TECHNISCHE UNIVERSITÄT DRESDEN

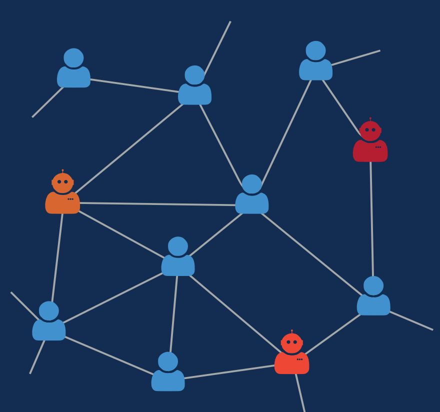
ROS | PRIVACY AND SECURITY

The Latent Behavior Space

Sequential Behavior Information Encoded in a Vector Space

Jan Reubold, Stephan Escher, Thorsten Strufe
TU Dresden

15th August 2017



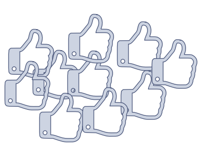
DRESDEN concept
Exzellenz aus Wissenschaft und Kultur

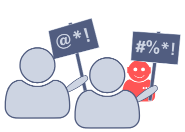
Social Bots in OSNs

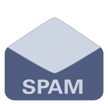
- Social Bots = automation software created to control an OSN account and tries to pose as a human

Intentions

Distributing Information

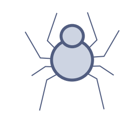






- prestige influencing
  (hype/denounce products, companies, people, ...)
- political influencing
  (framing, hype denounce political topics, ...)
- traditional malicious content
  (spam, phishing, malware)
- ‘legit’ distribution
  (news, weather, ...)
- ...

Harvesting Information

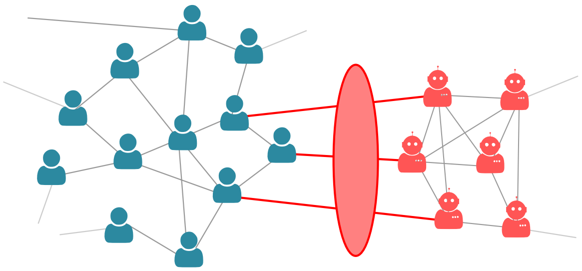


- ‘Crawler’
- Identity Theft
- Personalized information distribution
  (spear phishing, ...)
- ...

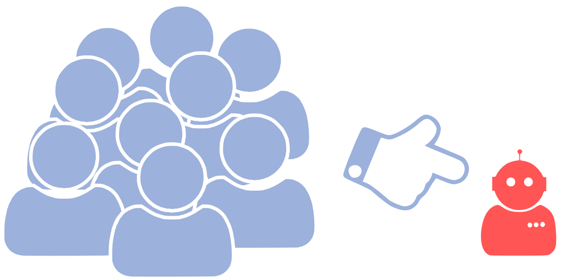
Social Bots in OSNs
Detection Mechanisms

- Countermeasures: Prevention, Detection, Awarness, ...

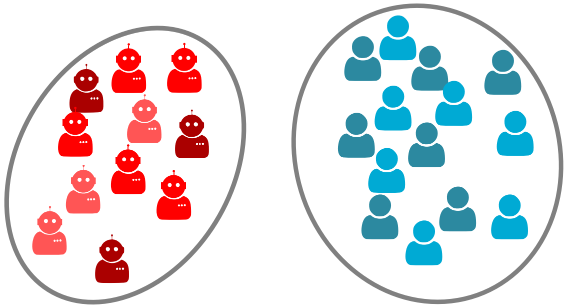
  - **Graph Based** - detect Sybils with social / interaction graph analysis



  - **Community Based** - user based bot detection + experts



  - **Machine Learning Based**
    - Behavior Based
    - Crowd Based - Coordinated activity of multiple 'users'



Behavior-Based Detection
Approaches I

- Sybil detection using clickstreams
- Two approaches (supervised, unsuperivsed)
  - SVM using 12 features:

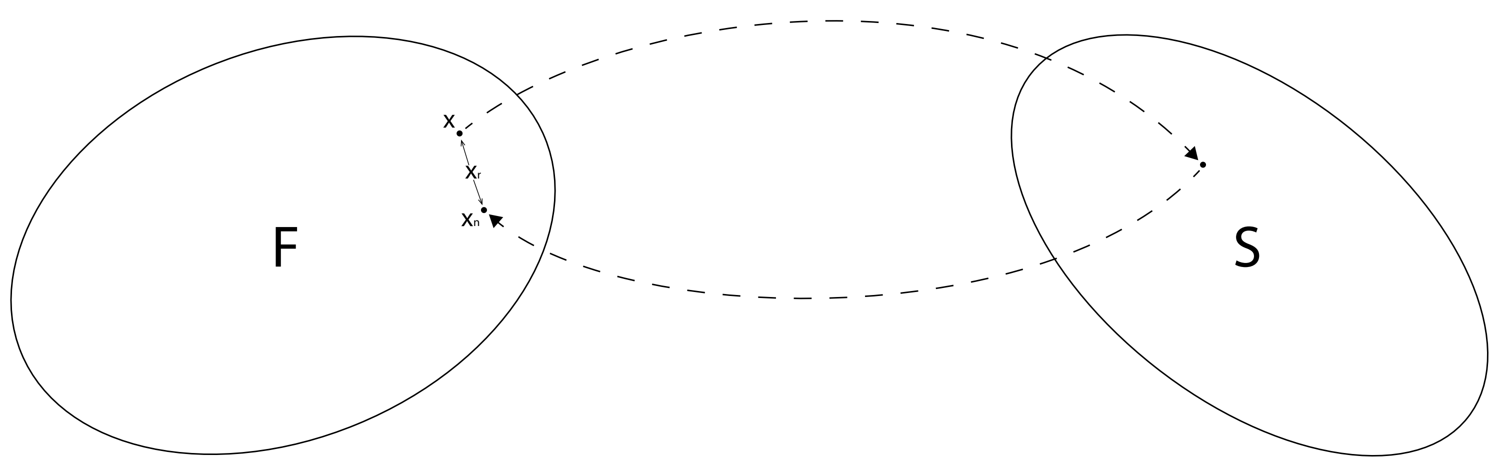
    ∅ clicks per session
    ∅ session length
    ∅ time between clicks
    ∅ # sessions per day
    Clickstreams → 8 Categories → BoW
  - Clustering:

    Pure clickstreams + clickstreams enriched with timining (e.g. [c_1, t_1, c_2, t_2, ...])
    Clickstreams + Timings → Distance Function → Graph

Wang, G., Konolige, T., Wilson, C., Wang, X., Zheng, H., & Zhao, B. Y. (2013, August). You Are How You Click: Clickstream Analysis for Sybil Detection. In USENIX Security Symposium (Vol. 9, pp. 1-008).

