Can We Use Trust in Online Dating?

James Stanier, Stephen Naicken, Anirban Basu, Jian Li and Ian Wakeman
University of Sussex
Brighton, UK
{*j.stanier, stephenn, a.basu, jl58, ianw*}*@sussex.ac.uk*

Abstract

Trust models have been used widely in the literature in a number of different contexts. We examine an emotive scenario where trust would be extremely useful: online dating. We explore the use of a semiring-based trust model with online dating in a social network. Introductions are facilitated by friend-of-a-friend connections in the network in a manner similar to some real world scenarios. We show how ethical and human factors, which are usually not considered, cause problems. We hope that as a result the trust community can work together to formulate new approaches to trust for emotive applications that accommodate ethical and human factors which are difficult to quantify.

1 Introduction

The notion of trust is an important property in determining if an agent should interact with another agent or system, typically in a specific context. While this property is complex, dependent on emotional factors that may be difficult to quantify, formalisms of trust have been proposed in order to allow for it to be used in computing applications, with Marsh's formalism [15] being widely used and cited in the literature. The formalism of trust, along with the increased threats that exist against systems and agents participating within those systems, has given rise to a plethora of trust models and trust management systems for a variety of application areas, e.g. peer-to-peer routing and transactions, online auctions, and recommender systems. Many of these trust systems and models are designed for interpersonal trust relationships. However, they are unsuitable for use in application scenarios where these relationships are complex, emotional and at times, irrational.

As an example we use online dating: a notoriously tricky business. In general, individuals create a profile on a dating website and then write about themselves and what they are looking for, upload some self-portrait photographs and answer some mandatory matching questions. Most dating websites implement a matchmaking process that attempts to recommend potential suitable users based on a user's preferences, characteristics and location. However, regardless of whether two people are highly matched according to a particular algorithm, these two people are still strangers. This can make initial online conversation difficult as the two parties know little of each other apart from what is presented in their profiles. Additionally, it makes the initial real life meeting uncomfortable as both parties may not live up to each other's expectations or have the same personality as they assume online.

As well as the social difficulties in communicating with a stranger, there are threats that exist in dating applications that vary greatly in their severity. For example, a malicious user is able to create one or many false profiles, particularly on free dating services, that can be used to potentially attack or harass users by engaging in inappropriate behaviour with them, or perhaps more damagingly, building trust with users through communication only to breach this trust later. Creating false profiles is especially easy since dating sites do not verify the authenticity of profile text and photographs.

While multiple malicious profiles are not necessary to implement the misbehaviour described above, as only one malicious user account is necessary where no trust or feedback system exists, multiple identities allow for more complex attacks. An attacker may make use of its many false profiles to target more of the user criteria space by generating a diverse set of profiles. Alternatively a targeted attack

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 1, number: 4, pp. 50-61

against a particular user or type of user can be performed by generating many similar profiles. Finally, the attacker can use many identities to perform a Sybil attack [5] should a trust model be implemented in a dating service. The latter results in well-behaved users perceiving the malicious profiles as genuine and trustworthy. The consequences of such attacks to the service provider can be significant in terms of quality of service, reputation and profit. While for the end user, their emotional well-being and trust in others when attempting to form relationships may be jeopardised, particularly so if the attack is coordinated against a single specific target.

To address these issues described above and others, the original aim of this work was to implement a trust model for use in dating applications that made use of the transitive trust relationships that exist in social networks. The motivation for this was based on the fact 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 which both reduces embarrassment and increases legitimacy in the meeting since they are both being facilitated by an existing friend who they trust. Secondly, by being introduced through a friend it is likely that the two parties already have something in common with each other as an intersection of the interests of themselves and the friend. Thirdly, compared to online dating communities that serve a sole purpose of match making, a social network provides a better foundation for modelling real life social interaction.

However, it soon became evident that this approach gives rise to issues that have not been addressed by previous trust models and are quite complex to solve. Application of techniques to develop such models and also use of existing models did not overcome the issues we found.

In this paper we broadly look at existing trust models, their applications and their taxonomy. We then present our attempt to use a decentralised trust approach to online dating by overlaying a dating service on an existing social network in order to utilise the social graph, where users can use the friend-of-a-friend (FOAF) links to seek recommendations to contact a potential date. We show why this does not work, and hence show that existing approaches to trust lack the ability to model complex human behaviour and fail to consider ethical issues.

2 Trust models

Trust models have been successfully applied in many situations such as Internet shopping [13], peer-to-peer (P2P) networks [23], and to distributed online entities [1]. In each scenario, the model seeks to improve the reliability of a given service by modelling the trustworthiness of agents, whether they are nodes in a network or online shops. By rewarding good behaviour and punishing bad behaviour over time, a general picture arises of how much an agent is trusted, which allows users to receive a better quality service.

A taxonomy of trust models has been presented [17] which categorizes system components in P2P reputation systems. In these reputation systems, the authors present three broad components of a trust model:

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 easily applicable to existing trust model applications. For example, in an online shopping situation, 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, yet solutions do not currently exist. This is because applying the criteria of the taxonomy is difficult in that application. In this paper, we use online dating as an example of a situation where existing trust models do not work.

3 A background to online dating

Online dating has become incredibly popular. A 2006 survey showed that nearly 7 million American adults have gone on a date with someone they met through a dating website [14], and in December 2008, on average, there were around 22.1 million unique visitors to dating sites [18]. Subscription-based dating websites are a lucrative business. The US online dating market is forecast to reach $932 million in 2011 with the European online dating market increasing from 2.8 million paid users to 6.0 million paid users [21].

In general, most dating sites allow a user to create a publicly visible profile which contains the user's statistics, personality traits and interests; what they are looking for in a potential partner; optional photographs and some free-text areas where they write whatever they choose. Then, the website uses a matchmaking algorithm to present users with others that are compatible based on the information they have entered. The user can then choose to contact a potential match with a message. If the two parties decide to, they can exchange actual email addresses or phone numbers once an initial contact has been made.

In the literature a number of issues have been raised highlighting problems with current online dating systems. Firstly there are inhibiting factors that prevent users from signing up in the first place. A study of Canadian daters [3] states that users would want to see a potential date in real life before actually dating them, along with the fact that they feel they cannot trust online dating users. A small percentage of people found embarrassment a major factor inhibiting usage.

Truthfulness is a recurring theme in the literature. Hancock et al. [10] compared 80 online daters' profile information to their real life appearance, and found 48.1% were deceptive about height, 59.7% about weight and 18.7% about age. Ellison et al. [7] interviewed 34 online daters about their self-presentation online, and found that some described an "ideal self" and a "potential future version" of the self rather than their actual personality.

The ratio of men to women has always been a contentious topic, as many dating websites do not want to disclose this information. The Canadian survey measured a ratio of 2 men for every 1 woman, whereas for Internet use in general, men only outnumber women by 7% [3]. This aspect, combined with the fact that men are the most likely to initiate contact, results in an overwhelming number of messages for "popular" female users. As these women receive a large amount of mail, men may find the experience dejecting after having many messages ignored. A study [8] showed that men contacted by women replied 26.4% of the time, and women contacted by men replied just 15.9% of the time. In extreme cases, mail may not be read at all. Plentyoffish.com[1] states that 0.1% of users receive more messages in 24 hours than their inbox can hold (currently 100 messages) in which case the website begins to delete them before they can be read. Free dating websites suffer heavily from this problem, especially for very attractive users.

Online daters may also feel that they invest too much in each person online before meeting. Parties may contact each other via messages for a long period of time before agreeing to meet in person. This

[1] http://www.plentyoffish.com/

already establishes an emotional connection between the users' online personas which may be very different to the actual chemistry felt between them in real life. The solution is to "take things offline" as quickly as possible, but since the two parties are strangers, it may take some time until they trust each other enough to do so.

Recently, services such as Zoosk[2] have been offering a dating service integrated with Facebook. Users can use one of these applications to be able to search other application users within their local area. However, aside from seeing which Facebook friends currently use the application, this approach is not far removed from traditional dating websites, where both users have no connection before the initial contact. We wanted to try and use the potential of a social network and the friendship relationships within in order to drive our FOAF approach to online dating.

4 Facilitated approach to dating

In this section, a facilitated approach to online dating is presented, based on existing trust systems, that seeks to simulate FOAF style introductions. If a user is interested in another, the intermediate friends between them can 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.

4.1 Computed factors

First, *Alice* is presented with a ranked simple paths to *Bob*. Ranking is a function 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, $w : E \to \mathbb{R}_+\{0,1\}$, 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 [20, 9], which shows that trust, personality and emotion can be perceived from short texts, e.g. status updates and wall posts. A simpler alternative that is implemented in Orkut[3], is to allow users of the social network the ability to specify the level of friendship with a friend.

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 participation 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*. This could perhaps be implemented by applying modifications to Yen's k-shortest path algorithm [24]. Presented with these k-paths, *Alice* 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

[2] `http://www.zoosk.com/`
[3] `http://www.orkut.com`

users on it is an individual whom she dislikes. The problem of finding the most trusted path has been addressed in P2P networks [16]. However, given the additional facilitation variable, we choose a more sophisticated approach by modifying the semiring-based trust model presented by Theodorakopoulos and Baras [22] 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.

$$(w(i,j),\omega_j)\otimes(w(j,k),\omega_k)=(w(i,j)w(j,k),\omega_j\omega_k) \tag{1}$$

$$(w_{ik}^{P1},\omega^{P1})\oplus(w_{ik}^{P2},\omega^{P2})=\begin{cases}(w_{ik}^{P1},\omega^{P1}), & \text{if } \omega^{P1}>\omega^{P2}\\ (w_{ik}^{P2},\omega^{P2}), & \text{if } \omega^{P1}<\omega^{P2}\\ (w_{ik}^{*},\omega^{P1}), & \text{if } \omega^{P1}=\omega^{P2}\end{cases} \tag{2}$$

$$(w_{ik}^{P1},\omega^{P1})\oplus(w_{ik}^{P2},\omega^{P2})=\begin{cases}(w_{ik}^{P1},\omega^{P1}), & \text{if } \alpha w_{ij}^{P1}+\beta\omega^{P1}>\alpha w_{ij}^{P2}+\beta\omega^{P2}\\ (w_{ik}^{P2},\omega^{P2}), & \text{if } \alpha w_{ij}^{P1}+\beta\omega^{P1}<\alpha w_{ij}^{P2}+\beta\omega^{P2}\\ (w_{ik}^{*},\omega^{*}), & \text{if } \alpha w_{ij}^{P1}+\beta\omega^{P1}=\alpha w_{ij}^{P2}+\beta\omega^{P2}\end{cases} \tag{3}$$

where $P1$ is a simple path from vertices i to k in G, $P2$ is a different simple path from i to k in G, $w_{ik}^{*}=max(w_{ik}^{P1},w_{ik}^{P2}),\omega^{*}$ is the facilitator value of the path chosen for w_{ik}^{*}, $\alpha,\beta\in\mathbb{R}_{+}\{0,1\}$ and $\alpha+\beta=1$.

Equation 1 defines a means to determine the rating of a simple path from i to k. The rating is a pair of the product of trust values between adjacent vertices on the path and the product of facilitator values of each node on the path. This approach is based on Theodorakopoulos and Baras's path ranking semiring. This is by no means definitive and other models to determining the trust of a path may be used.

To compare paths, two models are proposed in equations 2 and 3 respectively. Equation 2 determines the ranking of paths using the facilitator value and uses trust values only to split ties. The alternative, equation 3, requires two tunable values α and β to determine the importance of the trust and facilitator values to the ranking respectively. As with the evaluation of the path, other models may also be used.

Upon the termination of the algorithm implementing these equations, Alice is presented with a ranked set of k-simple paths to Bob. She is now in a position to select a path given her own personal criteria and for the next step, the recommendation algorithms, to begin.

4.2 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.

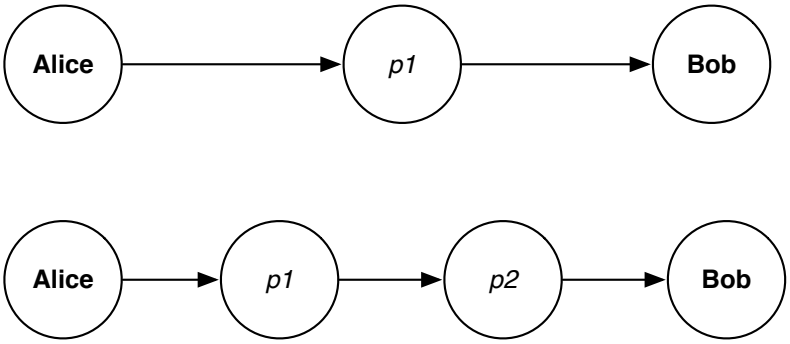

Figure 1: Degrees of seperation between Alice and Bob that are utilized in the facilitation algorithm.

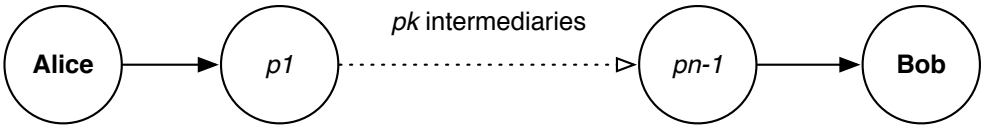

Figure 2: Degrees of separation which are too long to be considered for the algorithm. The p_k intermediaties do not know Alice and Bob in the social network.

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 $Alice \rightarrow p_1 \rightarrow p_{n-1} \rightarrow Bob$ (Figure 1).

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 (Figure 2).

Facilitation: This process depends on the degrees of separation between *Alice* and *Bob*. We enumerate the process in algorithm 1 for the different path lengths.

In algorithm 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. A visual representation of this algorithm for three degrees of separation is given in Figure 3.

Algorithm 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, and *Alice* must choose another.
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 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 are 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 2.

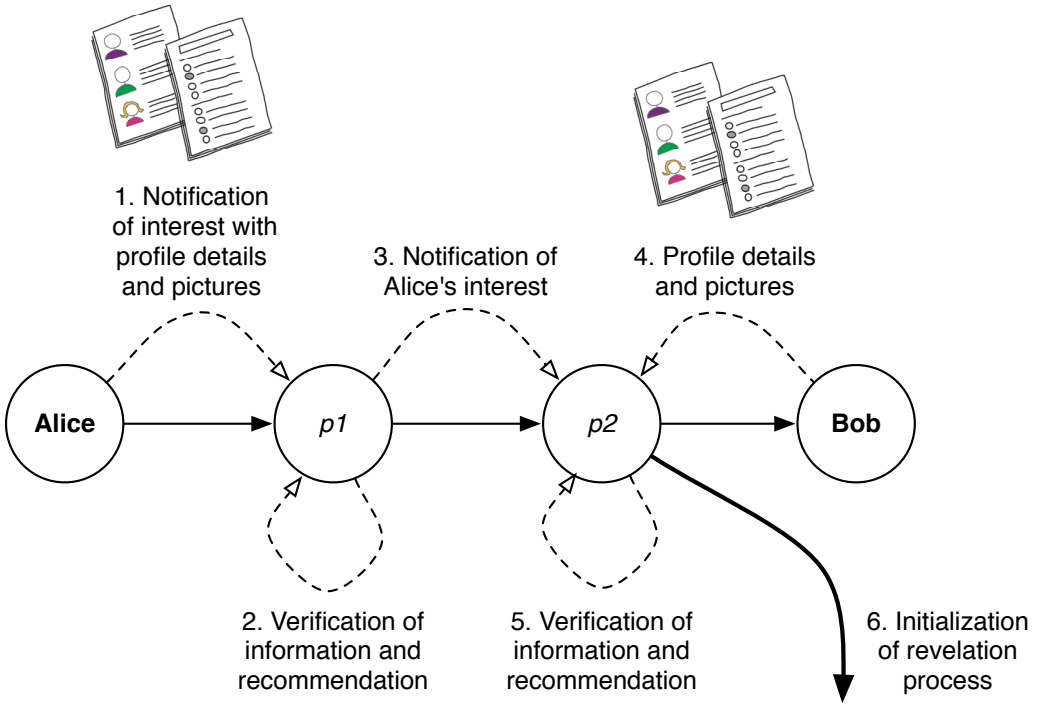

Figure 3: Visual representation of the facilitation algorithm for three degrees of separation.

Revelation: In order to protect identity, the revelation process, described in algorithm2, is tackled in a number of stages. A visual representation of this algorithm for 3 degrees of separation is also given in Figure 4. Unfortunately, in practice, this facilitated approach does not work. The fact it does not work highlights a number of problems with the use of trust in certain contexts.

Algorithm 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, having both now agreed to being interested in each other.
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.

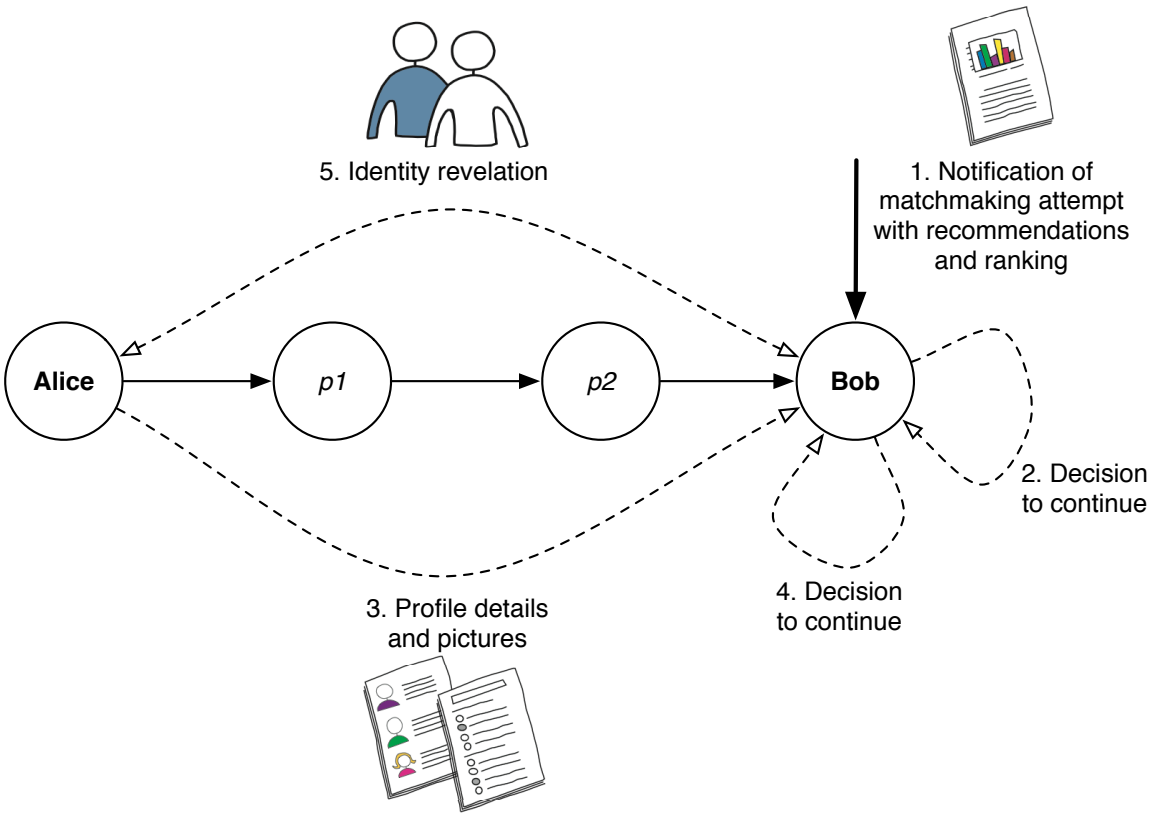

Figure 4: Visual representation of the revelation algorithm for three degrees of separation.

5 Why trust does not work

In order to show why traditional trust models do not work for "introduced by a friend" online dating, we review our model against the taxonomy of trust models [17] and also explore the human and ethical factors which affect the process.

5.1 Taxonomy comparison

The first category of the taxonomy is *information gathering*. Since daters provide their own information for their profiles, this data cannot be assumed to be true: people may lie or be deceitful. We attempted to overcome this problem by having facilitators verify this data, but there is a high chance of collusion between the facilitators and the owners of the data as they are friends, resulting in a chance of false validity ratings.

The second is *scoring and ranking*. Since transactions between users are long-lived (e.g. dating takes place over a long period of time) the relationships in the system are subject to change. This differs greatly from existing trust systems in the literature where transactions are short-lived (e.g. purchasing a product or downloading a file). Time-dependence is also an issue. If we imagine an acceptable turnaround time for any user in the path is a few days, for longer paths a communication attempt could take over a week, and then still fail. Additionally, the proposed system lacks any incentive to take part, especially in the case of the intermediate users. Different people or cultures may require a solid incentive, whereas others may have more altruistic behavior.

This leads into the third category, *response*. 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 yet not lose their trust rating. Users can also maliciously block introductions which wastes time or rate the validity of friend's data badly without them knowing. For example, in our example, another female user could prevent Alice's attempt to connect with Bob as she might also be interested in him! Additionally, after meeting up, parties can give malicious feedback ratings which in turn affects their perception from future potential interests.

5.2 Human and ethical factors

A number of human and ethical factors also contribute to the difficulty of modelling trust in online dating. Abdul-Rahman and Hailes state [2] that trust models for virtual applications are "largely impractical and artificial" and propose a new model based on word-of-mouth. However, for dating, we posit that good feedback from daters is a rare occurrence: if a date goes well it is likely the parties will stop using the service! Also, negative feedback could be used maliciously if one party feels disappointed or let down by a real life experience. This also contrasts with Resnick et al. [19] where the authors state that a critical property of a reputation is that "entities are long-lived, so there is an expectation of future interaction". In online dating, a bad experience can result in parties never interacting again. Good experiences result in the parties ultimately leaving the dating site.

Other sociological factors make trust difficult for dating. For example, Dion et al. [4] showed evidence of a "what is beautiful is good" stereotype, where people were more trusting of sexually attractive people. This effect may make a dater's trust less important to an unknown party. Drigotas et al. [6] highlight that low early relationship commitment level predicts later infidelity, which highlights the need for a dating trust model to account for an individuals commitment and need in the matchmaking process. Each individual dater's real-world trust may not correlate to a prediction in the model. For example, many psychological factors can decrease an individual's trust in others, such as parental divorce [11].

One important ethical issue is the risk of developing and testing trust models for dating. Lawson and Leck [12] state that some risks of online dating include "physical danger" and "loss of face and possible rejection". These are considerably higher stakes than are faced in other applications such as online shopping, raising the question of how is best ethically to develop and test trust in situations that involve emotional and physical risk.

6 Further work

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, such as online dating. Often, these difficult applications are the ones that would benefit most from them. How can we make trust work in these scenarios?

References

[1] A. Abdul-Rahman and S. Hailes. A distributed trust model. In *Proc. NSPW*, pages 48–60, New York, NY, USA, 1997. ACM.

[2] A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities. In *Proc. HICSS 33*, volume 6, pages 1–25, 2000.

[3] R. J. Brym and R. L. Lenton. Love Online: A Report on Digital Dating in Canada, 2001.

[4] K. Dion, E. Berscheid, and E. Walster. What is beautiful is good. *J. Personality and Social Psychology*, 24(3):285–290, December 1972.

[5] J Douceur. The Sybil Attack. *Proc. IPTPS*, pages 251–260, 2002.

[6] S.M. Drigotas, C.A. Safstrom, and T. Gentilia. An investment model prediction of dating infidelity. *J. Personality and Social Psychology*, 77:509–524, 1999.

[7] N. Ellison, R. Heino, and J. Gibbs. Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment. *J. Computer-Mediated Communication*, 11(2), 2006.

[8] A. T. Fiore, L. Shaw Taylor, X. Zhong, G. A. Mendelsohn, and C. Cheshire. Who's right and who writes: People, profiles, contacts, and replies in online dating. In *Proc. HICSS 43*, 2010.

[9] A. J. Gill, D. Gergle, R. M. French, and J. Oberlander. Emotion rating from short blog texts. In *Proc. CHI*, pages 1121–1124. ACM, 2008.

[10] J. T. Hancock, C. Toma, and N. Ellison. The truth about lying in online dating profiles. In *Proc. CHI*, pages 449–452. ACM, 2007.

[11] V. King. Parental divorce and interpersonal trust in adult offspring. *J. Marriage and the Family*, 64(3):642–656, 2002.

[12] H.M. Lawson and K. Leck. Dynamics of internet dating. *Social Science Computer Review*, 24(2):189, 2006.

[13] M. K. O. Lee and E. Turban. A trust model for consumer internet shopping. *Int. J. Electron. Commerce*, 6(1):75–91, 2001.

[14] M. Madden and A. Lenhart. Online Dating. Pew Internet and American Life Project. http://www.pewinternet.org/Reports/2006/Online-Dating.aspx, 2006.

[15] S. P. Marsh. *Formalising trust as a computational concept*. PhD thesis, University of Stirling, 1994.

[16] S. Marti, P. Ganesan, and H. Garcia-Molina. SPROUT: P2P Routing with Social Networks. In *Proc. P2P&DB*, March 2004.

[17] S. Marti and H. Garcia-Molina. Taxonomy of trust: categorizing P2P reputation systems. *Comput. Netw.*, 50(4):472–484, 2006.

[18] PCWorld. Online Dating: Analyzing the Algorithms of Attraction. http://www.pcworld.com/article/159884/, 2009.

[19] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman. Reputation systems. *Commun. ACM*, 43(12):45–48, 2000.

[20] L. E. Scissors, A. J. Gill, and D. Gergle. Linguistic mimicry and trust in text-based CMC. In *Proc. CSCW*, pages 277–280. ACM, 2008.

[21] Tekrati. U.S. Online Dating Market to Reach $932 Million in 2011, Says JupiterResearch. http://industry.tekrati.com/research/news.asp?id=8487, 2007.

[22] G. Theodorakopoulos and J. S. Baras. On trust models and trust evaluation metrics for ad hoc networks. *IEEE J. Selected Areas in Communications*, 24(2):318– 328, 2006.

[23] Y. Wang and J. Vassileva. Trust and reputation model in peer-to-peer networks. In *Proc. P2P*, page 150, Washington, DC, USA, 2003. IEEE Computer Society.

[24] J.Y. Yen. Finding the K Shortest Loopless Paths in a Network. *Management Science*, 17(11):712, 1971.

James Stanier is a PhD student in the Foundations of Software Systems group at the University of Sussex. His work is primarily in optimising compilers, specifically graph-based intermediate representations. He is also a Features Editor of ACM XRDS magazine.

Stephen Naicken is a PhD student in the Foundations of Software Systems group at the University of Sussex. His work lies in the area of trust models and publish/subscribe systems.

Anirban Basu is a Post-doctoral Researcher at Kikuchi lab at Tokai University working on a Japanese Ministry of Internal Affairs and Communications funded project in collaboration with Waseda University, Hitachi, NEC and KDDI. Also, he is a Visiting Research Fellow at the University of Sussex working with the Foundations of Software Systems group.

Jian Li is a PhD student in the Foundations of Software Systems group at the University of Sussex. He is working on distributed compilation of Java bytecode.

Ian Wakeman is a senior lecturer, leading the Foundations of Software Systems group of the School of Informatics at the University of Sussex. He has a BA in Electrical and Information Sciences from Cambridge University, a MS from Stanford University and a PhD from UCL. His research could be described as user-centred networking, investigating protocols and techniques to make computer networks work for people. This has spawned over 60 refereed papers in fields as diverse as congestion control for packetized video, programming languages for active networks and has more recently focused on trust based approaches for network and system configuration in pervasive computing.