Can We Use Trust in Online Dating?

James Stanier, Stephen Naicken, Anirban Basu, Jian Li, and Ian Wakeman

School of Informatics, University of Sussex, Falmer, East Sussex, UK, BN1 9QJ.
{j.stanier, stephenn, a.basu, jl58, ianw}@sussex.ac.uk,
http://www.informatics.sussex.ac.uk/research/groups/softsys/

Abstract. We show that the application of trust models to socially emotive applications such as online dating, while beneficial, is difficult due to the complexities of the interpersonal relationships that exist. These are discussed with respect to our initial attempt to design a transitive trust model for social network dating services and existing trust taxonomies. We hope that the issues discussed motivate researchers to consider more complex social relationships in the design of trust models.

1 Introduction

Trust is important in determining if an agent should interact with another agent or system, typically in a specific context. While this property is complex and dependent on emotional factors that are difficult to formalise, formalisms of trust have been proposed that allow trust to be used in computing applications [1]. Trust formalisms and the increased threats that exist against systems and their users have given rise to a plethora of trust management systems for a variety of application areas, e.g. peer-to-peer (P2P) and marketplaces. Many are designed for interpersonal relationships, but are unsuitable for use in scenarios where these are complex, emotional, and at times, irrational.

To highlight this, in this work, online dating is considered. These services lack trust systems, but there are a number of reasons why this should not be the case. Dating sites are increasing in popularity and market value, with the U.S. market estimated to reach a value of $932m by 2011 and the number of paying European users expected to increase to 6m[1]. Typically as services grow in popularity and value, they are increasingly targeted by attackers.

There are also user-related issues to be considered. Dating services implement a matchmaking process that attempts to recommend potential partners based on their profiles, preferences and location. Yet two well matched users are still strangers and this can make initial contact difficult as little is known other than information in their profiles. The initial real life meeting can also be awkward as both users may not live up to each other's expectations or have the same personality as they assume online. Hancock et al. [2] compared 80 online daters' profile information to their actual appearance, and found 48.1% were deceptive about height, 59.7% about weight and 18.7% about age.

[1] http://industry.tekrati.com/research/news.asp?id=8487

As well as the social difficulties in conversing with a stranger, threats exist in dating applications that vary greatly in their impact. An attacker could use many false profiles to perform a Sybil attack [3] to target a given user or type of user, resulting in well-behaved users perceiving these profiles as genuine and trustworthy. This allows the attacker to engage in malicious behaviour against users, and more damagingly, to build trust with them only to breach this later.

These issues show that trust models are required in online dating applications. The aim of this work was to implement a trust model for use in dating services that made use of the transitive trust in social networks. The motivation for this was that it is common in real life to meet potential partners through a degree of separation from an existing friend. This has a number of benefits. Firstly, the two parties are introduced by a mutually trusted friend which reduces embarrassment and increases legitimacy. Secondly, by being introduced, it is likely that the two parties share some common interests with the friend and in turn each other. Lastly, compared to existing dating services, the use of a social network provides a better foundation for matchmaking as it models real life social interaction. However, it soon became evident that dating gives rise to issues that have not been addressed by prior trust models.

In this paper, we broadly look at existing trust models, their applications and taxonomy. This is followed by the initial design of a facilitated approach to dating that assumes the presence of a dating service that overlays an existing social network. The approach makes use of the friend-of-a-friend (FOAF) concept in the social graph to match users. Finally, it is shown why this does not work, and a discussion of the issues in modelling trust in such applications is given.

2 Trust models

Trust models have been successfully applied to areas such as Internet shopping [4] and P2P networks [5]. Their aim is to improve reliability and performance of systems by modelling the trustworthiness of agents. At its simplest, trust is a function of behaviour, with behavioural history allowing the trustworthiness of an agent to be determined. Good behaviour increases trust and bad decreases it. Once the trustworthiness of an agent has been ascertained, others may decide if they wish to interact with it.

A taxonomy of trust has been presented [6] which identifies the components of P2P reputation systems and their mechanisms. These are: *a*) *Information gathering:* Identity scheme, information sources, information aggregation and stranger policy. *b*) *Scoring and ranking:* Good vs. bad behaviour, quantity vs. quality, time-dependence, selection threshold and peer selection. *c*) *Response:* Incentives and punishment.

This taxonomy is applicable to trust in other applications. For example, in an online shopping scenario, information gathering criteria are easily accessible, as each seller is publicly visible for a buyer to interact with. Scoring and ranking criteria can be fulfilled with both customer and critic reviews of that seller, along with the prices that are being offered for particular items in comparison

with their peers. The response criteria are also apparent: succeeding in being a trustworthy seller brings more customers and profit as a result, whereas repeated punishment will drive customers away. However, there are applications where trust models would be invaluable, but are difficult to implement. Analysing these applications with respect to the taxonomy raises a number of issues. In the rest of this paper, online dating is shown to be one such application.

3 Facilitated approach to dating

In this section, a facilitated approach to online dating is presented that seeks to simulate FOAF style introductions. If a user is interested in another, the intermediate friends between them may act as a path of facilitators that decide if the two are a suitable match.

Assuming that the user, *Alice*, wants to date *Bob*, a number of different routes may exist in the social network between them. The algorithms attempt to rank these simple path routes on on the pair-wise trust between users on the path and facilitation rankings. This helps *Alice* choose the best path to contact *Bob* without knowing any explicit detail about the intermediate friends.

3.1 Computed factors

First, *Alice* is presented with ranked simple paths to *Bob*. The rank function is of the degrees of separation between the two parties, the path trust and facilitation value.

Path trust: We assume the presence of a social network, modelled as a directed weighted graph $G = (V, E, w)$ where V is the set of all users, E the set of all edges connecting users (i.e. relationships) and w, a weight function, $w : E \rightarrow \mathbb{R}_+\{0, 1\}$, representing the trust that a source of a given edge has in the destination. While we make no assumption as to how this trust value is derived, one proposal is to build upon the work of Gill [7, 8], which shows that trust, personality and emotion can be perceived from short texts, e.g. status updates and wall posts.

Facilitator ranking: The trust values capture pairwise trust between individuals but do not measure their ability to act as facilitators in a matchmaking process. So, we assume a value, ω_v, that gives a $\mathbb{R}_+\{0, 1\}$ reputation value based on prior paticipations in matchmaking processes – the facilitation value of v.

The aim was to harness the transitive trust relationships that exist in the social network to facilitate matchmaking. The first process to achieve this is to propose a set of k-most trusted paths from *Alice* to *Bob*. *Alice*, presented with these k-paths, chooses one to be used in the matchmaking process. Her choice will be dependent not only on the trust value of the paths, but also personal variables that cannot be captured by the system, for example, she may decide not to choose the most trusted path if one of the users on it is an individual whom she

dislikes. The problem of finding the most trusted path has been addressed in P2P networks [9]. However, given the additional facilitation variable, we choose a more sophisticated approach by modifying the semiring-based trust model presented by Theodorakopoulos and Baras [10] so that the chosen k-most trusted paths are defined by a function over the pairwise trust values and the facilitation value of each intermediate vertex on the path. Due to space constraints we omit the mathematical preliminaries and details of this, opting instead to only present the facilitation model.

3.2 Path traversal and recommendations

Path reduction: We consider the three possibilities for a path chosen by *Alice*. Let the path chosen by Alice be $P = \{p_0, \ldots, p_n\}$ where each $p_k \in P$ is a person at k degrees of separation, with $p_n = Bob$ and $p_0 = Alice$. We observe that *Bob* could be at:

1. one degree of separation, i.e. $Alice \rightarrow Bob$. Here we assume *Alice* requires a facilitator, perhaps due to shyness as friendship already exists with Bob, so this becomes two degrees of separation, see 2.
2. two degrees of separation, i.e. $Alice \rightarrow p_1 \rightarrow Bob$ where p_1 is the common friend of both *Alice* and *Bob* to act as a single facilitator.
3. three degrees of separation, i.e. $Alice \rightarrow p_1 \rightarrow p_2 \rightarrow Bob$ where p_1 is a friend of *Alice* only; p_2 is a friend of *Bob* only. There is no single facilitator but p_1 and p_2 together (who are friends) act as facilitators.
4. more than three degrees of separation, i.e. $Alice \rightarrow p_1 \rightarrow p_2 \ldots p_{n-2} \rightarrow p_{n-1} \rightarrow Bob$ where p_1 is a friend of *Alice* only; p_{n-1} is a friend of *Bob* only. There is no single facilitator but p_1 and p_{n-1} together act as facilitators. However, the path $P^{'} = \{p_2, \ldots, p_{n-2}\}$ consists of persons who do not know *Alice* or *Bob*.

All intermediate persons in the path $P^{'}$ cannot directly be part of the facilitation process because of their lack of first-hand knowledge of both *Alice* and *Bob*. A path reduction algorithm through chain introductions can reduce the degree of separation to three, e.g. with an initial path $Alice \rightarrow p_1 \rightarrow p_2 \rightarrow p_3 \ldots p_{n-3} \rightarrow p_{n-2} \rightarrow p_{n-1} \rightarrow Bob$ the objective is to reduce this to $Alice \rightarrow p_1 \rightarrow p_{n-1} \rightarrow Bob$. To achieve this p_1 asks p_2 for an introduction to p_3. If p_2 honours this request, p_1 and p_3 are connected and p_1 asks p_3 for introduction to p_4 and so on with the path eventually becoming $Alice \rightarrow p_1 \rightarrow p_{n-1} \rightarrow Bob$.

From a social interaction perspective, the paths $Alice \rightarrow p_1 \rightarrow p_2 \rightarrow Bob$ and $Alice \rightarrow p_1 \rightarrow p_{n-1} \rightarrow Bob$ are different. In the former, p_1 and p_2 are friends, but in the latter, p_1 and p_{n-1} are introduced to one another for the sake of *Alice*'s interest to date *Bob* without knowing each other. Any intermediate person p_k has very little reason to co-operate other than altruism, although incentives may help to increase cooperation. A p_k has little reason to honour the request from p_1 to connect to p_{k+1} as p_k does not really know p_1. Therefore, we do not consider paths longer than three degrees.

Facilitation: This process depends on the degrees of separation between *Alice* and *Bob*. We enumerate the process in algorithm 3.2.1 for the different path lengths.

Algorithm 3.2.1 Facilitation algorithm

1: *Alice* picks a path, based on path ranking: $P = \{p_0, \ldots, p_n\}$ through the graph where each $p_k \in P$ is a person at k degrees of separation from $p_0 = Alice$.
2: If $p_n = Bob$ is at more than three degrees of separation from $p_0 = Alice$ then the path is unusable for aforementioned reasons.
3: If $p_n = Bob = p_2$ is at two degrees of separation from $p_0 = Alice$ then the sole facilitator, p_1, is notified of *Alice*'s desire to date *Bob*. p_1 is also presented with *Alice*'s and *Bob*'s "about me" and "looking for" criteria, and determines if *Alice*'s and *Bob*'s photographs and profile information are honest and up-to-date; and also if the couple match according to their specified criteria as well as p_1's knowledge of *Alice* and *Bob*. Given a match, p_1 initiates the revelation process in algorithm 3.2.2.
4: If $p_n = Bob = p_3$ is at three degrees of separation from $p_0 = Alice$ then *Alice*'s facilitator, p_1, is notified of *Alice*'s desire to date *Bob*. p_1 is presented with *Alice*'s "about me" and "looking for" criteria, and determines if *Alice*'s photographs and profile information is honest and up-to-date.
5: Similarly, *Bob*'s facilitator, p_2, is notified by p_1 of *Alice*'s interest and a similar process is applied on *Bob*'s information by p_2.
6: p_1 and p_2 (who are friends) communicate with each other to determine whether the couple match according to their specified criteria as well as p_1's knowledge of *Alice* and p_2's knowledge of *Bob*. Given a match, p_1 and p_2 initiate the revelation process described in algorithm 3.2.2.

In algorithm 3.2.1, either the single facilitator p_1 or the pair of facilitators p_1 and p_2 can refuse to facilitate, which is fed back to the initiator *Alice* who is then required to choose a different path or abandon the process.

Revelation: In order to protect identity, the revealing process, described in algorithm 3.2.2, is tackled in a number of stages.

4 Why trust does not work

To illustrate the issues that must be considered in the design of trust models for emotional applications, the model presented in this paper and current online dating systems are examined with respect to the trust taxonomy in section 2 [6]. These issues are primarily due to the complexities of relationships and are unaddressed by existing models and difficult to resolve.

Information gathering: Collecting the required information for trust systems poses a number of difficulties. Identities must be associated with historical behaviour, so they must be sufficiently persistent, spoof-resistant, unforgeable and where necessary, offer a degree of anonymity. While the latter is not an issue

Algorithm 3.2.2 Revelation algorithm

1: *Bob* is notified that somebody wishes to date him. He is given the ranking along with the recommendations that have been produced by immediate facilitator, p_2 or by the single facilitator p_1 depending on the degree of separation between *Alice* and *Bob*. If *Bob* does not wish to continue, he can cancel the matchmaking attempt with a written decision which is fed back to *Alice*.
2: If *Bob* wishes to continue, he is presented with the information that *Alice* made available to the matchmaking process, such as photographs and profile information. He is not given her name at this point. Since the photographs *Alice* selected are not publicly visible nor are they *Alice*'s profile photographs, this minimises the chance of him finding her accidentally in search.
3: If *Bob* still wishes to continue then the identities of both parties are revealed to each other by their immediate facilitators or by the single facilitator depending on the path length. From this point, they could add each other as friends on the social network (unless they already are friends) and message each other directly.
4: The dating process is then taken offline. Based on how the two parties get on, they are encouraged to rate how accurate the recommendation process was. This feeds into the facilitator ranking to use in future path computation.

as there is no need to hide the association between behaviour and identity, the others give rise to concerns.

Persistence and spoof-resistance can be ensured when a centralised server is used for managing identity, as is the case for all existing dating services. For the model presented in this work, this is also assumed to be true as existing social network services use centralised identity management. Unforgable identities are somewhat harder to ensure. As mentioned above, free dating services are susceptible to Sybil attacks [3], but those using a subscription business model lower their vulnerability as identity has a cost. Credit-card verification is an alternative way to prevent this and also ensure that minors can not use the system.

Even where persistence can be guaranteed, there will be churn in the user base of dating services. Users leave the service after finding a partner or because of negative experiences. Their feedback is important to those remaining in the system, but must decay in importance with time. By implementing the dating service as an application of an existing social network, users remain in the system even after having found a match as they continue to engage in other activities and can participate in facilitation.

Misleading identities must also be considered. *Alice* may lie in her profile so that her chosen target user is more receptive to her request for a date. While the facilitation model attempts to handle this by having the facilitators verify profile information, *Alice* and her next-hop friend may collude to defeat this.

Obtaining information to be used by a trust model is generally not an issue, as the data is available from users or the application. In P2P file sharing, users provide feedback on the quality of file download transactions. Models such as Eigentrust [11] provide no incentive for this, with users assumed to be altruistic with feedback.

Assuming such altruistic feedback behaviour in dating applications is naive. *Alice*, who has had a positive date with *Bob* has no incentive to provide good feedback on *Bob*, but disincentives. If *Bob*'s trustworthiness is public, rivals may emerge. *Alice* may decide to provide less favourable feedback, or as *Bob* faces the same dilemma, collude with him so that both do not provide any. The issue is clear, in marketplaces to which trust is typically applied, *Alice*'s and *Bob*'s goods are not limited in availability, so less competition exists for them. Here, each user's affections is a unique, scarce product, typically only available to one consumer, so a potential consumer is unlikely to recommend rivals to the seller.

In the facilitation model, *Bob* may not wish to rate p_{n-1} as a poor facilitator given that they are friends. Due to this conflict of interest, *Bob* may opt to not participate in the feedback process. Although the context is distinct to others in the relationship, due to emotional reasons, *Bob* may fear that p_{n-1} will mix them and damage their relationship.

By utilising a social network, the stranger policy is not an issue for the facilitation model, but is for standalone online dating services where a trust system exists. For the latter, users may opt to not interact with a new user, however it would be interesting to see to what extent this applies to attractive new users following on from the "what is beautiful is good" stereotype [12]. How less attractive new users are induced into the service is unclear.

Scoring and ranking: The only source of information available to the trust model is from users, those wishing to find partners and in the facilitation model, the facilitators too. Some reasons as to why they may choose to participate maliciously or not at all have been discussed above. Here, the focus is on the reasons as to why inconsistencies may exist in the users' feedback.

Inconsistent feedback is not unique to dating, examples can also be found in other applications, e.g. marketplaces. A buyer can rate two sellers differently, despite both transactions being successful, as its expectations of each differed greatly. Ratings may also be prejudiced for other reasons including personal beliefs. In social applications such as dating, inconsistencies are a complex problem that can only be addressed by understanding the nature of human trust, particularly the reasons why some are more trusting of others when forming relationships.

To understand the reasons behind these social science issues, a number of research papers were surveyed, with a some important observations made. Many people have differing relationship commitment levels and ethics, which highlights the call for a trust model to account for an individuals needs and desires from a relationship in the matchmaking process.

Many psychological factors can decrease an individual's ability to form trust with others, e.g. parental divorce. In addition, negative events between dating partners will have greater effect on anxious-ambivalent people [13]. The model must ensure that those who receive low feedback from those who have inhibiting psychological traits are not deemed to be bad users initially, as the nature of the individual providing the feedback should also be considered. However, acquiring it from users and modelling this information is a difficult task.

Response: Trust models depend on incentives and punishment to ensure cooperation from users, but for dating, this is complex. Punishing a user for being negative at a date may seem apt, but if he feels misled, he may be justified. Punishing facilitators raises issues, as they may have been misled about an individual or may have felt pressured into making the match.

For the facilitation model, by imposing a non-punishing time-out facility which could pass responsibility to another user if one is not active, malicious users could refuse to take part while keeping their trust rating. Users could maliciously block introductions or rate the validity of friend's data badly without them knowing. After meeting up, parties could give malicious feedback ratings which in turn affects their perception from future potential interests.

5 Conclusion

We see this paper as a call to arms for researchers to explore developing trust models for applications that have intricate human and ethical factors. Often, these difficult applications are the ones that would benefit the most from them.

References

1. Marsh, S.P.: Formalising trust as a computational concept. PhD thesis, University of Stirling (1994)
2. Hancock, J.T., Toma, C., Ellison, N.: The truth about lying in online dating profiles. In: Proc. CHI, ACM (2007) 449–452
3. Douceur, J.: The Sybil Attack. Proc. IPTPS (2002) 251–260
4. Lee, M.K.O., Turban, E.: A trust model for consumer internet shopping. Int. J. Electron. Commerce **6**(1) (2001) 75–91
5. Wang, Y., Vassileva, J.: Trust and reputation model in peer-to-peer networks. In: Proc. P2P, Washington, DC, USA, IEEE Computer Society (2003) 150
6. Marti, S., Garcia-Molina, H.: Taxonomy of trust: categorizing P2P reputation systems. Comput. Netw. **50**(4) (2006) 472–484
7. Scissors, L.E., Gill, A.J., Gergle, D.: Linguistic mimicry and trust in text-based CMC. In: Proc. CSCW, ACM (2008) 277–280
8. Gill, A.J., Gergle, D., French, R.M., Oberlander, J.: Emotion rating from short blog texts. In: Proc. CHI, ACM (2008) 1121–1124
9. Marti, S., Ganesan, P., Garcia-Molina, H.: SPROUT: P2P Routing with Social Networks. In: Proc. P2P&DB. (March 2004)
10. Theodorakopoulos, G., Baras, J.S.: On trust models and trust evaluation metrics for ad hoc networks. IEEE J. Selected Areas in Communications **24**(2) (2006) 318–328
11. Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In: Proc. WWW, ACM (2003) 640–651
12. Dion, K., Berscheid, E., Walster, E.: What is beautiful is good. J. Personality and Social Psychology **24**(3) (December 1972) 285–290
13. Simpson, J., Ickes, W., Grich, J.: When accuracy hurts: Reactions of anxious-ambivalent dating partners to a relationship-threatening situation. Journal of Personality and Social Psychology **76**(5) (1999) 754–769