Behavior-Based Detection
Approaches II

- Model for normal user behavior
- Behavior that does not fit $\Rightarrow$ anomalous behavior (sybil + cyborg detection)
- Unsupervised Method:
  - Principal Component Analysis (Feature space **F**)
    - # likes per day
    - # likes in specific categories (e.g. sports, politics, education)
    - Evolution of spatial distribution of observed like categories
- PCA $\Rightarrow$ latent subspace **S**



Viswanath, B., Bashir, M. A., Crovella, M., Guha, S., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2014, August). Towards Detecting Anomalous User Behavior in Online Social Networks. In USENIX Security Symposium (pp. 223-238).

Time-Series Data
Pipelines

Task: Prediction, Classification, ...
e.g. Social-Bot Detection

Input: Time-Series
e.g. Click-Traces
- Labels
- Additional Information

Time-Series Features:

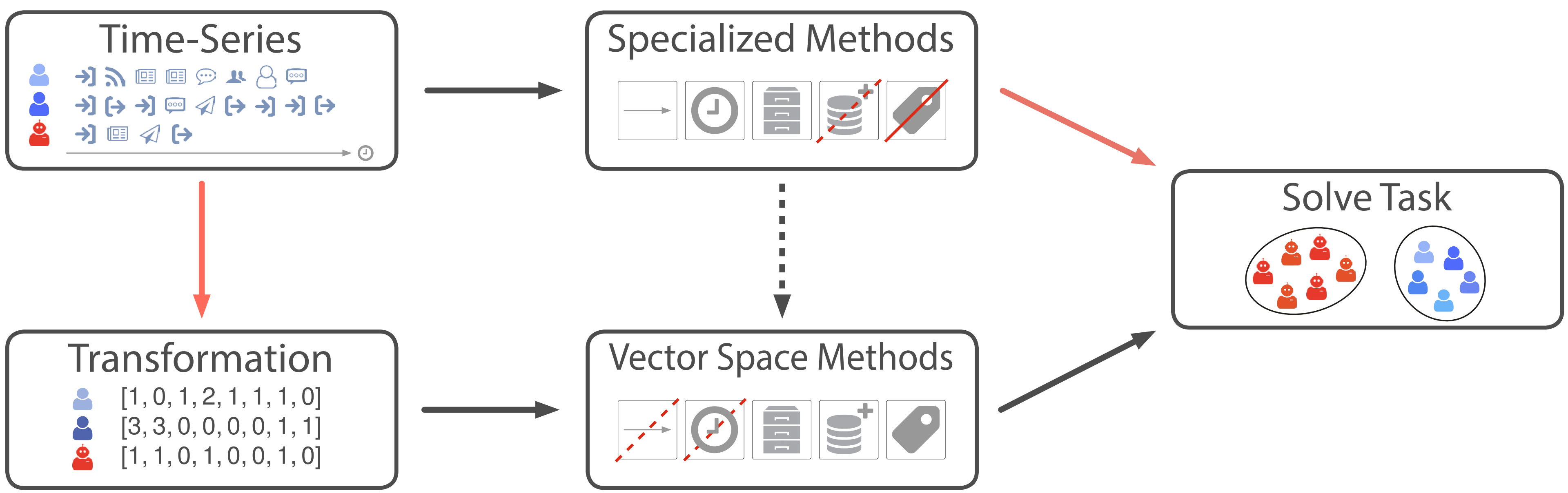
- Categorical-valued observations
  e.g. *login, send msg, share, ...*
- Temporal order
- Timinigs

Time-Series Data
Pipelines

Task: Prediction, Classification, ...
e.g. Social-Bot Detection

Input: Time-Series
e.g. Click-Traces
- Labels
- Additional Information

Time-Series Features:
- Categorical-valued observations
  e.g. *login, send msg, share, ...*
- Temporal order
- Timinigs



