A smartphone-based online social network trust evaluation system

ARTICLE · JANUARY 2013

READS
31

1 AUTHOR:

Charles Perez
Paris School of business, France
18 PUBLICATIONS **25** CITATIONS

SEE PROFILE

Noname manuscript No.
(will be inserted by the editor)

A smartphone-based online social network trust evaluation system

Charles PEREZ · Babiga BIRREGAH · Marc LEMERCIER

the date of receipt and acceptance should be inserted later

Abstract The number of smartphone users has increased significantly over the last decade. The number of people using social networking sites is also increasing, and these platforms offer many features through which individuals can communicate with their contacts. The digital sphere is an opportunity for communication, but it is also an unprecedented arena for malicious attacks. The high quantity of personal and/or sensitive data, coupled with the large number of users, is one of the main motivations of malicious actors. We introduce in this paper a novel trust indicator for evaluating the contacts of an online social network user. This analysis is particularly important since the security policy of online social networks rests on the principle that a user's contact is a person of trust. This assumption, not always verified as true, gives any number of people access to personal information. To address this problem, we propose applying a multi-layer model and to extend it by proposing overlapping features that highlight the level of overlap of a contact belonging to the set of social networking friends of a smartphone user. We prove the efficiency of these features in evaluating trust by using a case study with Facebook and Twitter.

Keywords online social networks, trust, mobile devices, illegitimate contacts, overlap, ML-model.

1 Introduction

Social networking sites are used widely nowadays; the success of such platforms is illustrated by Facebook, which has recently surpassed 1 billion users. With the emergence of smartphones, mobile users can now communicate at any time and from anywhere on social networks via mobile social applications. The convergence of social and mobile technologies enables users to be strongly connected with the digital world. One of the basics elements for user joining a social network is the notion of contacts (often called friends). These contacts are the individuals with whom the user wants to exchange and share information. While user contacts in a given social network are assumed to be trustworthy, Boshmaf et al. [2011] have shown that most online social networks (OSN) users are not paying enough attention while selecting or accepting friends. This vulnerability has been used to attack the Facebook Immune System and access the personal data of Facebook users. These findings have been confirmed by the work of Nagle and Singh [2009], which demonstrates that some profiles with malicious intent may exist in the contact list of users. Research has found that having at least one connection in common is a factor in deciding to accept of a friend request. Such decisions by users are clearly not secure, since most of the social networking sites are merely one small world (Kleinberg [2000], Caci et al. [2012]). As a result, any pair of users is separated by only a few connections, and the network is highly clustered. Although research has revealed the existence of untrustworthy contacts, as of yet, no clear solution to this problem has been proposed. Therefore, while one publishes personal information on online social networking sites, some illegitimate users are being granted access to potentially sensitive data. As stated in the security policies of social platforms, the user is responsible for the people belonging to his or her group of friends, and these people are assumed to be trustworthy. By way of example, Facebook

ICD (Charles Delaunay Institute) - UMR CNRS STMR 6279 University of Technology of Troyes, 12 Rue Marie Curie, CS 42060, 10 004 TROYES CEDEX E-mail: {charles.perez, babiga.birregah, marc.lemercier}@utt.fr

clearly states that one should only send friend request to *people you have a real-life connection to, like your friends, family, coworkers or classmates.* Also they indicate that *if you're interested in receiving updates from people you find interesting, but don't know personally (e.g. journalists, celebrities, political figures), try following them instead of sending them friend requests.* (Facebook [2013b]).
In this article, we address the problem of trust in connections by proposing a novel indicator that integrates the user's activity. The originality of our approach lies in the fact that the trustworthiness of user contacts is based on a social network analysis of the smartphone of the user. The smartphone is very rich in information, as it is closely tied to its user. This makes our approach fully personalized; it integrates the user's personal activity. The work presented in this article is an extension of our previous research (Perez et al. [2012]). Among the principal improvements, we provide a comprehensive survey of concurrent methods and research work that can contribute to the creation of the multi-layer model (denoted ML-model). We also extend the evaluation of the methodology to the Twitter microblogging platform. Finally, we validate the feasibility of the approach by providing a real-life example of an application (called *Socializer*) for evaluating trust in social networks. We also present the first findings gathered from this application. The reader can request an updated trial version of this application through email to the corresponding author. The identification of trusted relationships, as proposed in this work, could be used for the authentication of users based on their mobile social networks. As the overlapping contacts are user-centred and are based solely on user activity, the identification/participation of such contacts could serve as a way of authenticating them on a given system (smartphone or social media).
The remainder of the article is organized as follows: section 2 presents a state of the art on trust assessment of social networking sites and highlights the current limitations. In section 3, we present smartphone data modelling and introduce the multi-layer model. Such a model is at the core of our approach, and its validity rests on its ability to identify the inter-layer connections. For this purpose, we also detail in this section the possible approaches that one can perform to identify such connections. Section 4 introduces the proposed indicators that evaluate the level of contact overlap in the multi-layer model of a smartphone user. Section 5 presents a new direct trust indicator that relies on the overlap features of the ML-model. Section 6 evaluates the accuracy of the proposed approach on Twitter and Facebook. Section 7 illustrates the feasibility of the approach; it presents the deployed *Socializer* smartphone application and its related findings. Section 8 concludes this paper.

2 State of the art

One can identify two main approaches to securing social platforms against malicious activities: on the one hand, a set of approaches aimed at detecting malicious players; and, on the other hand, some solutions based on reputation systems. This section proposes an overview of the principal work done for each type of approach.

