# Risk Assessment in Decentralized Social Networks Based on Anomalous Behavior Detection

Advisors: Prof. Elena Ferrari, Prof. Barbara Carminati,
Naeimeh Laleh
Insubria University, Varese Como, Italy

# Introduction

- Decentralized Social Networks allow users to create a public or private profile
- Users interact with each other in the virtual environment
- Dramatic increase in online social network users
- Privacy is an enormous problem
- Some users are less concerned about information privacy
- Users by privacy setting couldn't control the resources published by other users
  - Can lead to security risks such as, identity theft and cyber stalking

# State of Art

- The success of I-social networks relies on the level of trust that members have with each other
- Trust is a measure of confidence that an entity or entities will behave in an expected manner.
- In online systems, trust is considered to be of two types:
  - **Direct trust:** is based on the direct experience of the member with the other party.
  - **Recommendation trust:** is based on experiences of other members in the social network with the other party.

# State of Art

- Trust information can be collected from three main sources:
  - **Attitude**: It related to user's like or dislike for something. This information is derived from a user's interactions.
  - **Experiences:** Experiences describe the perception of the members in their interactions with each other. Experiences may affect attitudes or behaviors.
    - **Positive experiences:** Encourage users to interact more in the community.
  - **Behaviors (**Patterns of interactions**):**
    - If a member is a highly active participant and suddenly stops participating, it means his trust decreased.

# State of Art

- Creating an environment where members can share their thoughts, opinions and experiences in an open and honest way without concerns about privacy
- Trust models classified into
  - Statistical and machine learning techniques
  - Heuristics based techniques
  - Behavior based techniques
- Some mechanisms based on user feedback/ experiences that are tools for reflection on user experiences.
- Trust models based on tie strength
  - Two close friends rarely exchange messages
  - Passive users just read, view other profiles and don't interact===decrease tie strength

# Behavior based Models:

- There are different types of activities in the community
  - Writing
  - Reading
  - Commenting on a post
  - Viewing information and Participating in an activity
  - Sending add request to others
- There are two types of interactions:
  - Active
    - Sending add request to others
    - Writing a post or commend
  - Passive
    - Regular visits to the community and Accepting add request
    - Reading a post or commend of others

# Behavior based Models:

- Model1: There are two particular behavior patterns as an expression of trust:
  - Conversation: If two users converse, they trust each other
  - Propagation: If user propagates information of others, the propagator trusts the information
- Model2: Model of trust based on long-time interaction and shorter distance
  - User of OSN has more friends (high degree)
  - Frequent communications with friends (minimum contact interval)
    - More secure
    - Higher trust value