Time-Series Data

Our Approach

Standardize scheme

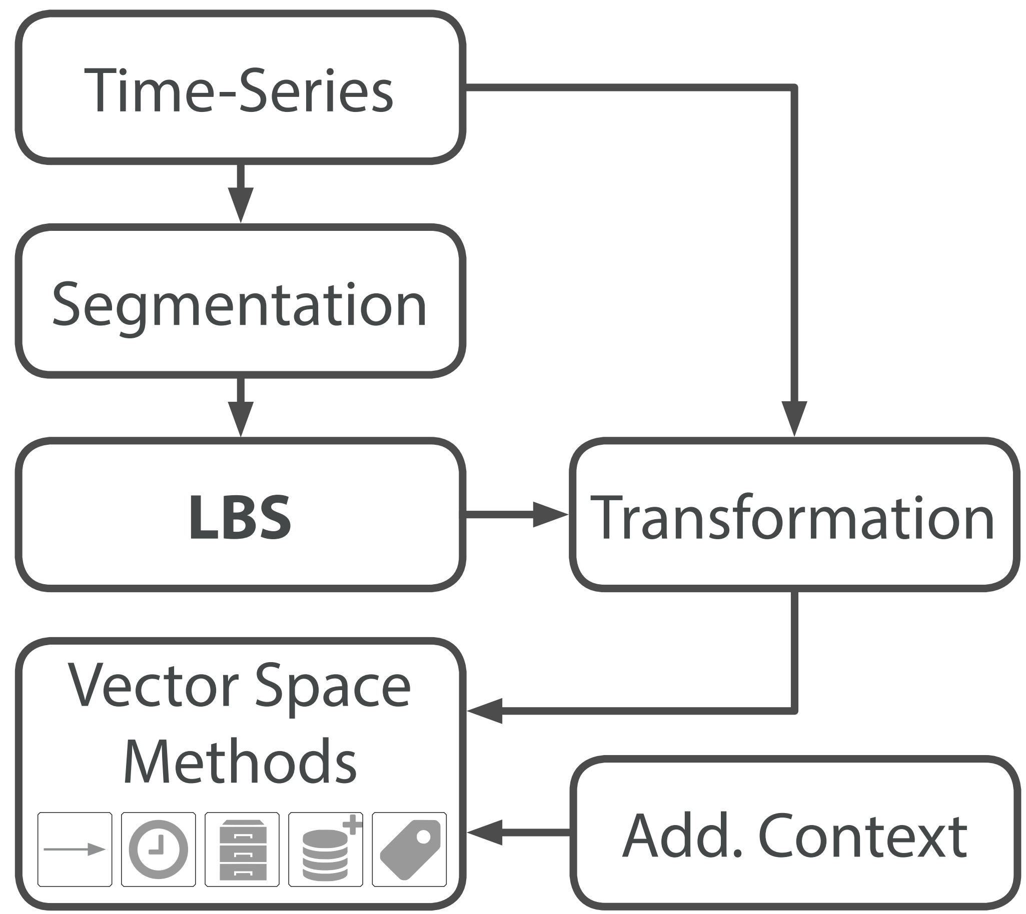
- Efficient use of vector space methods for time-series data (SVM, kNN, PCA, ...)

Idea

- Abstract & split time-series *(in parallel)*

Latent Behavior Space

- Span vector space by found patterns
- Express users by shown behavior pat-terns



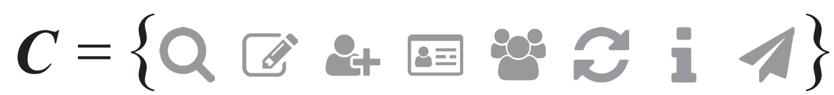
Our Approach
Setup and Concept

Input:

- Set of time-series
  e.g. user sessions on Facebook
- Time-series of categorical-valued observations
  e.g. 'send message', 'newsfeed', 'like'

Concept

- Abstraction of time-series data
- Represent by behavior patterns
  (called super states)



Time-Series Data

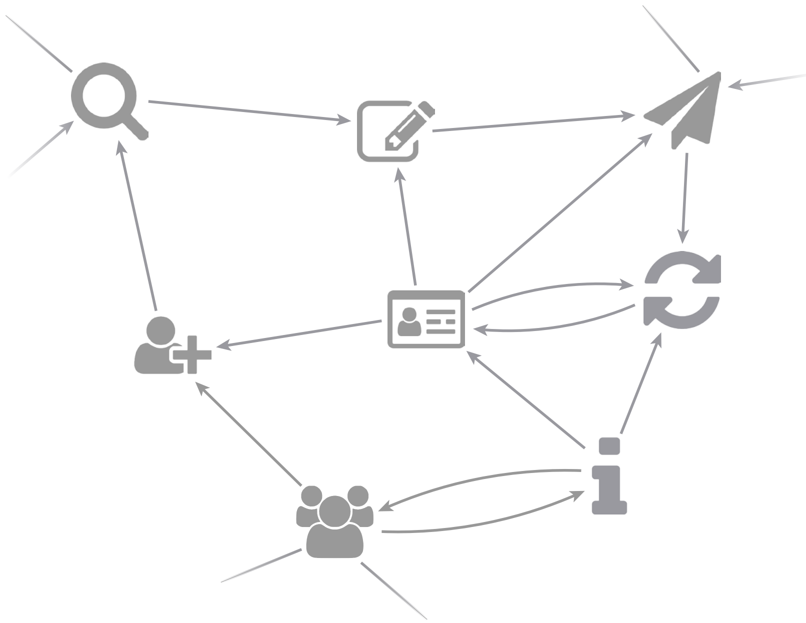
$$\boldsymbol{X} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_M\}$$ *Data*

$$\boldsymbol{x}_i = [x_{i1}, \ldots, x_{il_i}]$$ *Time-Series*

$$x_{ij} \in \boldsymbol{Y}, \quad z_{ij} \in \boldsymbol{C}$$ *Activity, Super State*

Our Approach

Super State Graph



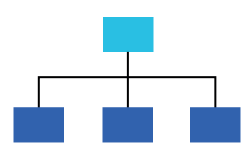
- Simple transition graph
- Transition probabilities governed by importance of super states

- Each node represents super state
  e.g. on click traces of an OSN:
  manifestation of an intention

Super State Graph

State Importance:

$$\beta \mid \gamma \sim Dir(\gamma)$$

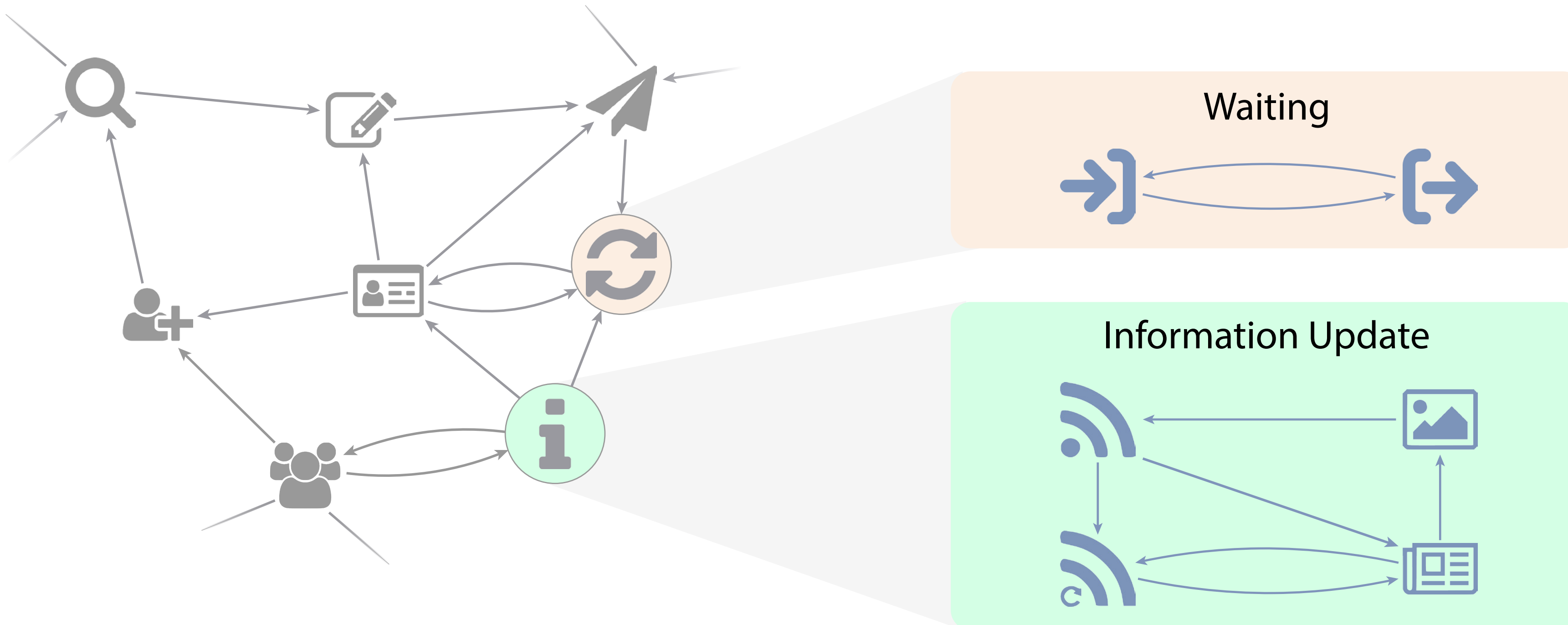


Transition Probability:

$$\pi_c \mid \alpha, \beta \sim Dir\left(\alpha\beta + (1-\tau)\rho \boldsymbol{1}_c\right)$$

Our Approach

Super States



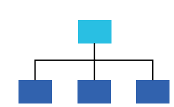
Super States

- *Initial-State Distribution*

$$\theta_c^I \mid \lambda \sim Dir(\lambda)$$

- *Transition Distribution (+End-State)*

$$G_c \mid \psi_c \sim Dir(\psi_c) \qquad \theta_{cs}^T \mid \lambda, G_c \sim Dir(\lambda G_c)$$



- *State-Duration Model*

$$\mu_{cs} \sim t_{\tilde{v}}\left(\mu_{cs} \mid \tilde{\mu}_{cs}, \tilde{\sigma}_{cs}^2 / \tilde{\kappa}_{cs}\right)$$

$$\sigma_{cs}^2 \sim \chi^{-2}\left(\sigma_{cs}^2 \mid \tilde{v}, \tilde{\sigma}_{cs}^2\right)$$

Our Approach

The Latent Behavior Space

- Segmentation of user behavior into known patterns
- Represent user by her behavior / exhibited patterns
- Use vector space methods

Latent Behavior Space

Transformation

$$v_u = \phi\left(\boldsymbol{X}_u\right)$$

- *Count-based*

$$\phi_{\tilde{\mathbf{z}}}^{O}\left(\boldsymbol{X}_u\right) \triangleq \frac{\sum_{(i,j)\in\tilde{\mathbf{z}}_u} \boldsymbol{1}_{z_{ij}}}{\left|\tilde{\mathbf{z}}_u\right|}$$

- *Time-based*

$$\phi_{\mathbf{z}}^{D}\left(\boldsymbol{X}_u\right) \triangleq \frac{\sum_{1\le i\le|\boldsymbol{X}_u|} \sum_{1\le \boldsymbol{j}\le l_{\boldsymbol{i}}} \boldsymbol{1}_{z_{ij}} t_{ij}}{\sum_{1\le i\le|\boldsymbol{X}_u|} \sum_{1\le \boldsymbol{j}\le l_{\boldsymbol{i}}} t_{ij}}$$

Our Approach

The Latent Behavior Space

- Segmentation of user behavior into known patterns
- Represent user by her behavior / exhibited patterns
- Use vector space methods

Latent Behavior Space

Transformation

$$v_u = \phi(\boldsymbol{X}_u)$$

- *Count-based*

$$\phi^{O}_{\tilde{\mathbf{z}}}(\boldsymbol{X}_u) \triangleq \frac{\sum_{(i,j)\in\tilde{\mathbf{z}}_u} \boldsymbol{1}_{z_{ij}}}{|\tilde{\mathbf{z}}_u|}$$

