

評判システムにおける結託攻撃の影響を軽減する計算方式

堺 竜太郎[†] 佐藤 文明[‡]

東邦大学大学院理学研究科[†] 東邦大学理学部[‡]

1. はじめに

近年ネットワーク技術の進歩や、インターネット接続環境の普及によりネットワーク利用者が増加している。ネットワーク上で利用者が情報交換や情報提供をするネットコミュニティでは多種多様な情報が提供されるため、コミュニティの参加者同士で情報を評価し、その評価を集約して評判として参加者に提示し、参加者への情報選択の指標を与える評判システムが提案されているが、評判システムが有効に機能するためには、質の良い評価を集めて信頼性の高い評判を計算する必要がある。

評判の計算方法として、EigenRumor アルゴリズム[1]を用いた計算方法が研究されている。しかし、EigenRumor では、他人と同じような振る舞いをしているユーザーが特定のオブジェクトを標的に攻撃をすると、不正な評価をされたオブジェクトの評判値が増え、評判システムを混乱させてしまうといった問題点がある。

そこで本稿では、EigenRumor が評判値の計算を行う際に評価者自身と評価者全体との評判値のズレを計算し、評判値を計算する提案手法を用いて複雑な条件の攻撃からの耐性の評価実験によって有効性を確認した。

2. EigenRumor

2.1. アルゴリズム

EigenRumor アルゴリズム (図 1) は PageRank[2] や HITS[3]と同様にリンクから生成した行列の固有ベクトルを計算することにより各スコアを計算することを基本とする。ただし、PageRank や HITS はオブジェクト間のリンクからオブジェクトの指示の度合いを示す隣接行列を生成するのに対し、EigenRumor はエージェント (参加者) とオブジェクト (情報) 間のリンクからエージェントからオブジェクトを提供の状態を表す提供行列 P とエージェントがオブジェクトを評価した状態を表す行列 E を生成することを特徴とする。情報提供スコアは参加者が良い情報を提供する能力を表し、情報評価スコアは参加者の情報評価能力の高さを表す。

```

 $\vec{a}^{(0)} = (1, \dots, 1)^T$ 
 $\vec{h}^{(0)} = (1, \dots, 1)^T$ 
while  $\vec{r}$  change significantly do
   $\vec{r}^{(k)} = \alpha P^T \vec{a}^{(k)} + (1 - \alpha) E^T \vec{h}^{(k)}$ 
   $\vec{r}^{(k+1)} = \vec{r}^{(k)} / \|\vec{r}^{(k)}\|_2$ 
   $\vec{a}^{(k+1)} = P \vec{r}^{(k+1)}$ 
   $\vec{h}^{(k+1)} = E \vec{r}^{(k+1)}$ 
end while
 $\vec{a}$ : 情報提供スコア
 $\vec{h}$ : 情報評価スコア
 $\vec{r}$ : 評判スコア

```

図 1 EigenRumor アルゴリズム

2.2. EigenRumor の評価

シミュレーションで EigenRumor の評価実験を行った。

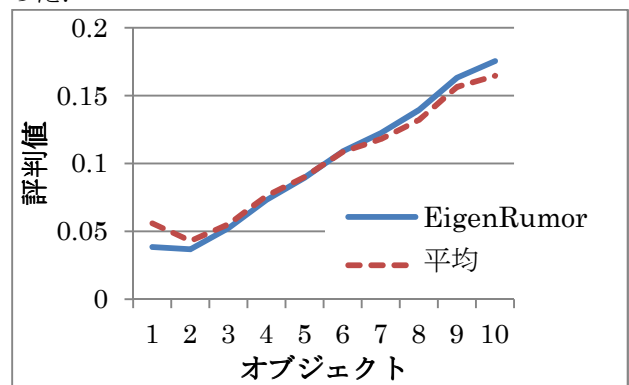


図 2 EigenRumor の評価

評価能力の高いユーザーを仮定し、オブジェクトに一定の評判値を与えるように設定し、評価能力の低いと仮定したユーザーには、評価能力の高いユーザーが支持した値の逆数の評価を与えるように設定し、得られる評判値で平均値計算との比較実験を行った。また、与える評判値は変化が見やすいようオブジェクトの番号が後になるほど高い評判値を得よう傾斜を与えた。参加者 10 人、オブジェクト数 10 個とし、提供行列 P 評価行列 E はそれぞれ最大 100 リンク存在するものとした。図 2 は評価実験の結果である。実験結果より、現在主に利用されている評判値の平均計算よりも EigenRumor のほうが攻撃耐性に優れていることが明らかである。

しかし、EigenRumor の問題点として、他人と同じような振る舞いをしているユーザーが特定のオブジェクトを標的に攻撃をすると、不正な評価をされ

A Calculation Method to Reduce Influence of Collusion Attack in Reputation System

[†]Ryutaro Sakai, Toho University, Graduate School of Science

[‡]Fumiaki Sato, Toho University, Department of science

たオブジェクトの評判値が増え、評判システムの全データに対して悪影響を与えてしまうことが挙げられる。そこで、シミュレーションにより、問題となっている攻撃への耐性の評価実験を行った。

参加者は乱数でオブジェクトを評価するものとし、不正なユーザーを 10 人用意し、不正なユーザーにはオブジェクトの 1 を通常の 5 倍の点数で評価するように設定した。参加者 100 人、オブジェクト数 100 個とし、提供行列 P 評価行列 E はそれぞれ最大 10000 リンク存在するものとした。(図 3)

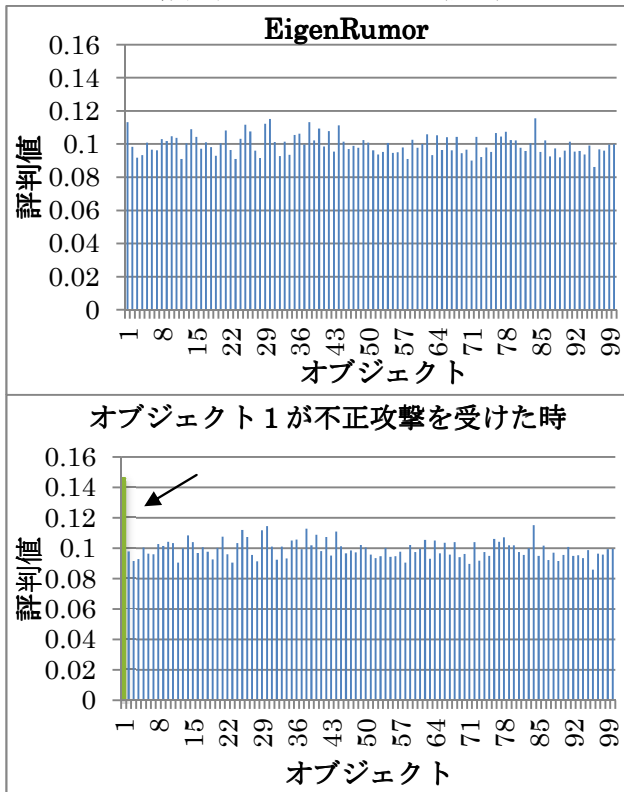


図 3 EigenRumor への結託攻撃の影響

実験結果より結託攻撃が行われていないオブジェクト 1 の評判値が約 0.11 であるのに対し結託攻撃が行われた場合評判値が約 0.15 と大きく影響を受けることが明らかとなった。そこで、このような結託攻撃による影響を軽減する計算方式を提案する。

3. 提案方式

提案方式では、評判値の計算を行う際、評価者自身と評価者全体との評価値のずれの標準偏差を計算し、それより大きくずれているようであれば評価値を平均値に置き換えて評価するようにした。(図 4)

閾値に標準偏差を用いたのは、EigenRumor アルゴリズムでは評価者の評価値が他のエージェントと近い場合には評価能力が上がり、評価値がばらけている場合には評価能力が下がるため、標準偏差が小さく評価能力の高いエージェントによる結託攻撃を効果的に軽減することができるためである。

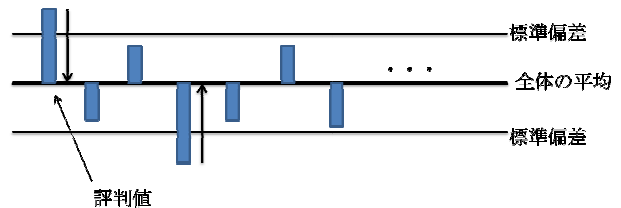


図 4 提案方式

4. 評価

プログラムで提案方式を実装し、EigenRumor との比較実験を行った。提案方式と EigenRumor のそれぞれの参加者に他人と同じ振る舞いを見せ、オブジェクト 1 に対して異常に高い評価を与える不正なユーザーを設定し、不正なユーザーの全体に占める割合を変化させて実験した。参加者 100 人、オブジェクト数 100 個とし、提供行列 P 評価行列 E はそれぞれ最大 10000 リンク存在するものとした。(図 5)

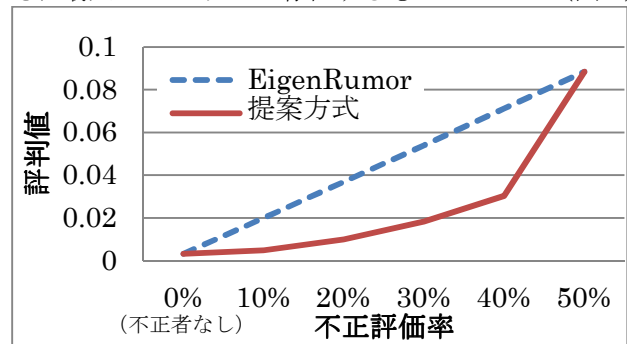


図 5 EigenRumor と提案方式の比較

実験結果より EigenRumor では大きく影響を受けていた結託攻撃による影響が提案方式では大幅に軽減されることが明らかになった。

5. まとめ

本稿では EigenRumor では防ぐことができなかった結託攻撃による影響を軽減する計算方式を提案した。今後の課題として、現在のアルゴリズムでは標準偏差を超えたものについて平均値を取らせるようにしているが、閾値や重みを利用したものに変更し評価を行ってみること。また、Web 上の評判システムからデータを入手し、実データを用いて評価を行ってみる予定である。

参考文献

- [1] 谷本直人 藤村孝 ネット上のコミュニティにおける情報の評判計算アルゴリズム EigenRumor 情報処理学会研究報告. マルチメディア通信と分散処理研究会報告 2005(3), 37-42, 2005-01-19
- [2] S. Brin and L. Page, "The Anatomy of a Large-scale Hypertextual Web Search Engine," in Proceedings of 7th International World Wide Web Conference, 1998.
- [3] J. M. Kleinberg, "Authoritative sources in hyperlinked environment," Journal of the ACM, Vol. 46, No. 5, 1999.