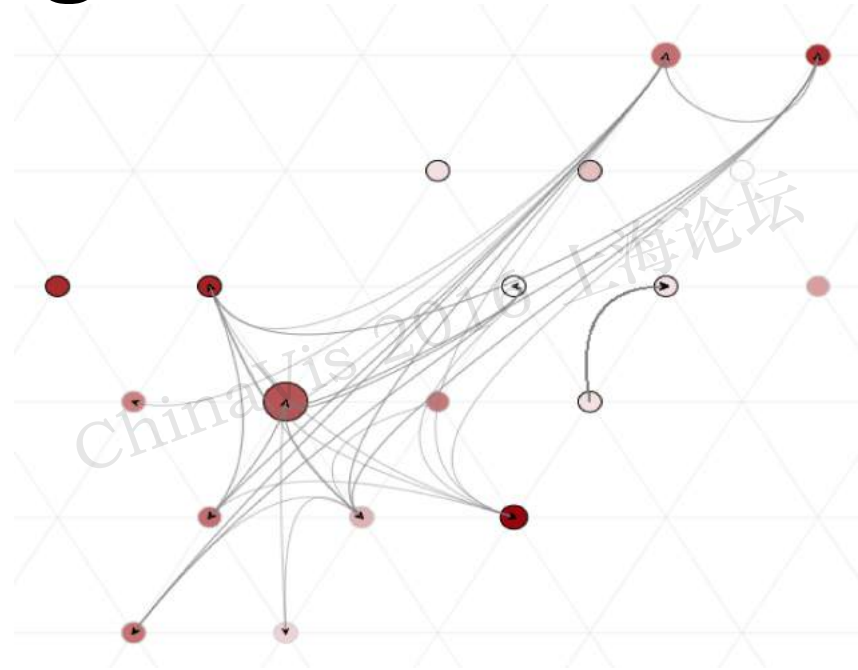
Features



Social Interactions



Showing the Social Interactions

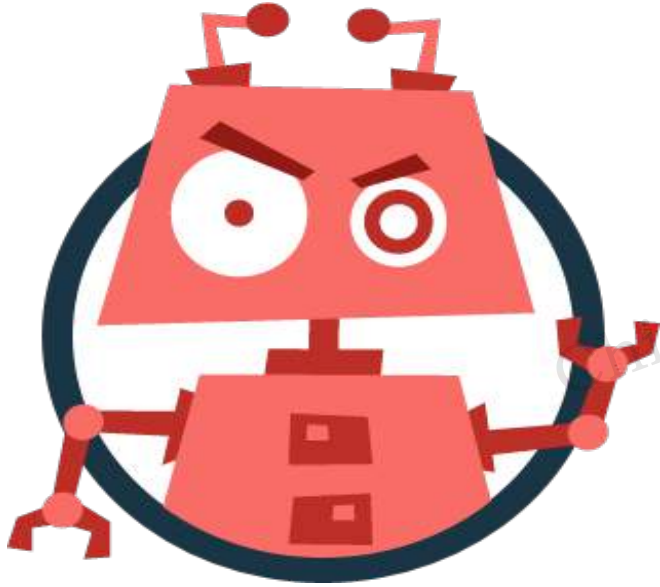


- Nodes indicate users
- Links indicate their social interactions (retweet/following)