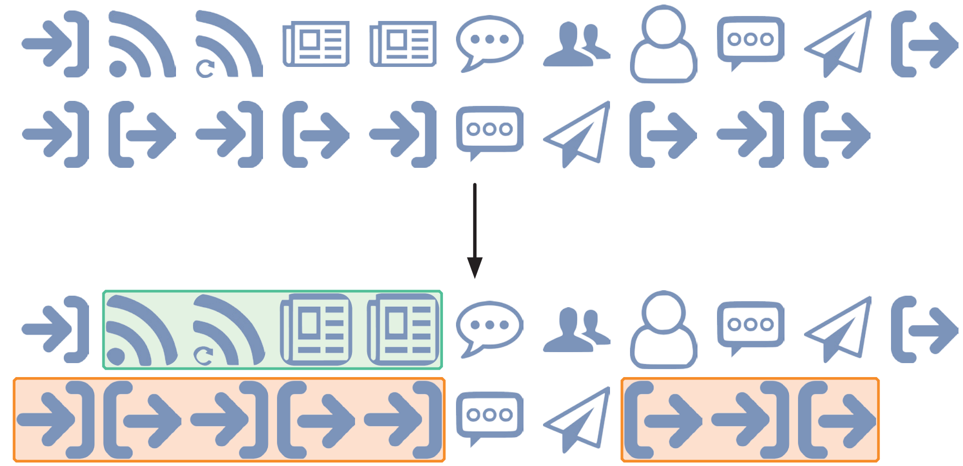
- *Time-based*

$$\phi^{D}_{\mathbf{z}}(\boldsymbol{X}_u) \triangleq \frac{\sum_{1\le i\le|\boldsymbol{X}_u|}\sum_{1\le j\le l_i} \boldsymbol{1}_{z_{ij}}\, t_{ij}}{\sum_{1\le i\le|\boldsymbol{X}_u|}\sum_{1\le j\le l_i} t_{ij}}$$

Our Approach

The Latent Behavior Space

- Segmentation of user behavior into known patterns
- Represent user by her behavior / exhibited patterns
- Use vector space methods



Latent Behavior Space

Transformation

$$v_u = \phi(X_u)$$

- *Count-based*

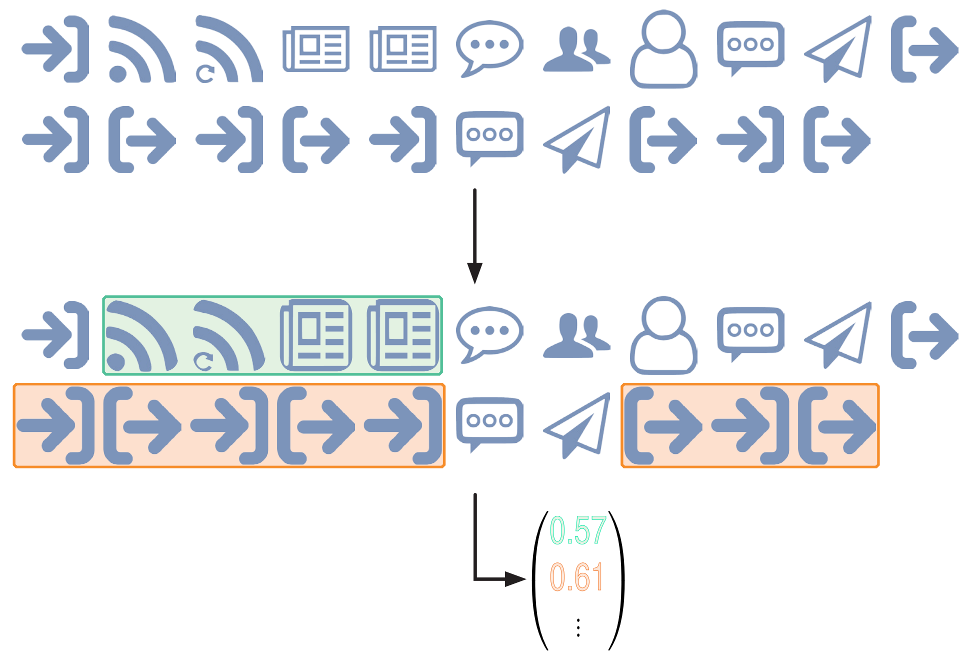
$$\phi_{\tilde{\mathbf{z}}}^{O}(X_u) \triangleq \frac{\sum_{(i,j)\in\tilde{\mathbf{z}}_u} \mathbf{1}_{z_{ij}}}{|\tilde{\mathbf{z}}_u|}$$

- *Time-based*

$$\phi_{\mathbf{z}}^{D}(X_u) \triangleq \frac{\sum_{1\le i\le|X_u|}\sum_{1\le j\le l_i} \mathbf{1}_{z_{ij}} t_{ij}}{\sum_{1\le i\le|X_u|}\sum_{1\le j\le l_i} t_{ij}}$$

Our Approach
The Latent Behavior Space

- Segmentation of user behavior into known patterns
- Represent user by her behavior / exhibited patterns
- Use vector space methods



Latent Behavior Space

Transformation

$$v_u = \phi(X_u)$$

- *Count-based*

$$\phi_{\tilde{\mathbf{z}}}^{O}(X_u) \triangleq \frac{\sum_{(i,j)\in\tilde{\mathbf{z}}_u} \mathbf{1}_{z_{ij}}}{|\tilde{\mathbf{z}}_u|}$$

