Interaction-based Reputation Model in Online Social Networks

Izzat Alsmadi[1], Dianxiang Xu[2] and Jin-Hee Cho[3]
[1]*Department of Computer Science, University of New Haven, West Haven, CT, U.S.A.*
[2]*Department of Computer Science, Boise State University, Boise, ID, U.S.A.*
[3]*US Army Research Laboratory, Adelphi, MD, U.S.A.*

Keywords: Online Social Networks, Reputation, User Attributes, Privacy, Information Credibility.

Abstract: Due to the proliferation of using various online social media, individual users put their privacy at risk by posting and exchanging enormous amounts of messages or activities with other users. This causes a serious concern about leaking private information out to malevolent entities without users' consent. This work proposes a reputation model in order to achieve efficient and effective privacy preservation in which a user's reputation score can be used to set the level of privacy and accordingly to determine the level of visibility for all messages or activities posted by the users. We derive a user's reputation based on both individual and relational characteristics in online social network environments. We demonstrate how the proposed reputation model can be used for automatic privacy assessment and accordingly visibility setting for messages / activities created by a user.

1 INTRODUCTION

As the use of online social network (OSN) applications becomes more and more popular than ever, many people share their daily lives by posting stories, comments, videos, and/or pictures, which may expose their private / personal information (Mansfield-Devine, 2008). In such contexts, privacy became a critical issue because private information can be exposed to the public (e.g., by search engines) without the user's consent.

This work proposes a reputation model that evaluates an individual's reputation based on his/her interactions with peers such as friends in OSNs. Reputation is defined as an opinion about an entity, either something or someone including a person, organization, service, etc., based on third parties' opinions (e.g., recommendations). In particular, many OSN sites have different mechanisms to estimate reputation. For example, *Facebook* uses the concept of a friend with three different levels such as close friend, friends, and acquaintances in order to categorize the closeness-based friendship. This kind of friends can be designated by an individual user and does not represent the degree of friendship based on the amount of interactions between two individual users. Similar to web ranking algorithms, some algorithms of scoring friendship use the number of interactions (e.g., likes, tags, posts, comments) to calculate the degree of friendship between two entities (Jones et al., 2013).

An individual user's reputation can be determined based on a variety of aspects of the user's attributes. One of the important attributes is whether the user feeds quality information such as correct, accurate, or credible information. While users are free to post their opinions, OSNs should promote propagation of credible information to maintain friendly, healthy OSN environments. To this end, we propose our reputation model in which reputation is computed based on a user's *personal attributes* embracing his/her background and affiliations and *relational attributes* including interactions with others and the reputation levels of the user's friends.

An example scenario can be as follows. User i continuously posts highly helpful, relevant information in OSNs. When user j continuously interacts with those posts fed by users i and j will be listed as one of top contributors for those activities. User j can list user i as one of his/her top peers. In terms of user j's reputation, user i, one of j's top peers, is a key contributor to improve user j's reputation. Accordingly, user i will be encouraged to post such types of activities that may attract more interactions with other peers, leading to increasing her/his reputation indirectly.

Many OSN applications are equipped with their

Alsmadi, I., Xu, D. and Cho, J-H.
Interaction-based Reputation Model in Online Social Networks.
DOI: 10.5220/0005668302650272
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 265-272
ISBN: 978-989-758-167-0

own algorithms to estimate peer relationships. For instance, *Facebook* calculates "close friends" or ranks each friend based on interactions including profile view, group interactions, the number of *likes* and/or recency of interactions. In this work, we aim to propose a generic model of reputation which can represent comprehensive aspects of an individual's trust based on collected information for statistical calculation / analysis but without revealing any private content of an individual such as activity content, or friends' identities without the user's consent. Therefore, our proposed reputation model is to assess an individual's reputation based on his/her individual and relational attributes while preserving the individual's privacy.

This paper has the following contributions:

- We propose a reputation model in which reputation score is derived from multiple aspects of a user, particularly, in terms of individual attributes and relational attributes. This way of estimating reputation is to ensure the quality of an information provider by assessing a user's personal attribute (e.g., work, education, interest groups) while assuring information credibility based on the popularity of activities created by the user. In addition, by assessing the quality of peers exhibiting active interactions through the user's activities, the reputation score of an entity can represent multidimensional aspects of trustworthiness in each entity.
- Although an entity's reputation value is derived from multidimensional aspects of his/her attributes, the proposed reputation model aims to preserve the user's privacy by not exposing any information to any peers without the user's consent. In particular, since reputation is estimated based on the amount of interactions but the content of activities / messages, an entity's privacy is well preserved unless the entity permits special actions to manually set the privacy level (e.g., special permission for a spouse to see all the activities / messages although he / she is not active on online interactions).
- The proposed reputation model is adaptive to reflect the dynamic evolution of an entity's reputation. As an entity's interactions or activities are updated, the entity's reputation is updated as well and accordingly it will be reflected in updating privacy setting for each peer on visibility of activities / messages the user posts. In addition, our reputation model allows human intervention (e.g., a user can manually modify privacy setting for a particular peer) when the automated system setting of privacy is not agreed with the need of a user. The reputation-based privacy setting can be an adaptive support mechanism for a user to set his/her privacy setting more effectively and efficiently.

The rest of this work is organized as follows. Section 2 discusses how an entity's reputation is derived by describing each component of reputation. Section 3 describes how the proposed reputation model is applied to privacy assessment in OSNs. Section 4 gives an overview of related work in terms of existing models of trust, reputation, and privacy in OSNs. Section 5 concludes this work and suggests future work directions.

2 REPUTATION MODEL

The focus of the proposed reputation system is on how to derive reputation score for a user, either an individual user or an organization, who has an account in social network media. In this work, we consider a graph G where an entity is a vertex, v_i and the social relationship between two entities, i and j, is an edge, $e_{i,j}$, as many studies assume. If two entities are connected with an edge, this means the two entities are friends to each other. But note that the degree of trust a different entity has towards a same third-party entity is different, implying the trust relationship is subjective and asymmetric (Cho et al., 2011).

We estimate an individual user's reputation score based on the following three components:

- *Personal attributes* including occupation, education level, affiliated groups, favorites, interest, or political leaning which may represent an entity's social identity;
- *Personal activities* representing the quality and quantity of interactions with other friends through posts, likes, tweets, creation of interest-driven groups;
- *Characteristics associated with an individual's friends* indicating the amount of interactions with friends and the friends' reputation levels;

The first component is called *individual attributes* while the other two components are called *relational attributes*. Figure 1 describes what characteristics of an individual user are considered to derive a reputation score as discussed above. To be specific, top L personal attributes, top M personal activities, and top K peers are considered to derive the user's overall reputation. Individual user i's reputation score, R_i, can be given by:

$$R_i = \alpha \times P_{i,L} + \beta \times P_{i,M} + \mu \times R_{i,K} \quad (1)$$

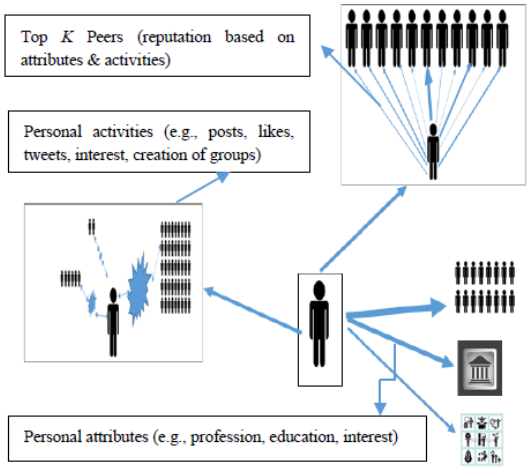

Figure 1: Components of Reputation Score.

$P_{i,L}$ is i's reputation score towards top L personal attributes, $P_{i,M}$ is i's reputation score towards top M personal activities, and $R_{i,K}$ represents i's top K friends' reputation scores. Each reputation component is weighted by α, β, and μ which can be adjusted based on the need of a given OSN application. Each reputation score is computed by

$$P_{i,L} = \sum_{l=1}^{L} P_{i,l} \quad (2)$$

$$P_{i,M} = \sum_{m=1}^{M} P_{i,m} \quad (3)$$

$$R_{i,K} = \sum_{k=1}^{K} R_{i,k} \text{ for } e_{i,k} > 0 \quad (4)$$

Note that $e_{i,k} > 0$ means users i and k are friends to each other. $P_{i,l}$ is attribute l's score, $P_{i,m}$ is activity m's score, and $R_{i,k}$ is user k's reputation score where i has attribute l, activity m, and friend k. The score of each reputation component is computed as:

- The rank of top personal attributes is derived from the reputation scores of the OSN websites of i's current profession, highest degree institution and joined social network groups;
- The rank of top personal activities is determined based on the amount of popular activities a user has (e.g., popular posts, activities); and
- The rank of top peer's reputation is calculated based on reputation scores for peers who interact most with individual i's activities.

2.1 Top Personal Attributes

A user entity, either individual user or organization (e.g., company, universities, or government), may have its individual online social network page. All the entities may have their gateways to the different OSNs in addition to the main entity portal. For some entities, their social network pages are visited as often as their main portals by having a great number of members, friends, or subscribers. Estimated reputation scores of those entities can be used for several possible use cases. For example, the rank of a university (e.g., academic reputation) may be significantly impacted by the entity reputation score.

If an entity is an individual user (e.g., person, professional service provider), we consider three personal attributes in terms of three categories including personal background (e.g., education, occupation, interest, political leaning), involved activities, and peers' activities, as discussed earlier. If an entity is an organization or service provider, the personal background is replaced with the attributes and past reputation of an organization such as a number of employees (e.g., students, members), quality of employees (e.g., acceptance rate for a university), salary levels, and/or historical reputation (e.g., top ranked for best work places).

2.2 Top Personal Activities

We consider what kinds of activities an entity[1] is involved with and how popular the activities are among its peers. For example, when entity i creates activity l which receives a large amount of positive feedback by entity i's peers, referred by other individual entities j's (e.g., likes, favorites, tweets, retweets, positive comments), entity i's reputation may increase due to its popular activity l. Each activity can be weighted differently depending on importance or specific needs. For simplicity, we consider each activity is weighted equally in this work. More specifically, we consider *positive popularity* as a form of reputation in which we distinguish negative feedback from positive feedback. To be specific, we calculate the reputation or i's personal activity l as

$$P_{i,l} = \frac{I^{+}_{i,l}}{I^{+}_{i,l} + I^{-}_{i,l}} \quad (5)$$

$I^{+}_{i,l}$ indicates the number of positive feedback and $I^{-}_{i,l}$ is the number of negative feedback on activity l, respectively. The example can be 'likes' or 'dislikes' for posts / activities.

Even if entity i's peer, j, is listed in entity i's top peers, entity j is not necessarily highly active to in-

[1] An entity refers to a user in OSNs. We interchangeably use an entity or a user to refer to a person or an organization in OSNs.

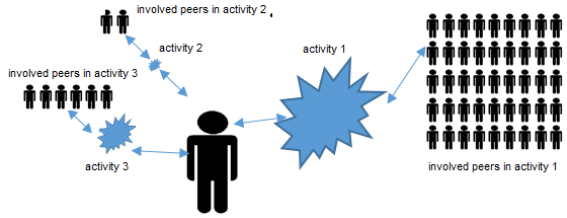

Figure 2: Activity Rank.

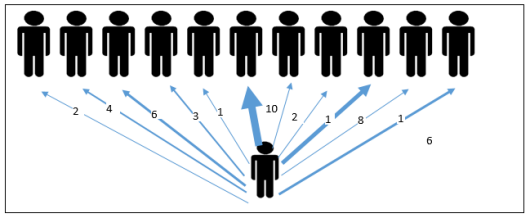

Figure 3: Edge Rank.

N1	25.0	5.2	22.0	5.4	14.0	2.5	N3, N9, ...
N2	35.6	75.0	2.5	50.0	88.0	9.1	N1, N70, ...
N3	70.0	12.0	23.0	12.0	9.0	5.2	N30, N35 ...
N4	40.0	5.4	16.6	18.0	18.0	4.0	N9, N14, N30, N35 ...
N5	29.0	70.0	25.0	25.0	23.0	8.2	, N36, N35...
N6	50.0	66.0	50.0	7.2	23.0	12.3	N19, ...
N7	24.0	22.0	5.2	19.0	18.0	3.3	N3, ...
N8	75.0	66.0	15.1	88.0	58.0	13.5	N12, N30, N35 ...
N9	30.0	30.0	24.0	23.0	18.0	5.4	N30, N39 ...
N10	14.8	88.0	58.0	131.0	60.0	23.1	N20, ...
N11	23.0	5.4	20.0	20.0	18.0	3.3	N9, N30, N35, ...
N12	75.0	131.0	4.9	142.0	54.0	15.1	N15, N30, N35 ...
N13	23.0	21.0	20.0	19.0	18.0	4.1	N30, N35 ...
N14	58.0	23.1	54.0	162.0	49.0	16.6	N10, N30, N35 ...
N15	30.0	28.0	21.0	20.0	18.0	4.9	N30, N35 ...
N16	60.0	7.2	49.0	157.0	55.0	14.5	N19, N30, N35 ...
N17	21.0	23.0	20.0	23.0	12.0	4.0	N10, N50, N35 ...
N18	54.0	157.0	55.0	168.0	58.0	35.6	N30, N55 ...
N19	40.0	23.0	20.0	58.0	23.0	7.2	N30, N35 ...
N20	49.0	3.3	58.0	168.0	70.0	14.8	N30, N35 ...

Figure 4: Edge Rank Table with Top Friends Markings.

volve a high ranked activity l led by entity i. Commonly, the highly ranked activity l tends to be liked by most of peers, rather than a particular set of peers.

Activities are ranked based on the volume of interactions with friends, as shown in Figure 2. In this model, we assume that all activities and types of interactions with friends have an equal weight.

2.3 Top Peers' Reputation

We consider user i's peers', j's, reputation in order to derive user i's reputation as well. User i assesses j's reputation based on the trust i has in j based on the interactions between i and j. The interactions include the amount of interactions involved in the activities created by user i. That is, when user j provides highly positive feedback towards i's activity, l, such as likes, tweets, retweets, favorites, trust, comments, etc., i's trust towards j increases. Note that the trust i estimates towards j is about the relationship between i and j, not based on j's personal attributes. Trust is *asymmetric* in relationships. Even if j provides a large amount of highly positive feedback towards i's activity, it does not mean user i also provides the exactly the same amount of positive feedback towards user j's activity. There would be a different number of activities each i or j is involved with; i and j may have different personal disposition such as introvert or extrovert which may respond differently towards an activity. However, a certain level of reciprocal relationship may exist which can be broadly said 'friendly', 'indifferent', or 'hostile' relationship although the amount of responsiveness towards each other may not be exactly same. Edge $e_{i,j}$ indicates there exists an edge between i and j. Edge rank of $e_{i,j}$ indicates the amount of interactions between these two users, by increasing the rank upon interaction. This is demonstrated in Figure 3 where the thickness of a line between two entities indicates the degree of trust from a trustor (evaluator) to a trustee (evaluatee). Note that as the trust relationship is asymmetric, we distinguish edge $e_{i,j}$ from edge $e_{j,i}$.

Each user may request a monthly report for edge rank statistics. For simplicity, we represent the active peer as binary such as active (i.e., existence of interactions) vs. inactive (i.e., no interaction) per the user's activity.

3 REPUTATION-BASED PRIVACY ASSESSMENT

We target our proposed reputation model to be applied to privacy assessment in various social networking sites (e.g., Facebook, Twitter, LinkedIn, Snapchat). Here we discuss a case study for privacy assessment based on activity logs collected at real time.

Figure 4 shows a dataset of 20 users (i.e., nodes) that can be collected from a social networking site. We assume that the social networking site allows users to create different types of activities (e.g., text, image, post, video, etc.) and to add other users to their page as friends such as *Facebook*. Each user interacts with his/her friends via activities it creates.

Each column represents three reputation components discussed in Section 2, including *personal attributes*, *personal activities*, and *peers' reputation*. For this case study, we pick a set of weights for reputation components, α, β, and μ which are set to 0.8, 0.3, and 0.05 respectively, where each weight is ranged in $[0, 1]$.

	α = 0.8				β = 0.3						μ = 0.05						
	Personal Attributes			Part1	Highest Activities					Part2	Highest Peers					Part3	Reputation
N1	3	7	6	12.8	8	7	6	4	2	7.98	25	5.2	22	5.4	14	2.5	23.3
N2	1	7	5	10.4	8	8	8	5	5	11.16	35.6	75	162	50	88	9.1	30.7
N3	4	7	5	12.8	8	8	7	7	6	11.34	70	12	23	12	9	5.24	29.4
N4	5	8	4	13.6	9	9	9	8	8	14.79	40	5.4	27	18	18	4.0	32.4
N5	3	8	5	12.8	9	9	7	7	7	12.57	29	70	25	25	23	8.2	33.6
N6	1	4	6	8.8	9	8	8	7	6	12.36	50	66	50	7.2	23	12.3	33.4
N7	6	6	7	15.2	10	10	10	9	7	16.8	24	22	20	19	18	3.3	35.3
N8	7	3	8	14.4	10	8		8	5	6.9	75	66	75	88	58	13.5	34.8
N9	8	2	9	15.2	6	6	6	5	5	8.04	30	30	24	23	18	5.4	28.6
N10	4	9	9	17.6	6	6	5	4	4	6.9	14.8	88	58	131	60	23.1	47.6
N11	5	7	10	17.6	6	5	5	4	3	6.15	23	5.4	20	20	18	3.3	27.1
N12	6	6	7	15.2	7	7	7	6	6	10.11	75	131	60	142	54	15.1	40.5
N13	2	4	6	9.6	7	7	7	7	4	9.81	23	21	20	19	18	4.1	23.5
N14	3	5	2	8	8	8	7	6	5	10.74	58	23	54	162	49	16.6	35.3
N15	4	3	4	8.8	9	9	7	7	7	12.57	30	28	21	20	18	4.9	26.2
N16	8	4	3	12	9	8	8	8	6	12.66	60	7.2	49	157	55	14.5	39.1
N17	9	10	4	18.4	10	9	9	6	6	13.89	21	23	20	23	12	4	36.2
N18	2	6	5	10.4	10	7	7	7	5	11.01	54	157	55	168	58	35.6	57.0
N19	3	7	7	13.6	6	6	6	5	5	8.04	40	23	20	58	23	7.2	28.8
N20	4	4	6	11.2	9	8	8	6	5	11.76	49	3.3	58	168	70	14.8	37.8

Figure 5: Example of Reputation Score Table.

In this case study, we weigh more on personal characteristics (i.e., individual reputation) than relational characteristics (i.e., interactions with friends via activities & peers' reputation). A weight of each reputation component can be adjusted depending on the need or requirement of a given OSN. α, β, and μ are fixed for all users for fairness. The weights can be periodically updated based on historical data in order to avoid any dominance of a single component.

To measure reputation based on personal attributes, current work, highest education, and affiliated interest groups are considered and their own scores are included as part of individual score. The reputation rank can be derived for those entities from the same OSN. For top peers or activities, we use top five peers or activities to represent an individual user's reputation. We equally weight each personal attribute, peer, or activity for simplicity in this work. However, it can be adjusted in order to reflect different criteria of reputation.

In Figure 5, the following features are presented:

- The three constant weights (i.e., α, β, μ) can have a significant impact on the overall reputation value. The values of those weight parameters should be fixed for all users. Ultimately, they should be calculated based on the analysis of a large volume of historical data in the same OSN in order to identify the importance of each attribute in determining the value of each weight.
- When users are in the top 5 peers of each other (e.g., a spouse or a couple), we call it a *circular dependency* problem. The reputation scores for a couple listed in top peers of each other should not be calculated simultaneously. We should ensure to avoid circular dependency problem so that it is unlikely that top 5 activities for the same couple will be adjusted simultaneously. Similarly, a circular dependency may occur between an organization (e.g., universities or companies) and its affiliated individuals. Reputation ranks of such entities (e.g., universities or companies) are expected to change less frequently in comparison with those of individual users.
- Users may increase their reputation ranks trough various ways including legitimate or illegitimate activities. Reputation models should detect anomaly behavior in the evolution of reputation.

One application for using friends' automatic classification system is to decide visibility levels on users' created activities. Close friends should be given higher visibility access. Higher privacy corresponds to lower visibility on sensitive information. Sentimental analysis can be used to automate the process of privacy level classification. This can work as an alternative to users' manual classification for the privacy level of their posted activity. Friends with high trust edges (e.g., spouse, couple, close friends) can be assigned to high privacy/visibility while friends with low trust edges (e.g., acquaintances) can be assigned to low privacy/visibility. Thus, top K peers can have the highest visibility/privacy.

The advantages of the proposed privacy assessment model are summarized as follows:

- Privacy assessment can be automatically set based on the calculated edge rank of each peer; users only need to set privacy category (e.g., low, medium, high) for an activity they create, and the eligible peers for the post visibility will be automatically determined based on the edge rank of each peer.
- If the system's automatic decision of post visibility is not agreed by a user, the user can manually modify the visibility to a particular peer. This allows the flexibility that accepts a user's input in order to be adaptive to the user's need. That is, privacy assessment system dynamically determines a user's privacy setting based on top K peers identified over time or upon activities / interactions. But the system always allows the user to manually change the privacy setting depending on the need.
- Privacy assessment system allows a user to classify his/her friends based on the customized friendship categories by setting the range of each category. For example, based on the rank of each friend, a user can categorize: 75% and above for close friends (i.e., high visibility); 75% to 25 % for normal friends (i.e., medium visibility); and below 25% and below for acquaintances (i.e., low

visibility). Such three level classification can be used to control privacy and visibility of posts. A user can select the thresholds such as 75% and 25% as the above.

4 RELATED WORK

In this section, we discuss what trust, reputation, and privacy are and how they are used, measured, and implemented in OSN environments.

4.1 Trust Models in OSNs

Trust is defined as "assured reliance on the character, ability, strength, or truth of someone or something" (Merriam and Webster Dictionary, 2015). Trust indicates a relationship between two entities called a trustor and trustee in which the trustor assesses its subjective opinion towards the trustee based on given criteria. Since trust is a multidisciplinary concept, different types of trust relationships are used depending on a domain such as e-commerce settings, automatic computing, or communication networks (Cho et al., 2011).

The nature of trust has the following inherent properties (Cho et al., 2011):

- *Subjective*: Since a human entity has a different opinion based on its own subjective view, different individual entities may have different views towards a same entity;
- *Asymmetric*: When two entities are friends to each other, they may not trust each other with a same degree. That is, *A* may not trust *B* as much as *B* trusts *A*. In an extreme case, trust between two individuals can be directional such as the case that *A* trusts *B* while *B* does not trust *A* (Hardin, 2002).
- *Non-transitive*: Trust is not completely transitive or transferable. Although trust in communication networks has used to be transitive or transferable in PGP (Pretty Good Privacy) using the web of trust (Stallings, 1995), it is not true in social networks where an entity is a human and may have a different subjective perception or cognition in information processing.
- *Dynamic*: Trust decays over time without continuous interactions or changes as context changes. In social networks, the fluctuations of the quality and quantity of interactions hinder the continuous evolution of trust.
- *Context-dependent*: Trust is affected by a domain context. In particular, when a situation changes over time, the degree of perceived also changes. Jøsang and Pope (2005) call the context-dependent trust *decision trust* while the context-independent trust *reliability trust*. Decision trust is affected by what situation a trustor and trustee are placed (e.g., whether to use a wore rope to escape from a fire situation in building).

The concept and properties of trust have been utilized in various types of OSN applications in the literature. Ganzaroli (2002) and Murphy (2006) see trust as the continuous process to be built in institutional and structural contexts in addition to subjective viewpoints. Grabner-Krauter (2009) treats trust as an indicator of an individual's confidence in dynamic decision making context in which trust is used as an instrumental support emphasizing its practical use, in addition to subjective trust based on emotional nature.

Ferlander (2003) and Kavanaugh et al. (2005) discuss two types of trust in terms of the degree of information sharing. *Thick trust* is formed based on strong social ties through frequent direct interactions while *thin trust* is a weak social tie which is formed only based on a small amount of information sharing. In this sense, how much information is shared between two entities in social networks can be an indicator of more interactions leading to thick trust. This is often called *social capital* when the social relationship introduces productivity in real life (e.g., recruitment through social networks such as *LinkedIn*) (Woolcook, 2001).

Graph theories have been popularly used to model trust relationships in social networks (Marti et al., 2005; Zhang et al., 2006). Common challenges in using graph theory are in three-fold: (1) graph complexity where typical social networks are large in number of nodes, volume of interactions, etc.; (2) scaling of trust (e.g., binary, real number in [0, 1], nominal, categorical); and (3) validation of trust models in terms of trust accuracy. Richardson et al. (2003) consider continuous trust values, rather than categorical or nominal trust scale.

Kuter and Golbeck (2007) evaluate interactions between friends to rate movies by developing a trust model called *FilmTrust*. Compared to product ratings provided by many commercial websites, this rating can be seen to individuals as more "trustworthy" because the rates are evaluated based on their friends. In our reputation model, we add more dimensions of personal and relational attributes to derive reputation score which reflects the concept of multidimensional trust or reputation in evaluating an entity or service.

Trust in social networks can be highly dependent on density and centrality (Buskens, 1998). Trust between friends can increase or decrease based on com-

mon interest (Khambatti et al., 2004). Unlike this work, although our reputation model considers groups to evaluate a peer's reputation rank, we also consider other factors such as the amount of interactions in a particular activity. The number of common groups between two individuals may not necessary indicate a strong tie. We consider both quality and quantity of interactions in groups with common interest.

In the web context and network graphs, nodes may not necessary be human individuals as they can be web agents, crawlers, bots (Hang and Singh, 2010), routers or routing protocols (Marti et al., 2005), websites, articles, products. Trust between those agents will increase or decrease over time based on historical data. Malicious users can have negative impacts on trust models (Caverlee et al., 2008) because their misbehavior can impact their own trust as well as other nodes who are interacting with them. As a result, trust model should include methods to enhance reliability and counter malicious behaviors.

Although trust models have been used to estimate trust of an individual entity (e.g., person, machine), the concept of trust has been extended to refer to trust in an organization, not an individual person, such as companies, groups, government, clubs, and so on (Grabner-Krauter and Bitter, 2015; Granovetter, 1992). The concept of trust used for organizations is called *enterprise trust*. Granovetter (1992) define influence based on two aspects: (1) influence based on relations between individuals; and (2) influence based on social network structure. The former is more related to trust in the behavior of an individual while the latter refers to trust derived from where an entity is located in a given social network. The metrics of measuring individual trust and enterprise trust have been used differently. Individual trust is measured based on closeness, intimacy, or emotional support while enterprise trust has been estimated based on density or cohesiveness of an associated network, technology, software, system or network architectures used in an organization.

While the concept of trust is used to indicate the relationship between two entities, a more general sense of trust towards a particular entity is estimated based on opinions by multiple entities. We call it *reputation* whose concept and models of reputation are discussed as below.

4.2 Reputation Models in OSNs

Reputation is defined as general beliefs or opinions towards someone or something (Merriam and Webster Dictionary, 2015). Although the concept of reputation is overlapped with that of trust in terms of subjective perception, expectation, or belief about capability, honesty, or reliability of something or someone, it has a more aspect of objective concept than that of trust because it tends to rely on more aggregated opinions of multiple entities (Hussain and Chang, 2007).

In OSN environments, reputation is often measured based on the amount of interactions. In particular, the concept of friendship and its measurement based on various behavioral attributes are adopted in order to quantify the degree of friendship with the goal of measuring an entity's reputation (Traud et al., 2011; Hossmann et al., 2011; Nguyen et al., 2013). The example metrics of friendship are based on the types of relationships including relatives, spouse, neighborhood, friendship, work colleagues, school alumni, common interests, or hobbies (Jones et al., 2013). Reputation models using the concept of friendship have been used for various social network applications such as spam detection (Gao et al., 2012), categorization of relationships based on interactions (Akbas et al., 2013), and trust propagation based on the amount of interactions between friends.

5 CONCLUSION

In this work, we proposed a reputation model where reputation is derived from three main components: personal attributes, personal activities, and peers' reputation. In addition, we showed an application of the proposed reputation model for privacy assessment. The key idea of this reputation-based privacy model is that privacy levels for each friend or post can be automatically set based on dynamic estimation of reputation score of each friend. That is, the estimated reputation score is used to determine the visibility of any posts or activities by a user.

We plan our future work directions as: (1) investigating the circular dependency problem of reputation scores; (2) examining how to distinguish popularity obtained by high interactions with multiple friends from that by high interactions with a single friend; and (3) implementing / validating this model through empirical studies.

REFERENCES

Akbas, M. I., Avula, R. N., Bassiouni, M. A., and Turgut, D. (2013). Social network generation and friend ranking based on mobile phone data. In *Proceedings of the International Conference on Communications*, pages 1444–1448.

Buskens, V. (1998). The social structure of trust. *Social Networks*, 20(3):265–289.

Caverlee, J., Liu, L., , and Webb, S. (2008). Social trust: Tamper-resilient trust establishment in online communities. In *Proceedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL08)*, pages 104–114.

Cho, J., Swami, A., and Chen, I. (2011). A survey of trust management in mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, 13(4):562–583.

Ferlander, S. (2003). The Internet, social capital and local community. Technical report, University of Sterling.

Ganzaroli, A. (2002). Creating trust between local and global systems. Technical report, Erasmus University Rotterdam.

Gao, H., Chen, Y., Lee, K., Palsetia, D., and Choudhary, A. N. (2012). Towards online spam filtering in social networks. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

Grabner-Krauter, S. (2009). Web 2.0 social networks: The role of trust. *Journal of Business Ethics*, 90:505–522.

Grabner-Krauter, S. and Bitter, S. (2015). Trust in online social networks: A multifaceted perspective. *Forum for Social Economics*, 44(1):48–68.

Granovetter, M. (1992). Problems of explanation in economic sociology. Technical report, Harvard Business School Press, Boston, MA, USA.

Hang, W. C. and Singh, M. P. (2010). Trust based recommendation based on graph similarities.

Hardin, R. (2002). *Trust and Trustworthiness*. Russell Sage Foundation.

Hossmann, T., Legendre, F., Nomikos, G., and Spyropoulos, T. (2011). Stumbl: Using facebook to collect rich datasets for opportunistic networking research. In *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks(WOWMOM)*, pages 1–6.

Hussain, F. K. and Chang, E. (2007). An overview of the interpretations of trust and reputation. In *The Third Advanced International Conference on Telecommunications (AICT 2007)*.

Jones, J. J., Settle, J. E., Bond, R. M., Fariss, C. J., Marlow, C., and Fowler, J. H. (2013). Trust in online social networks: A multifaceted perspective. *Plos One Journal*.

Jøsang, A. and Pope, S. (2005). Semantic constraints for trust transitivity. *Proceedings of Asia-Pacific Conf. of Conceptual Modeling*, 3.

Kavanaugh, A., Reese, D. D., Carroll, J. M., and Rosson, M. (2005). Weak ties in networked communities. *The Information Society: An International Journal*, 21(2):119–131.

Khambatti, M., Dasgupta, P., and Ryu, K. D. (2004). A role-based trust model for peer-to-peer communities and dynamic coalitions. In *IEEE Information Assurance Workshop*.

Mansfield-Devine, S. (2008). Anti-social networking: Exploiting the trusting environment of web 2.0. *Network Security*, 2008(11):4–7.

Marti, S., Ganesan, P., and Garcia-Molina, H. (2005). Sprout: P2p routing with social networks. In *Current Trends in Database Technology-EDBT*. Springer Berlin Heidelberg.

Merriam and Webster Dictionary (2015). Trust and Reputation Definition.

Murphy, J. (2006). Building trust in economic space. *Progress in Human Geography*, 30(4):427–450.

Nguyen, T., Chen, M., and Szymanski, B. (2013). Analyzing the proximity and interactions of friends in communities in gowalla. In *Proceedings of IEEE 13th International Conference Data Mining Workshops*, pages 1036–1044, Dallas, Texas, USA.

Richardson, M., Agrawal, A., and Domingos, P. (2003). Trust management for the semantic web. In *Proceedings of the Second International Semantic Web Conference, Sanibel Island, Florida*.

Stallings, W. (1995). The pgp web of trust. *BYTE*, 20(2):161–162.

Traud, A. L., Mucha, P. J., and Porter, M. A. (2011). Social structure of facebook networks. *Physica A*, 391(16):4165–4180.

Woolcook, M. (2001). The place of social capital in understanding social and economic outcomes. *Canadian Journal of Policy Research*, 2(1).

Zhang, Y., Chen, H., and Wu, Z. (2006). A social network-based trust model for the semantic web. In *Proceedings of the 6th International Conference on Autonomic and Trusted Computing*, pages 183–192.