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
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:

- **Model 1:** 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

- **Model 2:** 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

- **Overall 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 balance between send and receive for majority of users in each group
       - If some one send a lot and didn’t receive
       - 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

<table>
<thead>
<tr>
<th>User ID</th>
<th>Education</th>
<th>Age</th>
<th>Gender</th>
<th>No. Interaction</th>
<th>Current City</th>
<th>Hometown</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Master</td>
<td>25</td>
<td>Male</td>
<td>22</td>
<td>Milan</td>
<td>Milan</td>
</tr>
<tr>
<td>3</td>
<td>master</td>
<td>25</td>
<td>Male</td>
<td>114</td>
<td>Varese</td>
<td>Milan</td>
</tr>
<tr>
<td>4</td>
<td>PhD</td>
<td>27</td>
<td>Female</td>
<td>58</td>
<td>Varese</td>
<td>Varese</td>
</tr>
<tr>
<td>7</td>
<td>PhD</td>
<td>24</td>
<td>Female</td>
<td>58</td>
<td>Milan</td>
<td>Varese</td>
</tr>
</tbody>
</table>
Probability Based Clustering

- Categorical Features: $\text{Pr}[a=v|C1]$
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%. \( P(\text{bachelor}) + P(\text{master}) + P(\text{PhD}) = 1 \)

<table>
<thead>
<tr>
<th>Education</th>
<th>Cluster 1</th>
<th>Cluster 2</th>
<th>Cluster 3</th>
<th>Cluster 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bachelor</td>
<td>10%</td>
<td>75%</td>
<td>80%</td>
<td>30%</td>
</tr>
<tr>
<td>Master</td>
<td>45%</td>
<td>25%</td>
<td>0%</td>
<td>25%</td>
</tr>
<tr>
<td>PhD</td>
<td>45%</td>
<td>0%</td>
<td>20%</td>
<td>45%</td>
</tr>
</tbody>
</table>
Expectation-Maximization (EM)

- Use three steps:
  - **Initialization**: Guess the parameters ($\mu$, $\sigma$, $\rho$) to calculate the cluster probability for each cluster.
  - **Expectation**: Calculate the cluster probability and reestimate the parameters.
  - **Maximization**: Calculation of the distribution parameters ($\mu$, $\sigma$, $\rho$) increase the likelihood of the distributions in each iteration to maximize it.

\[
\mu_\Lambda = \frac{w_1 x_1 + w_2 x_2 + \ldots + w_n x_n}{w_1 + w_2 + \ldots + w_n}
\]

\[
\sigma^2_\Lambda = \frac{w_1 (x_1 - \mu)^2 + w_2 (x_2 - \mu)^2 + \ldots + w_n (x_n - \mu)^2}{w_1 + w_2 + \ldots + w_n}
\]
<table>
<thead>
<tr>
<th>User ID</th>
<th>Education</th>
<th>Age</th>
<th>Gender</th>
<th>No. Interaction</th>
<th>Current City</th>
<th>Hometown</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Master</td>
<td>25</td>
<td>Male</td>
<td>22</td>
<td>Milan</td>
<td>Milan</td>
</tr>
<tr>
<td>3</td>
<td>PhD</td>
<td>25</td>
<td>Male</td>
<td>114</td>
<td>Varese</td>
<td>Milan</td>
</tr>
<tr>
<td>4</td>
<td>PhD</td>
<td>27</td>
<td>Female</td>
<td>58</td>
<td>Varese</td>
<td>Varese</td>
</tr>
<tr>
<td>7</td>
<td>Master</td>
<td>24</td>
<td>Male</td>
<td>58</td>
<td>Milan</td>
<td>Varese</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Education</th>
<th>Age</th>
<th>Gender</th>
<th>No. Interaction</th>
<th>Current City</th>
<th>Hometown</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bachelor</td>
<td>22</td>
<td>Male</td>
<td>120</td>
<td>Milan</td>
<td>Bologna</td>
<td>10%</td>
</tr>
<tr>
<td>Master</td>
<td>22</td>
<td>Male</td>
<td>80</td>
<td>Milan</td>
<td>Milan</td>
<td>15%</td>
</tr>
<tr>
<td>PhD</td>
<td>22</td>
<td>Male</td>
<td>80</td>
<td>Varese</td>
<td>Milan</td>
<td>60%</td>
</tr>
<tr>
<td>PhD</td>
<td>36</td>
<td>Female</td>
<td>80</td>
<td>Varese</td>
<td>Varese</td>
<td>30%</td>
</tr>
<tr>
<td>PhD</td>
<td>32</td>
<td>Female</td>
<td>120</td>
<td>Varese</td>
<td>Bologna</td>
<td>15%</td>
</tr>
<tr>
<td>Master</td>
<td>24</td>
<td>Female</td>
<td>22</td>
<td>Milan</td>
<td>Bologna</td>
<td>20%</td>
</tr>
<tr>
<td>Master</td>
<td>24</td>
<td>Male</td>
<td>58</td>
<td>Milan</td>
<td>Varese</td>
<td>70%</td>
</tr>
</tbody>
</table>
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)

\[
GRS(x_i) = \begin{cases} 
  \text{Anomaly} & \text{if } PCL \ x_i \ \text{is} \geq T_p \\
  \text{Normal} & \text{if } PCL \ x_i \ \text{is} < T_p 
\end{cases}
\]
EM Result for Anomaly Detection

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

<table>
<thead>
<tr>
<th>DATE</th>
<th>INDEX</th>
<th>ID</th>
<th>MESS</th>
<th>MEAS</th>
<th>MEAS...</th>
<th>MEASURES</th>
<th>MEASURES...</th>
<th>M...</th>
<th>M...</th>
<th>MEASURE</th>
<th>CLUSTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-06-24</td>
<td>10022600010011</td>
<td>2</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>109</td>
<td>0</td>
<td>934.5...</td>
<td>5500000</td>
<td>2</td>
</tr>
<tr>
<td>2008-06-07</td>
<td>1602265262521</td>
<td>4</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>188.5...</td>
<td>13999999000</td>
<td>4</td>
</tr>
<tr>
<td>2008-06-13</td>
<td>20112279641</td>
<td>4</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>103</td>
<td>0</td>
<td>453.5...</td>
<td>3000000</td>
<td>3</td>
</tr>
<tr>
<td>2008-11-06</td>
<td>20210345421</td>
<td>4</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>70</td>
<td>0</td>
<td>372.5...</td>
<td>583058</td>
<td>3</td>
</tr>
<tr>
<td>2008-05-07</td>
<td>2101227801</td>
<td>4</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>896.5...</td>
<td>5999999000</td>
<td>2</td>
</tr>
<tr>
<td>2008-05-10</td>
<td>3601263511</td>
<td>0</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>875.2...</td>
<td>6995100000</td>
<td>4</td>
</tr>
<tr>
<td>2008-05-01</td>
<td>3602102249511</td>
<td>4</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>560.6...</td>
<td>4900000</td>
<td>49</td>
</tr>
<tr>
<td>2008-05-06</td>
<td>10012000180332</td>
<td>2</td>
<td>0</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>14.05...</td>
<td>4200000</td>
<td>1</td>
</tr>
<tr>
<td>2008-05-04</td>
<td>3040200500921</td>
<td>2</td>
<td>0</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1.042...</td>
<td>9900000</td>
<td>2</td>
</tr>
<tr>
<td>2008-07-02</td>
<td>20280229221</td>
<td>2</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>55</td>
<td>0</td>
<td>934.3...</td>
<td>3800</td>
<td>2</td>
</tr>
<tr>
<td>2008-06-24</td>
<td>202103455421</td>
<td>4</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>51</td>
<td>0</td>
<td>372.5...</td>
<td>19946010</td>
<td>2</td>
</tr>
<tr>
<td>2008-05-03</td>
<td>32012005210591</td>
<td>2</td>
<td>0</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>19.99...</td>
<td>3000000</td>
<td>1</td>
</tr>
<tr>
<td>2008-07-19</td>
<td>202810201591</td>
<td>2</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>76</td>
<td>0</td>
<td>1069....</td>
<td>2000000</td>
<td>1</td>
</tr>
<tr>
<td>2008-11-09</td>
<td>20283023592521</td>
<td>2</td>
<td>1</td>
<td>D</td>
<td>12</td>
<td>1</td>
<td>70</td>
<td>0</td>
<td>324.6...</td>
<td>2451000</td>
<td>1</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Normal relationship</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>X110X11X1X101110111</td>
<td>1</td>
</tr>
<tr>
<td>X111X11X1X011111110?</td>
<td>2</td>
</tr>
<tr>
<td>X111X10X1X110111011</td>
<td>3</td>
</tr>
<tr>
<td>X101X01X1X111111111</td>
<td>4</td>
</tr>
<tr>
<td>X011X11X1X111110111</td>
<td>5</td>
</tr>
<tr>
<td>X011X0?XXX000000001</td>
<td>6</td>
</tr>
<tr>
<td>X11?X01XXX111111111</td>
<td>7</td>
</tr>
<tr>
<td>X1?1X00XXX000000001</td>
<td>8</td>
</tr>
<tr>
<td>X111X1?X1X110111111</td>
<td>9</td>
</tr>
<tr>
<td>X100X10X1X000000001</td>
<td>10</td>
</tr>
</tbody>
</table>
LRS: Risk of Creating Relationship

- Target User
- Stranger
- Window of friends of stranger
- Check New Relationship in White list
  - Family Relationship
  - Colleague
  - Neighbors

Top common relationship in the white list:

<table>
<thead>
<tr>
<th>Normal relationship</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>X110X11X1X101110111</td>
<td>1</td>
</tr>
<tr>
<td>X111X11XIX01111110?</td>
<td>2</td>
</tr>
<tr>
<td>X111X10XIX11011011</td>
<td>3</td>
</tr>
<tr>
<td>X101X01XIX111111111</td>
<td>4</td>
</tr>
<tr>
<td>X011X11XIX111110111</td>
<td>5</td>
</tr>
<tr>
<td>X011X01XIX111111111</td>
<td>6</td>
</tr>
<tr>
<td>X11?X01XIX111111111</td>
<td>7</td>
</tr>
<tr>
<td>X1?X00XX000000000</td>
<td>8</td>
</tr>
<tr>
<td>X111X?XIX110111111</td>
<td>9</td>
</tr>
<tr>
<td>X100X10XIX0000000001</td>
<td>10</td>
</tr>
</tbody>
</table>
References:

References:

References:

Thanks for your attention