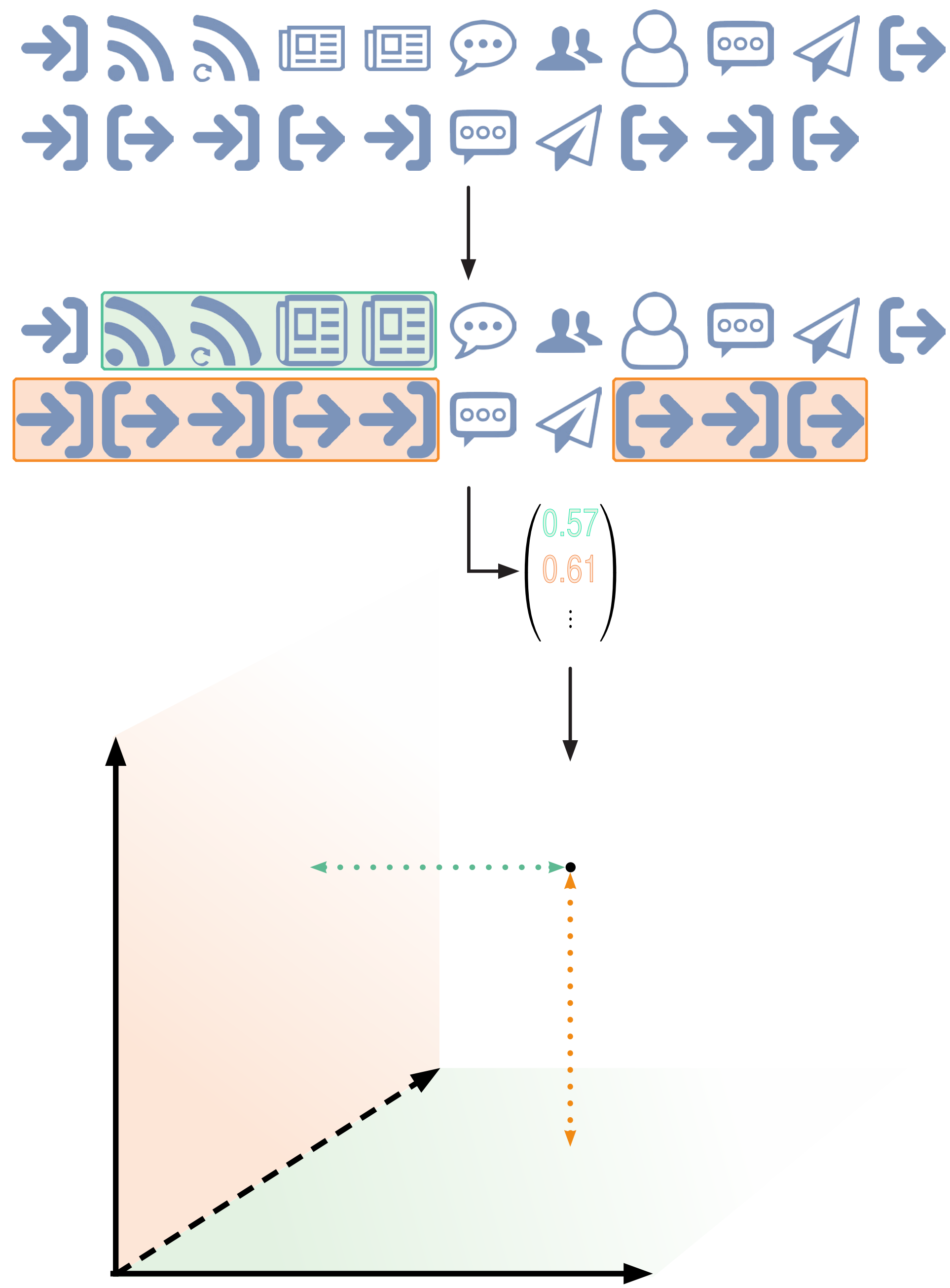
- *Time-based*

$$\phi_{\mathbf{z}}^{D}(X_u) \triangleq \frac{\sum_{1\le i\le|X_u|}\sum_{1\le j\le l_i} \mathbf{1}_{z_{ij}} t_{ij}}{\sum_{1\le i\le|X_u|}\sum_{1\le j\le l_i} t_{ij}}$$

Our Approach

The Latent Behavior Space

- Segmentation of user behavior into known patterns
- Represent user by her behavior / exhibited patterns
- Use vector space methods



Latent Behavior Space

Transformation

$$v_u = \phi\left(\boldsymbol{X}_u\right)$$

- *Count-based*

$$\phi^{O}_{\tilde{\mathbf{z}}}\left(\boldsymbol{X}_u\right) \triangleq \frac{\sum_{(i,j)\in\tilde{\mathbf{z}}_u} \boldsymbol{1}_{z_{ij}}}{\left|\tilde{\mathbf{z}}_u\right|}$$

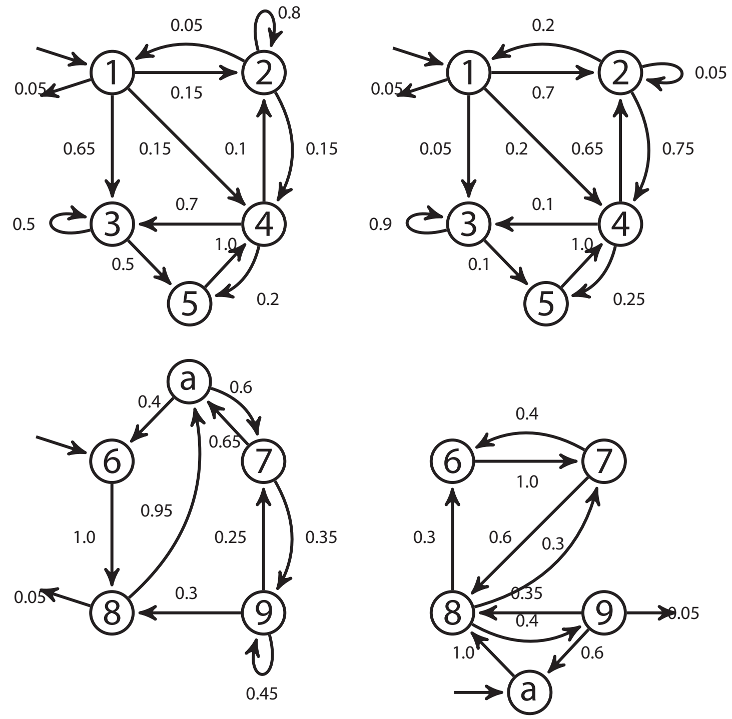
- *Time-based*

$$\phi^{D}_{\mathbf{z}}\left(\boldsymbol{X}_u\right) \triangleq \frac{\sum_{1\le i\le|\boldsymbol{X}_u|}\sum_{1\le j\le l_i} \boldsymbol{1}_{z_{ij}} t_{ij}}{\sum_{1\le i\le|\boldsymbol{X}_u|}\sum_{1\le j\le l_i} t_{ij}}$$