# Problems in Behavior Based Models

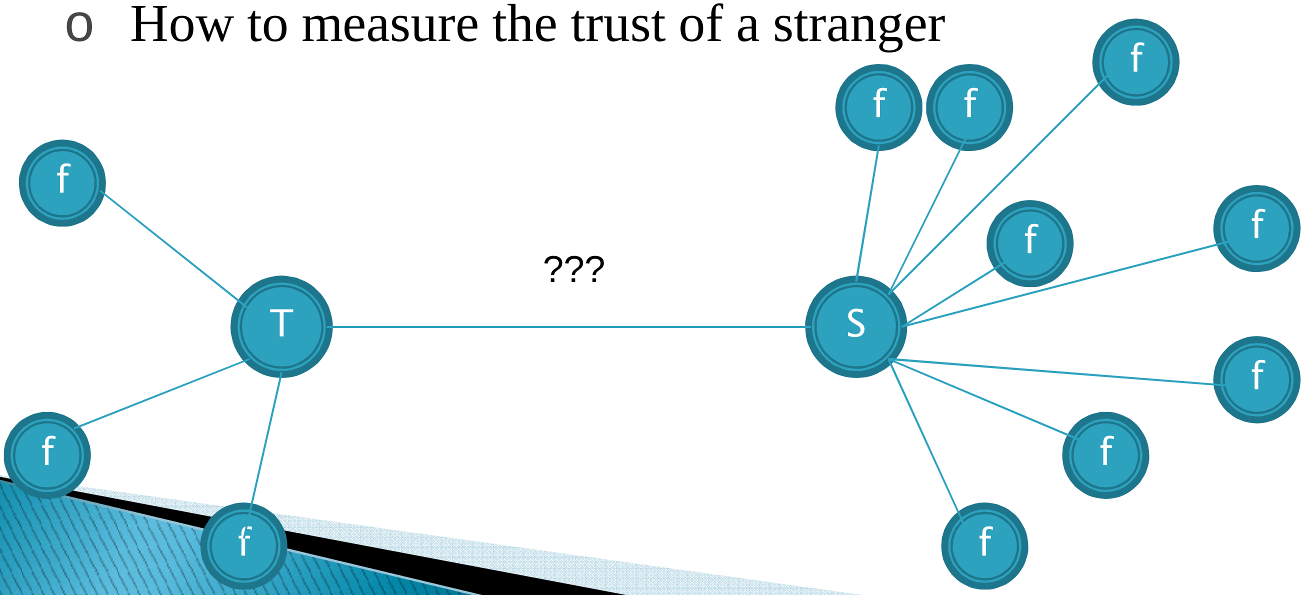
- A pair can be friends with each other but rarely exchange messages
- Some users are passive and they just read and view other profiles
- Some users may send a lot of messages, but never receive a response
- A user with high number of friends and interactions is more secure
- User with a lot of friends has an anomaly behavior

# Problems in Behavior Based Models

- Having a lot of friends only cannot be a sign of trust.
- User that propagates a lot of information of users.
- User may sends a lot of friendship invitation  and no one accept.
- One stranger may be trustworthy for one user but not trustworthy for another user.

# The goal of this project

- Before a user becomes friends with a stranger
  - Can a stranger be trusted?
  - How much is risky to create a relationship with a stranger?
  - How to measure the trust of a stranger



# The goal of this project

- **Our goal is** to identify trust and risk patterns------Good solution for default privacy setting for a user
  - Machine learning techniques
  - Behavior-based techniques
- **Overal approach:**

1- Find anomalous behaviors

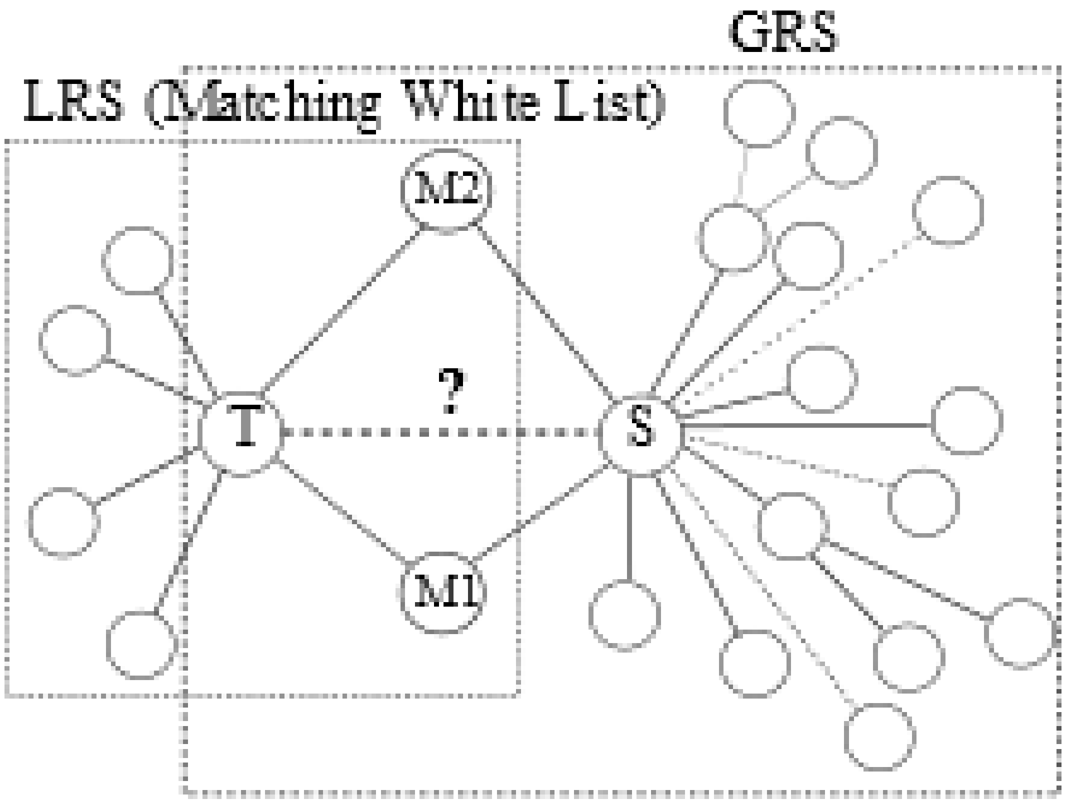
- Have anomaly behavior that can be risky
- Different behavior in compare of other users in a group
  - There is a blance between send and receive for majority of users in each group
  - If some one send a lot and did’t recive
  - In passive group, if someone propagates a lot of information to others

2- Risk of relationship between target user and stranger

# Overall Approach

- We analyse user behavior (patterns of interactions) globally and locally to assign two risk scores
- GRS: Global Risk Score
  - The result of anomaly detection algorithm
- LRS: Local Risk Score
  - How much is risky
  - Based on patterns of interactions
  - Matching relationship with user’s white list

# Overall Approach



# Global Risk Score

- Anomaly detection approaches in behavior analysis can be classified in three categories
  - Supervised learning
    - Each behavior labeled as anomalous or not
  - Unsupervised learning
    - Label is not required
  - Semi supervised learning
    - Few labeled behaviors

# GRS: What is behavior? Outlier?

- Global Risk Score- Behavior?
  - Sets of features that occur together by user's activities

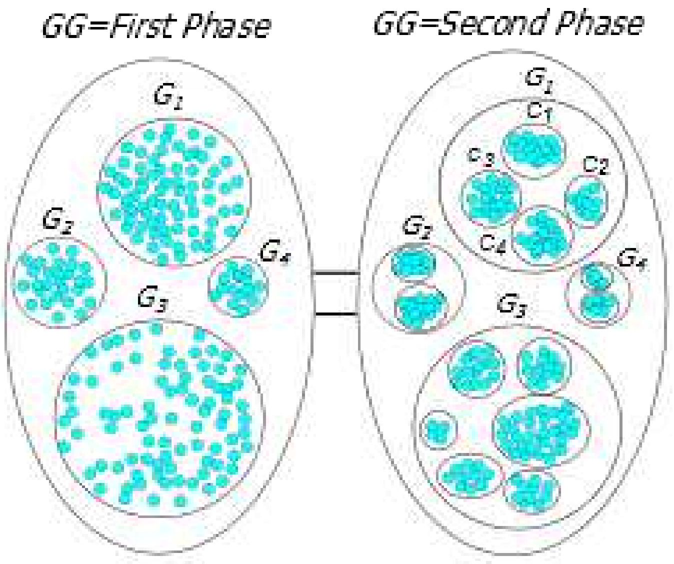
$B_1$={**a**, **b**, **c**}
$B_2$={**a**, **b**, **d**, **e**, q}
$B_3$={**b**, **c**, **d**, f, g}
$B_4$={**a**, **c**, **e**, **d**, h, i}
$B_5$={j, k, l, m, n, o, p , q}
$B_6$={r, s, t, u, v, w, x, y}

# Global Risk Score : Features

- Global Risk Score- Find anomalous behaviors
  - Distribution of behavior of each user across all other users
- Two group of features
  - Grouping
    - Profile (Education, Location, Age and number of friends, Internationality)
    - Attitudes (Passive, Active)
  - Behavior
    - Longevity
    - Number of add request sent
    - Variety of same family name in user's network
    - How many percent of profile items
    - Number of Propagated information
    - Number of like
    - Comment/ tag/ post

# GRS: Global Risk Score

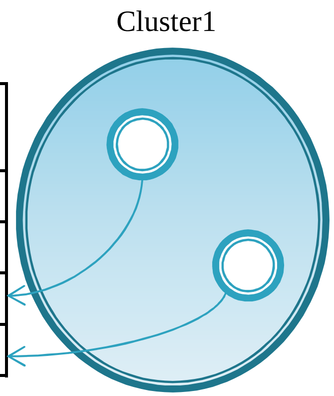
- There are two phases:
  - Cluster users based on Grouping features
  - Cluster each group based on Behavioral features



# GRS: Probability Based Clustering

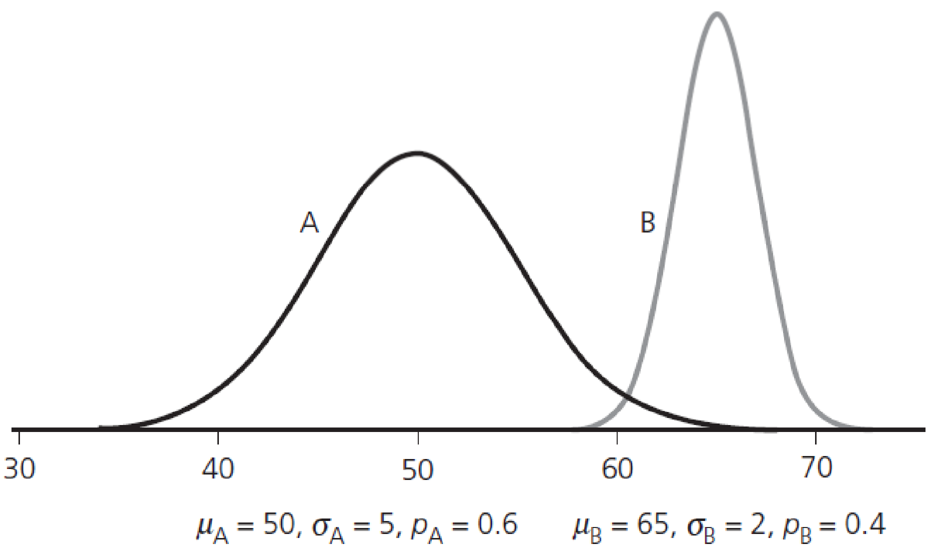
- Every user with his behavior has a certain probability to a given cluster
- There is K probability distributions, representing K clusters
- Each distribution gives the probability
- A particular behavior would have a certain set of features values to be member of that cluster

| User ID | Education | Age | Gender | No. Interaction | Current City | Hometown |
|---|---|---|---|---|---|---|
| 2 | Master | 25 | Male | 22 | Milan | Milan |
| 3 | master | 25 | Male | 114 | Varese | Milan |
| 4 | PhD | 27 | Female | 58 | Varese | Varese |
| 7 | PhD | 24 | Female | 58 | Milan | Varese |



# Probability Based Clustering

- Categorical Features: Pr[a=v|C1]



# Probability Based Clustering

- **Numeric Features:** Consider a Normal distribution with a mean and standard deviation for each feature, Probability Density Function
- If we have an equal number of education level as bachelor, PhD, master, our global distribution for each education would be 25%.  P(bachelor)+P(master)+P(PhD)=1

| Education | Cluster 1 | Cluster2 | Cluster 3 | Cluster 4 |
|---|---|---|---|---|
| Bachelor | 10% | 75% | 80% | 30% |
| Master | 45% | 25% | 0% | 25% |
| PhD | 45% | 0% | 20% | 45% |

# Expectation-Maximization(EM)

- Use three step:
  - **Initialization:** Guess the parameters (μ, σ, ρ) to calculate the cluster probability for each cluster
  - **Expectation:** Calculate the cluster probability and reestimate the parameters
  - **Maximization:** Calculation of the distribution parameters (μ, σ, ρ) increase the likelihood of the distributions in each iteration to maximize it.

$$\mu_A = \frac{w_1 x_1 + w_2 x_2 + \ldots + w_n x_n}{w_1 + w_2 + \ldots + w_n}$$

$$\sigma_A^2 = \frac{w_1 (x_1 - \mu)^2 + w_2 (x_2 - \mu)^2 + \ldots + w_n (x_n - \mu)^2}{w_1 + w_2 + \ldots + w_n}$$

| User ID | Education | Age | Gender | No. Interaction | Current City | Hometown |
|---|---|---|---|---|---|---|
| 2 | Master | 25 | Male | 22 | Milan | Milan |
| 3 | PhD | 25 | Male | 114 | Varese | Milan |
| 4 | PhD | 27 | Female | 58 | Varese | Varese |
| 7 | Master | 24 | Male | 58 | Milan | Varese |

| Education | Age | Gender | No. Interaction | Current City | Hometown | Probability |
|---|---|---|---|---|---|---|
| Bachelor | 22 | Male | 120 | Milan | Bologna | 10% |
| Master | 22 | Male | 80 | Milan | Milan | 15% |
| PhD | 22 | Male | 80 | Varese | Milan | 60% |
| PhD | 36 | Female | 80 | Varese | Varese | 30% |
| PhD | 32 | Female | 120 | Varese | Bologna | 15% |
| Master | 24 | Female | 22 | Milan | Bologna | 20% |
| Master | 24 | Male | 58 | Milan | Varese | 70% |

Mining Model

# GRS: User Grouping Phase

- Clustering users based on some grouping features
  - Profile
    - Education
    - Location
    - Age
    - Number of friends
    - Internationality
  - Attitudes
    - Passive
    - Active

# Anomaly/Outlier Detection Phase

- We cluster all users in each cluster based on behavior features to predict anomaly behavior
- The result of the "PredictCaseLikelihood" function is the Global Risk Score(GRS)

$$GRS(x_i) = \begin{cases} Anomaly & \text{if } PCL\ x_i \text{ is } \geq T_p \\ Normal & \text{if } PCL\ x_i \text{ is } < T_p \end{cases}$$

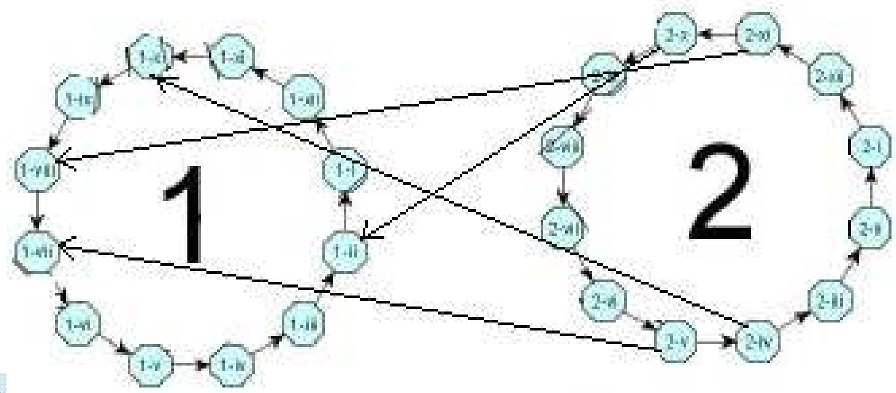
# EM Result for Anomaly Detection

- Behaviors that are far from any of clusters indicate as anomalous behavior

| [DEPOSITAM... | [DEPOSITAMO... | [... | [... | [D... | [D... | [... | [Meas... | [Meas... | [Meas... | [Measures].... | [M. | [Measures].[... | [... | Expression | $CLUSTER |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2008-08-24 ... | 100280010011 | 2 | 1 | D | 12 | 1 | 109 | 0 | 934.5... | 5500000 | 2 | 0 | 0 | 0 | Cluster 2 |
| 2008-05-07 ... | 1602225225221 | 4 | 1 | D | 12 | 1 | 0 | 0 | 188.5... | 13399999000 | 4 | 0 | 0 | 0 | Cluster 8 |
| 2008-08-18 ... | 201102789641 | 4 | 1 | D | 12 | 1 | 103 | 0 | 453.5... | 3000000 | 3 | 0 | 0 | 0 | Cluster 4 |
| 2008-11-09 ... | 202103455421 | 4 | 1 | D | 12 | 1 | 70 | 0 | 372.5... | 5363055 | 3 | 0 | 0 | 0 | Cluster 4 |
| 2008-05-07 ... | 21010272801 | 4 | 1 | D | 12 | 1 | 0 | 0 | 896.5... | 5930000000 | 2 | 0 | 0 | 0 | Cluster 8 |
| 2008-05-10 ... | 360136511 | 0 | 1 | D | 12 | 1 | 2 | 0 | 875.2... | 6995100000 | 4 | 0 | 0 | 0 | Cluster 8 |
| 2008-05-01 ... | 3601102240511 | 4 | 1 | D | 12 | 1 | 0 | 0 | 560.6... | 49000000 | 49 | 0 | 0 | 0 | Cluster 8 |
| 2008-05-06 ... | 18018001810332 | 2 | 0 | D | 12 | 1 | 2 | 0 | 14.05... | 4200000 | 1 | 0 | 0 | 8.99844035077263E-201 | Cluster 2 |
| 2008-05-04 ... | 2818005488921 | 2 | 0 | D | 12 | 1 | 0 | 0 | 1.043... | 9900000 | 2 | 0 | 0 | 4.23111531494548E-151 | Cluster 10 |
| 2008-07-02 ... | 202800295021 | 2 | 1 | D | 12 | 1 | 55 | 0 | 934.3... | 3800 | 2 | 0 | 0 | 3.31517148202206E-99 | Cluster 4 |
| 2008-06-24 ... | 202103455421 | 4 | 1 | D | 12 | 1 | 51 | 0 | 372.5... | 19946010 | 2 | 0 | 0 | 1.11196726201352E-81 | Cluster 4 |
| 2008-05-03 ... | 32018005210591 | 2 | 0 | D | 12 | 1 | 0 | 0 | 19.99... | 3000000 | 1 | 0 | 0 | 5.38400079566377E-69 | Cluster 10 |
| 2008-07-19 ... | 202810201591 | 2 | 1 | D | 12 | 1 | 76 | 0 | 1058.... | 200000 | 1 | 0 | 0 | 8.77333184899138E-07 | Cluster 2 |
| 2008-11-09 ... | 2028003858251 | 2 | 1 | D | 12 | 1 | 70 | 0 | 324.6... | 2481000 | 1 | 0 | 0 | 0.00244739280369199 | Cluster 2 |

# Local Risk Score(LRS)

- We want to find how much is risky for a target user to create a relationship with a stranger based on patterns of interactions with him and profile features ?
- To assign this risk score, we compare all features of two user1 with user 2 to create a white List  for target user1