2.1 Malicious user detection

The detection of malicious messages or profiles has been addressed by numerous scientific studies as a problem of classification. Already used for spam detection in e-mail inboxes, this approach has been adapted for social networks (Fette et al. [2007]). In this context, a malicious profile refers to a given digital entity that publishes unsolicited and/or malicious URLs on the given social networking site. Most of approaches that are based on classification consider the existence of two classes: malicious and innocuous profiles. These approaches constitute a training set for each class (a.k.a reference sample) and apply the related mathematical approaches (e.g. decision tree, Bayesian networks and support vector machines). The quality of detection mostly depends on the three following factors: (1) the quality of the training sample, (2) the method and related parameters used and (3) the type of variables included in the model.

The reference sample can be created in many ways. Firstly, as in the approach Wang [2010a,b], the creation of a set of reference profiles can be based on manual analysis by experts. Thus, a set of variable size (usually between 100 and 500 profiles) is scrutinized on the platform and then classified with one of the two labels, as determined by experts. Some works (Lee and Sumiya [2010], Lee et al. [2010], Stringhini et al. [2012]) propose the creation of *honey pot* profiles to attract the malicious profiles on social platforms. These have specific characteristics (photo profile, description), and their management is optimized in order to get the attention of malicious actors on the platform. In the case of Twitter, Perez et al. [2011] proposed automating this process. This approach uses the reports of users regarding disturbing profiles. The platform allows malicious profiles to be reported by inserting the @Spam or @Twitter references in

References	Profile	Behavioral	Message	Graph	Web
Stringhini et al. [2012]		x	x	Local	
Abu-Nimeh et al. [2011]		x	x		URLs
Wang [2010b]			x	Local	
Benevenuto et al. [2010]	x	x	x	Local	
Ghosh et al. [2012], Gayo Avello [2011]				Global	
Perez et al. [2011]	x	x	x	Local	URLs & content
Lee and Sumiya [2010], Lee et al. [2010]	x	x	x	Local	

Table 1 Comparison of approaches based on the indicator used

the tweets. Using the Twitter Search API and filtering according to the two references, it allows a significant amount of malicious profiles to be identified. However, the validation of an expert is not overlooked. Benevenuto et al. [2010] propose the creation of a set of profiles, starting with the malicious URLs of websites listed as dangerous. The approach scans the network messages for these URLs and detects the profiles that send such messages. In order to classify messages or users, it is often necessary to represent them as mathematical vectors. A vector contains a set of attributes that describe the represented entity. Regarding social media, these characteristics are measurable indicators of the activity of a profile. We propose classifying them into five categories: *Profile*, *Behaviour*, *Message*, *Web* and *Graph*.

- *Profile* refers to profile information such as age, gender or location.
- *Behaviour* is defined by a set of dynamic indicators that reveals the behaviour of a user online (e.g. number of messages sent, frequency of messages).
- *Message* relates to any aspect regarding the attributes of messages. As an example, the number of URLs and keywords used in the messages.
- *Web* is a category that identifies approaches that consider the analysis of cited URLs and related websites in the detection of malicious profiles.
- *Graph* reflects the possible integration of graph theory indicators, which can be important for revealing the position of the profile in the digital social network. These indicators can be local (e.g. node degree), semi-local (e.g. degree of neighbouring nodes) or global (e.g. Eigenvector centrality). Note that the latter is very expensive in terms of digital platform analysis, due to the large amount of nodes (several million).

Table 1 summarizes the indicators used by the various works in the literature.

2.2 Reputation system

Golbeck [2006] proposed a definition of trust for web-based services. It states that trust in a relation is: *a person engaging in an action with another person based on the belief that the future actions of people will benefit us.* A large amount of the work done is devoted to the establishment of a trust indicator for the profiles of digital social platforms (Kim et al. [2012]). Known primarily on e-marketing platforms (e.g. eBay), reputation systems have been enriched in order to better integrate and evaluate the quality of the behaviours of a profile Gunes et al. [2012]. Some works have proposed features that allow the detection and penalisation of fraudulent actions (e.g. shilling attacks, link farming). These indicators are constantly improved and adapted to integrate a variety of fraudulent behaviours and to adapt to the majority of social networking sites.
We can distinguish two main types of trust evaluation in social media: first, approaches that propose a calculation of a direct assessment of trust; and, second, the approaches that analyse trust propagation in networks. A comparison of these two approaches are available in the work Massa and Avesani [2007]. Here we present approaches involving the direct calculation of reputation on social media platforms.

Wang [2010a] has proposed to use prestige as a trust value. The prestige of a profile is equal to the ratio of the number of incoming links by the sum of incoming and outgoing links. On Twitter, this score is equal to the ratio of the number of followers of a profile by the total number of friends and followers. This feature expresses the attractiveness of a profile among the population of Twitter users

and assumes that attractive profiles are trustworthy.

Nepal et al. [2011] propose a model to assess trust in digital social networking communities. Here, the notion of trust derives from two main types of interactions: one based on the popularity of these communities and one based on engagement in these communities. The first criterion aims to highlight the trusted profiles that significantly attract users in social networks. It is evaluated based on the positive interactions between a pair of users. Positive interactions are interactions involving a positive exchange between the users involved. The second criterion is related to the involvement of a user in a community. Involvement in a given community is measured based on two aspects: passive or active engagement. