SpamResist: Making Peer-to-Peer Tagging Systems Robust to Spam

Ennan Zhai, Ruichuan Chen, Eng Keong Lua*
Long Zhang, Huiping Sun, Zhuhua Cai
Sihan Qing, Zhong Chen

Peking University & *Carnegie Mellon University
Roadmap

I. What is the tag spam in P2P tagging systems?

II. What are the existing solutions on this problem?

III. Our approach?
Roadmap

I. What is the tag spam in P2P tagging systems?

II. What are the existing solutions on this problem?

III. Our approach?
Tagging Systems

There are some tagging services-based systems in our lives … …
To meet the challenge, such as DoS or single point failure, tagging services are introduced into P2P content systems... ...
P2P Tagging Systems

To meet the challenge, such as DoS or single point failure, tagging services are introduced into P2P content systems...

For example, Tagster is an open source DHT-based P2P tagging system.

(http://isweb.uni-koblenz.de/research/tagster)
Tag Spam

The results for searching tag “iphone” in MyWeb.
The results for searching tag “iphone” in MyWeb.

When we click this link, we will find the following page ......
This Figure is not related to iPhones.

Small ROBOTIC BOATS from all over the world are set to race each other next year across the Atlantic, some 4,000 miles from Brittany, France, to the Caribbean. The race, called Microtransat 2008, was conceived by a computer scientist at the University of Wales, Aberystwyth. Entry boats must be “fully autonomous” (they can use GPS), self-sufficient in terms of energy (via solar panels) and no longer than 13 feet.

Original post by Mike

IPod Copying Software
Copy all your iPod content back into iTunes. PC or Mac. Try it free.

Archived at Google
Tag Spam

This Figure is not related to iPhones.

We can also observe that this site has been assigned many other popular but irrelevant tags.

Small ROBOTIC BOATS from all over the world are set to race each other next year across the Atlantic, some 4,000 miles from Brittany, France, to the Caribbean. The race, called Microtransat 2008, was conceived by a computer scientist at the University of Wales, Aberystwyth. Entry boats must be "fully autonomous" (they can use GPS), self-sufficient in terms of energy (via solar panels) and no longer than 13 feet.

Original post by Mike

iPod Copying Software
Copy all your iPod content back into iTunes, PC, or Mac, Then It's Free

Sponsored by Google

everything, ipod, ipod photos, ipod link, iphone hack, ipod work, ipod news, ipod video, 60 gig, iphone price drop, iphone business, iphone rumors, buy, ipod, iphone, linux, itunes, podcasting, iphone search, iphon, link, iphone user, ipod base, mac, ipod auction, apple, the apple store, ipod, itbook, iphone, ipod nano, ipod stories, songs, apple, reveal, apple information, apple work, ipod update, apple company, iphone deals, itunes download, apple superstore, apple search, ipod player, review, iphone software, apple mac, ipod, iphone information, macworld, ipod downloads, itunes search, ipod generation, ipod stereo, iphone games, iphone wifi, iphone blog, ipod information
That is the problem of tag spam!

**Definition of Tag Spam:** The erroneous or misleading tags that are generated by some malicious users to confuse the normal users in the systems.
Roadmap

I. What is the tag spam in P2P tagging systems?

II. What are the existing solutions on this problem?

III. Our approach?
Roadmap

I. What is the tag spam in P2P tagging systems?

II. What are the existing solutions on this problem?

III. Our approach?
Related Work

Detection-based Mechanisms.

Demotion-based Mechanisms.

Interface-based Mechanisms.
Related Work

Detection-based Mechanisms.

Demotion-based Mechanisms.

Interface-based Mechanisms.
Related Work

Detection-based Mechanisms.

Demotion-based Mechanisms.

Interface-based Mechanisms.
Related Work

Detection-based Mechanisms.

Demotion-based Mechanisms.

Interface-based Mechanisms.
Roadmap

I. What is the tag spam in P2P tagging systems?

II. What are the existing solutions on this problem?

III. Our approach?
What is the tag spam in P2P tagging systems?

What are the existing solutions on this problem?

Our approach?
SpamResist is a demotion-based mechanism, and encompasses two key parts:

- Reliability Mechanism;
- Social Network-based Enhancement.
SpamResist is a demotion-based mechanism, and encompasses two key parts:

- Reliability Mechanism;
- Social Network-based Enhancement.
For each tag (e.g., Sea) search, client calculates a **reliability degree** for each respondent, and uses weighted averaging to compute the rank of the search results.
For each tag (e.g., Sea) search, client calculates a **reliability degree** for each respondent, and uses weighted averaging to compute the rank of the search results.

The peer who annotated some local files with “Sea” will respond the client with these files. We call this peer as respondent.
For each tag (e.g., Sea) search, client calculates a reliability degree for each respondent, and uses weighted averaging to compute the rank of the search results.

Weight is the reliability degree of the owner of each response resource.
What is reliability mechanism?

For each tag (e.g., Sea) search, client calculates a **reliability degree** for each respondent, and uses **weighted averaging** to compute the rank of the search results.

Weight is the **reliability degree** of the owner of each response resource.

How the client to compute the reliability degree for each peer?
How to compute reliability?

Reliability degree is a personalized score assigned to each peer by the client, and SpamResist proposes two schemes for the client to calculate the reliability degrees of two categories of peers respectively:

• Unfamiliar peers;

• Interacted peers.
Reliability degree is a personalized score assigned to each peer by the client, and SpamResist proposes two schemes for the client to calculate the reliability degrees of two categories of peers respectively:

- Unfamiliar peers;
- Interacted peers.

Normally, the behaviors that peer $A$ downloads some files from peer $B$ are called *interactions* between $A$ and $B$. 
Reliability degree is a personalized score assigned to each peer by the client, and SpamResist proposes two schemes for the client to calculate the reliability degrees of two categories of peers respectively:

- Unfamiliar peers;
- Interacted peers.

The peers that the client has never interacted with.
Unfamiliar Peer’s Reliability

\[
R_{A,B} = \frac{\sum_{f_i \in F} \left( \sum_{t_j \in C_{f_i}} |P(f_i, t_j)| \right)^2}{\sqrt{\sum_{f_i \in F} \left( \sum_{t_j \in T_A} |P(f_i, t_j)| \right)^2}} \sqrt{\sum_{f_i \in F} \left( \sum_{t_j \in T_B} |P(f_i, t_j)| \right)^2}
\]

where

- \( F \): The set of files owned by \( A \) and \( B \) in common.
- \( f_i \): The \( i^{th} \) file of the common file set \( F \).
- \( C_{f_i} \): The set of the tags annotated by \( A \) and \( B \) in common to the file \( f_i \).
- \( t_j \): The \( j^{th} \) tag of the tag set.
- \( T_x \): The set of tags annotated by the peer \( x \) to the file \( f_i \).
- \( P(f_i, t_j) \): The set of annotation that annotated \( f_i \) with \( t_j \).
- \( |P(f_i, t_j)| \): The size of \( P(f_i, t_j) \).
Reliability degree is a personalized score assigned to each peer by the client, and SpamResist proposes two schemes for the client to calculate the reliability degrees of two categories of peers respectively:

• Unfamiliar peers;
• Interacted peers.

The peers that the client has interacted with.
Interacted Peer’s Reliability

The client stores the previous experiences from the interacted peers in his own experience vector \( (EV_{A,B}) \).

\[
\left< v_{A,B,1}, v_{A,B,2}, \ldots, v_{A,B,n} \right>
\]
Interacted Peer’s Reliability

The client stores the previous experiences from the interacted peers in his own experience vector \((EV_{A,B})\).

\[
\left\langle v_{A,B,1}, v_{A,B,2}, \ldots, v_{A,B,n} \right\rangle
\]

Specifically, for the peer \(B\) that client \(A\) has interacted with, \(A\) maintains a vector of length \(n\) storing the most recent \(n\) experiences with \(B\), and as new experiences are appended the oldest ones are removed.
Interacted Peer’s Reliability

\[
\vartheta_{A,B,k} = \lambda_{A,B,k} \cdot R_{A,B,k}, \quad 1 \leq k \leq n
\]  

(2)

where

- \( \lambda_{A,B,k} \): The evaluation of the interaction which is represented by the \( k \)th element of \( EV_{A,B} \), and the value is \(-1\) or \(+1\), where \(-1\) represents erroneous annotation and \(+1\) represents accurate annotation.

- \( R_{A,B,k} \): The reliability degree, from \( A \) to \( B \), of the interaction which is represented by the \( k \)th element of \( EV_{A,B} \).
The client stores the previous experiences from the interacted peers in his own experience vector \((\text{EV}_{A,B})\).

\[
\langle v_{A,B,1}, v_{A,B,2}, \ldots, v_{A,B,n} \rangle
\]

Reliability degree from A to B (interacted peer for A) is:

\[
\frac{v_{A,B,1} + v_{A,B,2} + \ldots + v_{A,B,n}}{n}
\]
SpamResist is a demotion-based mechanism, and encompasses two key parts:

- Reliability Mechanism;
- Social Network-based Enhancement.
SpamResist is a demotion-based mechanism, and encompasses two key parts:

- Reliability Mechanism;
- Social Network-based Enhancement.
Social Network-based Enhancement

• Re-compute the ranking score (RS) for the result file whose RS is lower than 0.5.

• If more than half of friends have RS higher than 0.5, re-locate the position.

• According to average of scores higher than 0.5.
Social Network-based Enhancement

<table>
<thead>
<tr>
<th>Alice’s search result</th>
<th>Ranking Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>sea.jpg</td>
<td>0.4</td>
</tr>
</tbody>
</table>
Social Network-based Enhancement

Alice’s search result | Ranking Score
---|---
sea.jpg | 0.4

Alice’s Friends
Social Network-based Enhancement

Alice’s search result | Ranking Score
---|---
sea.jpg | 0.4

Alice’s Friends

Ranking Scores

0.7 0.8 0.4
Social Network-based Enhancement

<table>
<thead>
<tr>
<th>Alice’s search result</th>
<th>Ranking Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>sea.jpg</td>
<td>0.4</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Alice

Alice’s Friends

(0.7 + 0.8) / 2 = 0.75
Alice's search result | Ranking Score
---|---
sea.jpg | 0.4

\[(0.7 + 0.8) / 2 = 0.75\]
### Social Network-based Enhancement

<table>
<thead>
<tr>
<th>Alice’s search result</th>
<th>Ranking Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>sea.jpg</td>
<td>0.75</td>
</tr>
</tbody>
</table>

Alice’s Friends

\[(0.7 + 0.8) / 2 = 0.75\]
### Social Network-based Enhancement

<table>
<thead>
<tr>
<th>Alice’s search result</th>
<th>Ranking Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>sea.jpg</td>
<td>0.4</td>
</tr>
</tbody>
</table>

- **Alice**
  - Ranking Score: 0.5
- **Alice’s Friends**
  - Ranking Score: 0.3, 0.2
Social Network-based Enhancement

- The details about social network-based enhancement mechanism of SpamResist please see our paper.
Social Network-based Enhancement

- The details about social network-based enhancement mechanism of SpamResist please see our paper.

- The practical issue on unreliable friends please see our paper.
Evaluation

Search Models:

• Boolean Model.
• Occurrence Model.
• Coincidence Model.
• PINTS.
Evaluation

Search Models:

- Boolean Model.
- Occurrence Model.
- Coincidence Model.
- PINTS.
The search strategy of Boolean is the system randomly ranks the results associated with the search tag.
Evaluation

Search Models:

- Boolean Model.
- Occurrence Model.
- Coincidence Model.
- PINTS.
Evaluation

Search Models:

• Boolean Model.
• Occurrence Model.
• Coincidence Model.
• PINTS.
Occurrence model ranks the search results based on the number of annotations containing the searched tag and returns the top ranking results.
Evaluation

Search Models:

- Boolean Model.
- Occurrence Model.
- Coincidence Model.
- PINTS.
Evaluation

Search Models:

- Boolean Model.
- Occurrence Model.
- Coincidence Model.
- PINTS.
Coincidence model assigns each user a score computed by the number of the annotations overlapped with other users in the system.
Evaluation

Search Models:

- Boolean Model.
- Occurrence Model.
- Coincidence Model.
- PINTS.
Evaluation

Search Models:

- Boolean Model.
- Occurrence Model.
- Coincidence Model.
- PINTS.
The strategy of PINTS is the client first generates a feature vector to store a characteristic score for each peer in system; then, using the vector, the client aggregates the information of annotations selectively, and randomly ranks the search result.
Evaluation

Threat Models:

- **Random Attacks**: randomly annotate misleading tags to the resources in the system;

- **Targeted Attacks**: collusively annotate resources with the same misleading tags;

- **Tricky Attacks**: annotate resources with both correct and misleading tags. This attack could make some anti-spam scheme unusable.
Evaluation

The impact of random attack under 20% random attackers (more detail see paper)
Evaluation

The impact of targeted attack under 20% targeted attackers (more detail see paper)
Evaluation

The impact of tricky attack under 20% tricky attackers (more detail see paper)
Conclusion

SpamResist is a novel social reliability-based mechanism towards spam-free and personalized tag search results in the P2P tagging systems.
Q & A