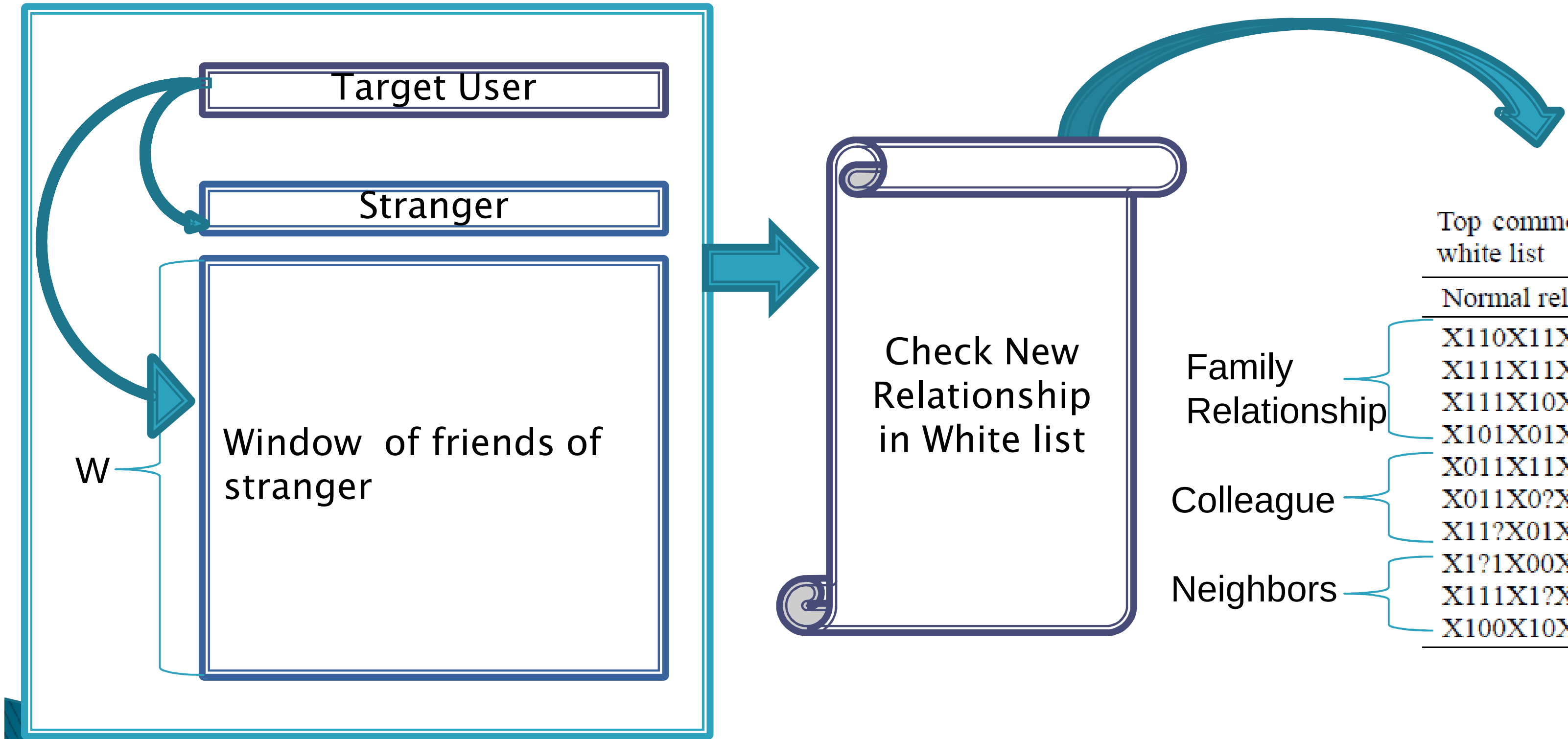
# LRS: What is inside the White List

- White List

Top common relationship in the white list

| Normal relationship | ID |
|---|---|
| X110X11X1X101110111 | 1 |
| X111X11X1X01111110? | 2 |
| X111X10X1X110111011 | 3 |
| X101X01X1X111111111 | 4 |
| X011X11X1X111110111 | 5 |
| X011X0?XXX000000001 | 6 |
| X11?X01XXX111111111 | 7 |
| X1?1X00XXX000000001 | 8 |
| X111X1?X1X110111111 | 9 |
| X100X10X1X000000001 | 10 |

# LRS: Risk of Creating Relationship




Top common relationship in the white list

| | Normal relationship | ID |
|---|---|---|
| Family Relationship | X110X11X1X101110111 | 1 |
| | X111X11X1X01111110? | 2 |
| | X111X10X1X110111011 | 3 |
| | X101X01X1X111111111 | 4 |
| Colleague | X011X11X1X111110111 | 5 |
| | X011X0?XXX000000001 | 6 |
| | X11?X01XXX111111111 | 7 |
| Neighbors | X1?1X00XXX000000001 | 8 |
| | X111X1?X1X110111111 | 9 |
| | X100X10X1X000000001 | 10 |

# References:


- Sherchan, Wanita, Surya Nepal, and Cecile Paris. "A survey of trust in social networks." *ACM Computing Surveys (CSUR)* 45.4 (2013): 47.
- Nepal, Surya, Wanita Sherchan, and Cecile Paris. "STrust: a trust model for Social Networks." *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*. IEEE, 2011.
- Adali, Sibel, and Jennifer Golbeck. "Predicting Personality with Social Behavior." *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*. IEEE Computer Society, 2012.
- Adali, Sibel, Fred Sisenda, and Malik Magdon-Ismail. "Actions speak as loud as words: Predicting relationships from social behavior data." *Proceedings of the 21st international conference on World Wide Web*. ACM, 2012.
- Li, Ming, and Alessio Bonti. "T-OSN: A Trust Evaluation Model in Online Social Networks." *Embedded and Ubiquitous Computing (EUC), 2011 IFIP 9th International Conference on*. IEEE, 2011.

# References:


- Bouguessa, Mohamed. "Unsupervised Anomaly Detection in Transactional Data." *Machine Learning and Applications (ICMLA), 2012 11th International Conference on*. Vol. 1. IEEE, 2012.
- Papadimitriou, Panagiotis, Ali Dasdan, and Hector Garcia-Molina. "Web graph similarity for anomaly detection." *Journal of Internet Services and Applications*1.1 (2010): 19-30.
- DuBois, Thomas, Jennifer Golbeck, and Aravind Srinivasan. "Predicting trust and distrust in social networks." *Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom)*. IEEE, 2011.
- Akcora, Cuneyt Gurcan, Barbara Carminati, and Elena Ferrari. "User similarities on social networks." *Social Network Analysis and Mining* (2013): 1-21.
- Akcora, Cuneyt Gurcan, Barbara Carminati, and Elena Ferrari. "Privacy in social networks: How risky is your social graph?." *Data Engineering (ICDE), 2012 IEEE 28th International Conference on*. IEEE, 2012.

# References:


- Adali, Sibel, et al. "Measuring behavioral trust in social networks." *Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on*. IEEE, 2010.
- Arnaboldi, Valerio, Andrea Guazzini, and Andrea Passarella. "Egocentric Online Social Networks: Analysis of Key Features and Prediction of Tie Strength in Facebook." *Computer Communications* (2013).
- Huang, Bert, et al. "A flexible framework for probabilistic models of social trust."*Social Computing, Behavioral-Cultural Modeling and Prediction*. Springer Berlin Heidelberg, 2013. 265-273.
- Smyth, Padhraic. "Probabilistic model-based clustering of multivariate and sequential data." *Proceedings of the Seventh International Workshop on AI and Statistics*. San Francisco, CA: Morgan Kaufman, 1999.
- Kuusela, Mikael, et al. "Semi-supervised anomaly detection-towards model-independent searches of new physics." *Journal of Physics: Conference Series*. Vol. 368. No. 1. IOP Publishing, 2012.

# Thanks for your attention