ChinaVis 2016 上海论坛

Introduction
Visualization Design
Evaluation

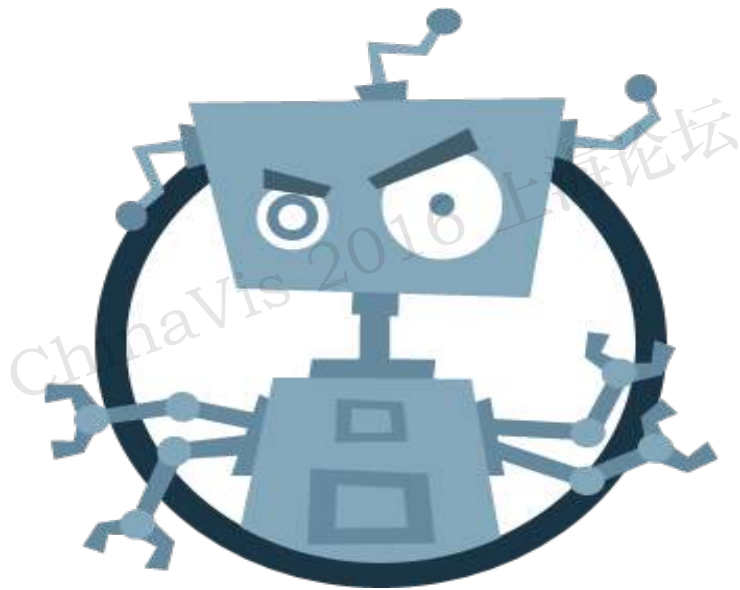
Evaluation: Bot Detection Challenge



Bot Influence Challenge

- The goal of the influence challenge was to
 - design social bots in Twitter to promote the advantages of vaccination
 - influence a target network of users who are supporters of anti-vaccine
- Lasted for a month during Dec 2014
- 8000 target users, 4 million tweets

Evaluation



Bot Detection Challenge



Social Bot Detection Challenge

Detect fully automated social bot
twitter to **promote the advantage**
vaccination and **influence a target**
network of users who tweet or re
messages of anti-vaccine nature.

Goal:

ChinaVirus

Iteratively Model Tuning

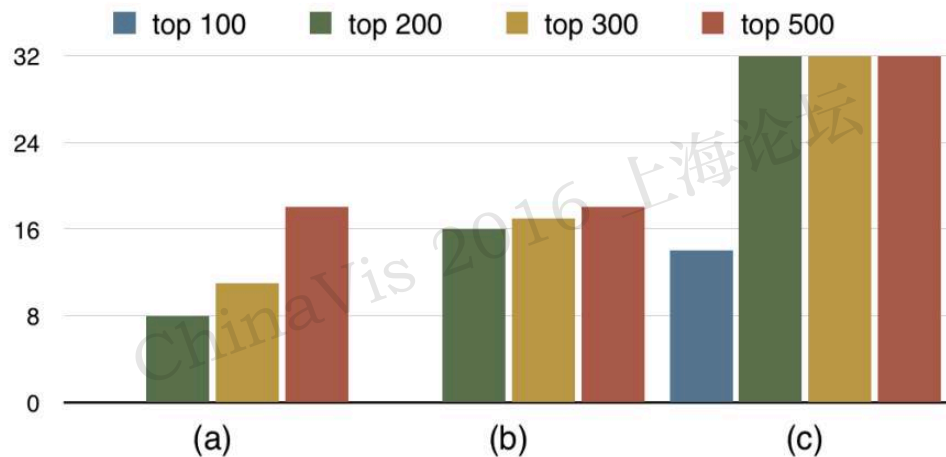
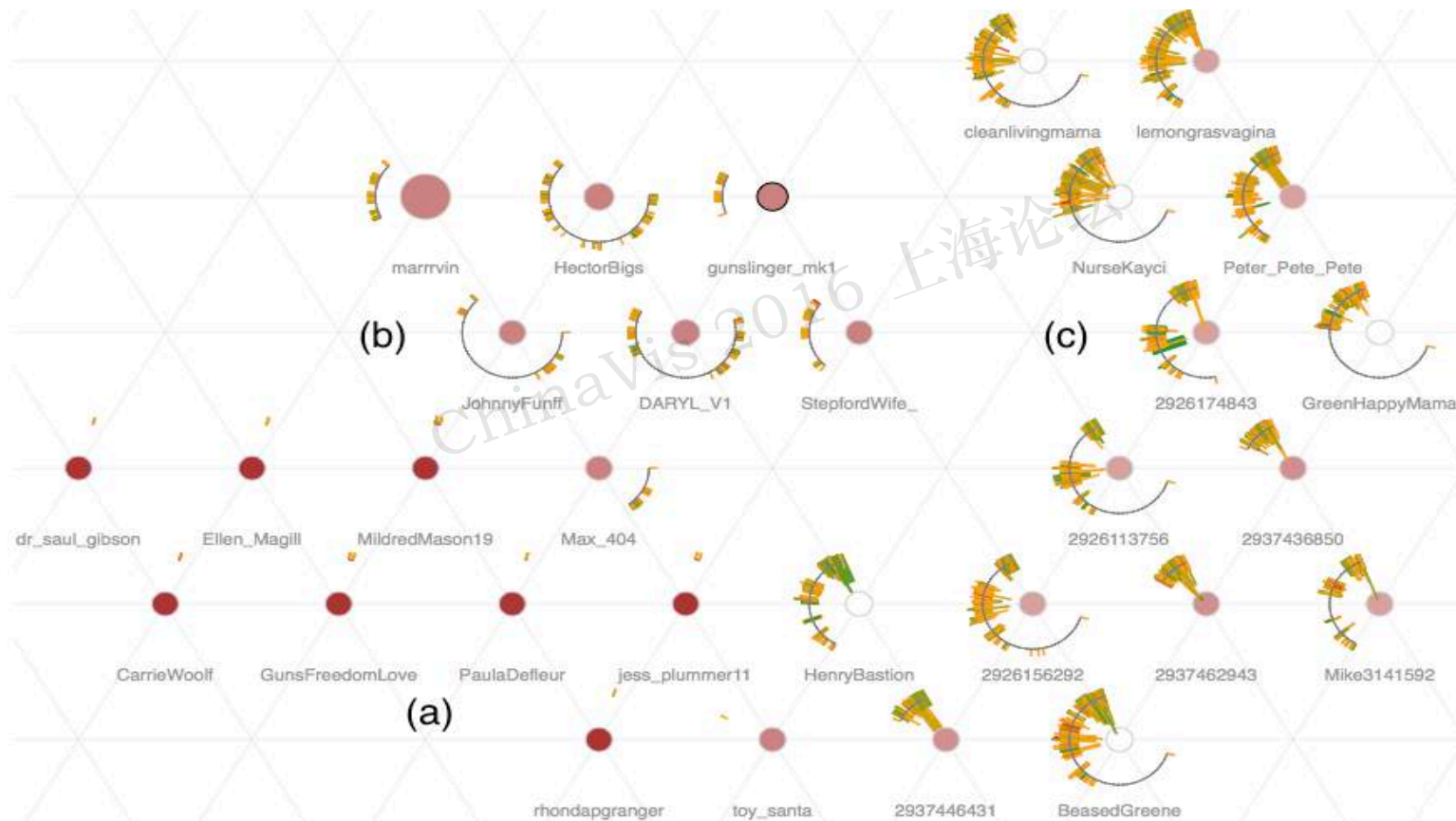
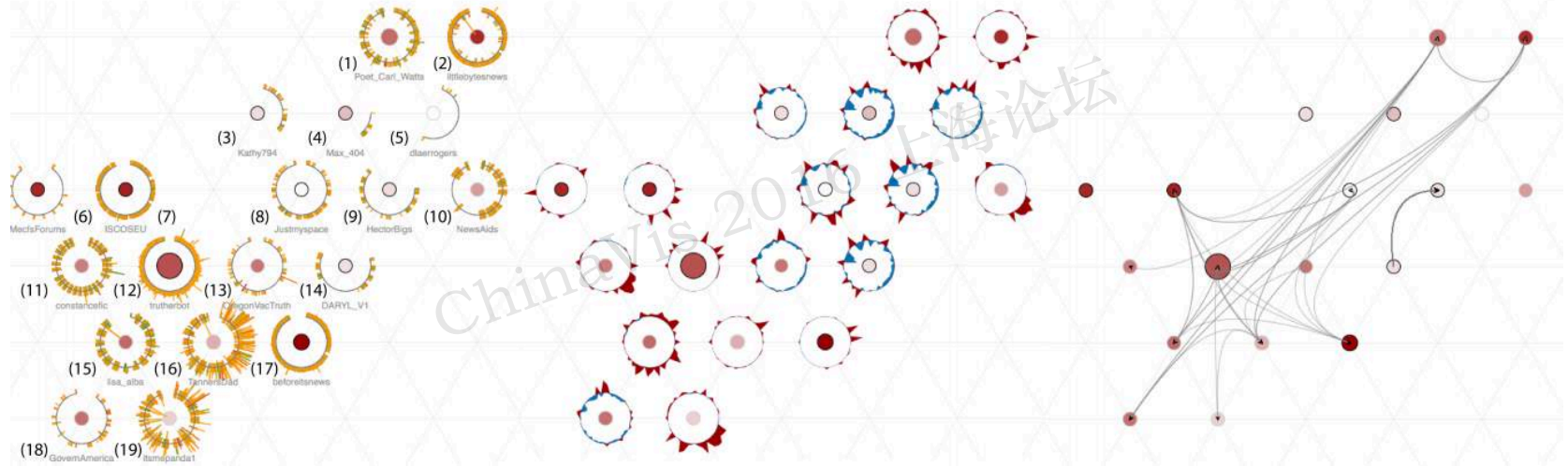