Controlled Setting
Evidence

Evidence on controlled settings

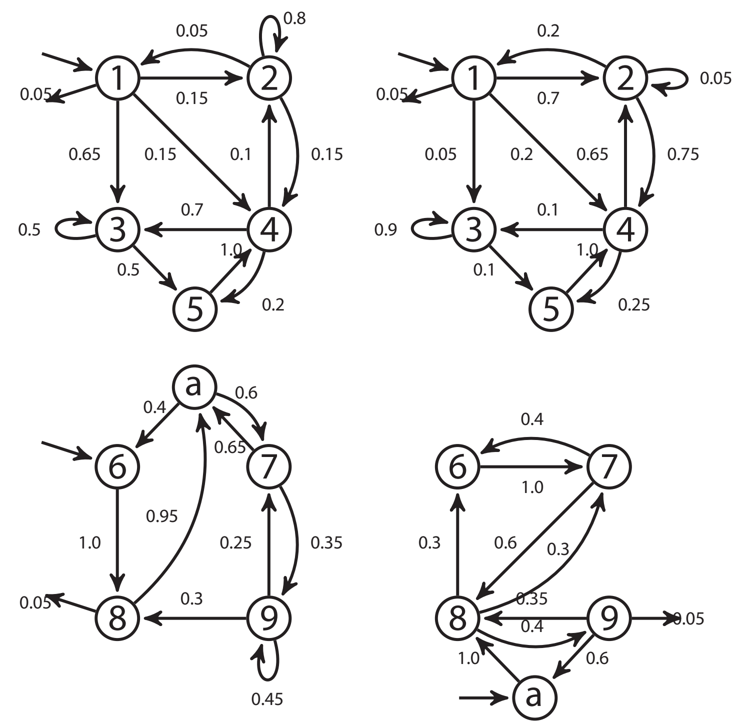
- Impact of sequential information for process recovery
  - 3 scenarios (sets of super states)
  - Scenario I → III: Increasing state space overlap
  - Recovery of processes (FNR)

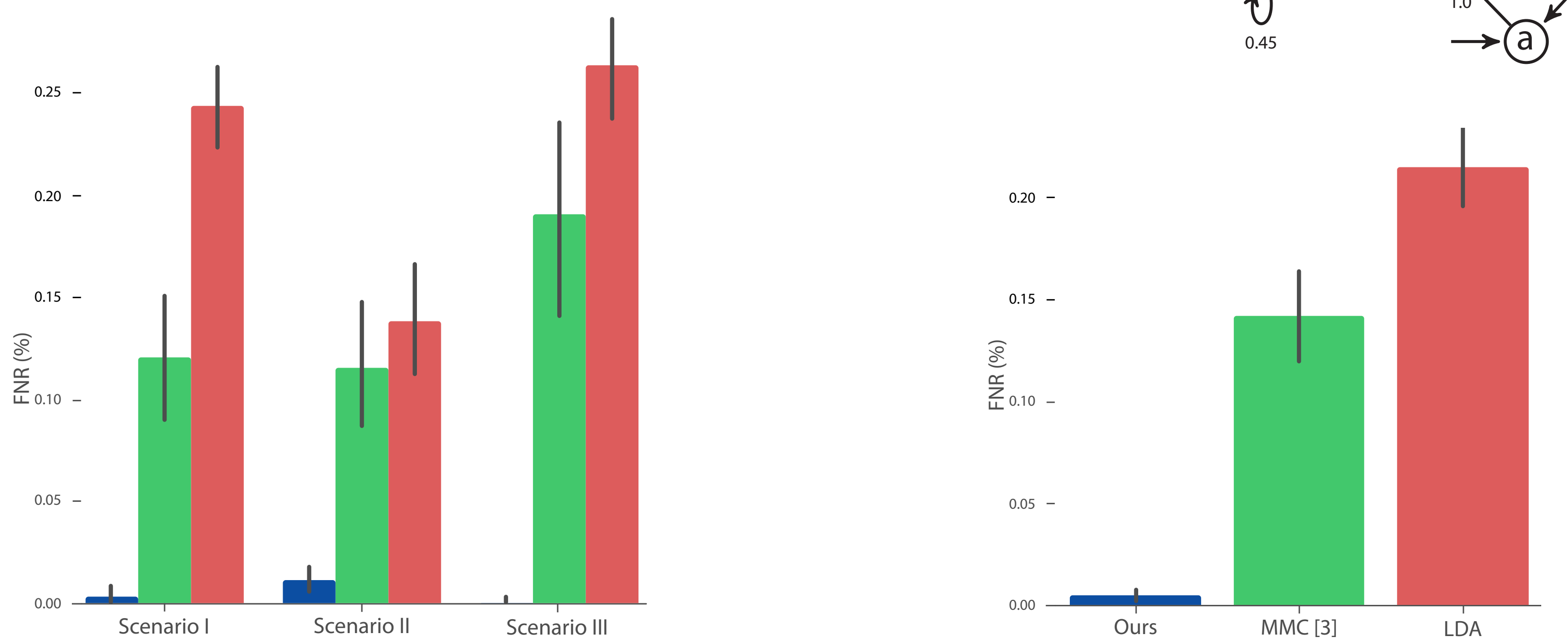


Controlled Setting
Evidence

Evidence on controlled settings

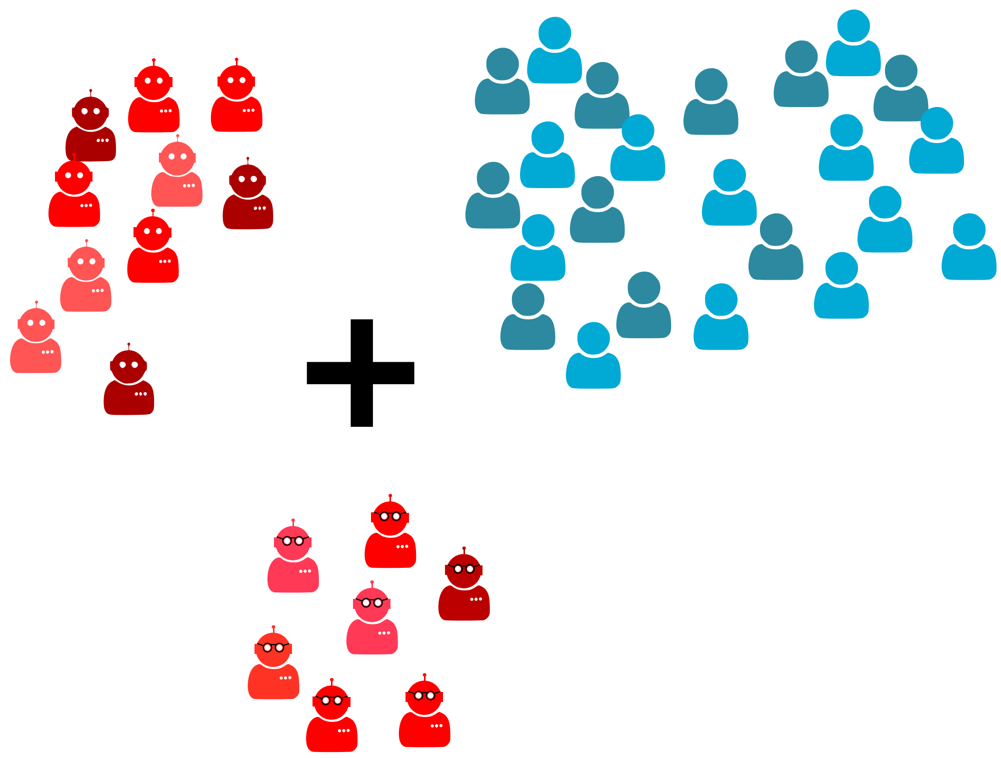
- Impact of sequential information for process recovery
    - 3 scenarios (sets of super states)
    - Scenario I → III: Increasing state space overlap
    - Recovery of processes (FNR)





Social Bot Detection
Work in Progress

- Develop attacker models based on characteristics
    - Profile Characteristic (Sybils, Cyborgs, Zombies, ...)
    - Social Bot-Networks (Union of social bots)
    - Massattacks vs Targeted Attacks
    - OSN Structure
    - Complexity (send every hour, user based behavior)
- Enrich real-world data set with behavior traces of theoretical attackers



Our Approach

Summary

Feature Design
by leveraging behavior patterns

Goal: Vector space + time-series

Problem: Loss of information

Approaches:

Direct:
Integrate sequential information into time-series

Abstraction:
Learn patterns from time-series
$\rightarrow$ represent time-series by patterns

Our Approach
Summary

Feature Design
by leveraging behavior patterns

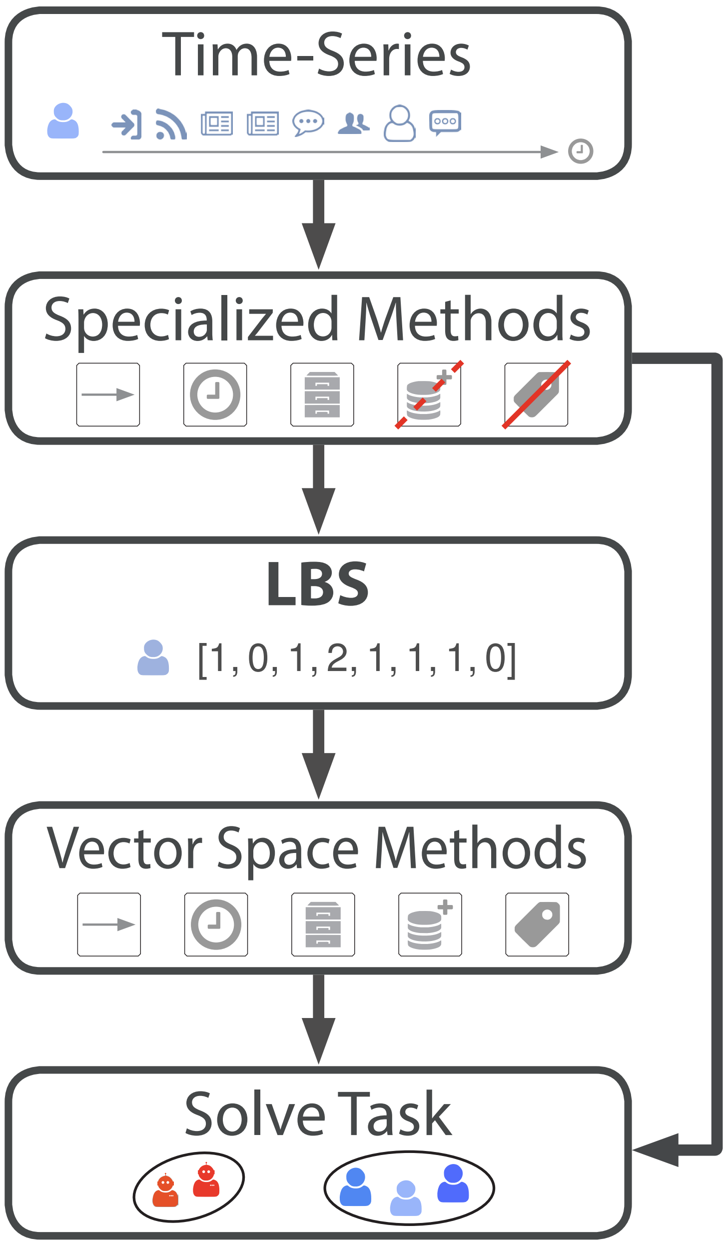
Goal: Vector space + time-series

Problem: Loss of information

Approaches:

Direct:
Integrate sequential information into time-series

Abstraction:
Learn patterns from time-series
→ represent time-series by patterns



Future Work

Current Work

- Evaluate on real-world data (replace individual transformations with LBS)
- Evaluate impact of loss of information (segmentation → LBS)
- Build theoretical attacker models

General

- Further work on social bot detection (behavior graph)
- Investigate influence streams (e.g. by means of frames) and echo chambers

Future Work

Current Work

- Evaluate on real-world data (replace individual transformations with LBS)
- Evaluate impact of loss of information (segmentation → LBS)
- Build theoretical attacker models

General

- Further work on social bot detection (behavior graph)
- Investigate influence streams (e.g. by means of frames) and echo chambers

Thank you! Questions?