Fig. 11. Performance tests of TLOF model respectively based on the parameter settings (a) before the contest, (b) after 5 bots were detected, and (c) after about half of the bots (16) were known.

Final Results

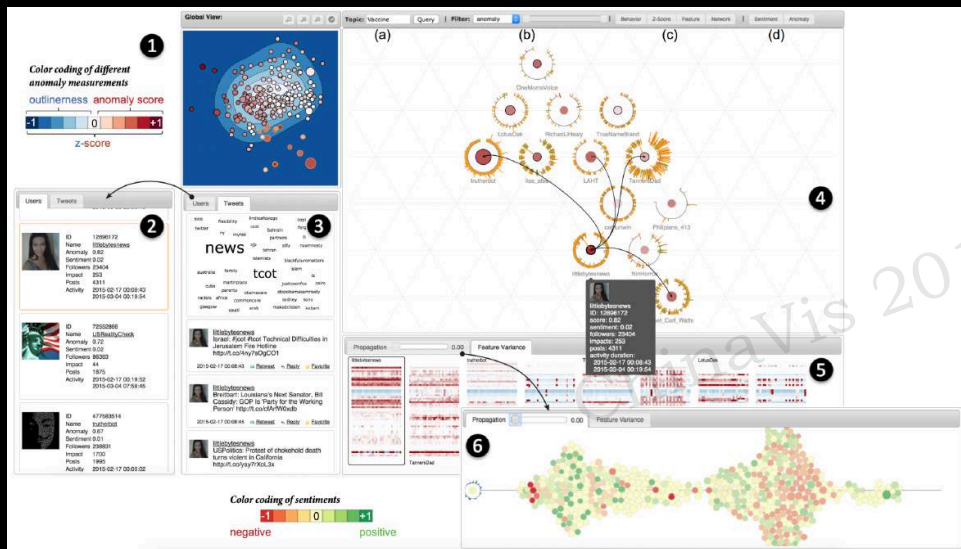


Conclusion



TargetVue: Visual Analysis of Anomalous User Behaviors in Online Communication Systems, IEEE TVCG, (VAST 2015)

Thank You !



Nan Cao, NYUSH VisLab
Assistant Professor, NYU ShangHai, China
Research Assistant Professor, NYU Tandon, USA
<http://nancao.org>

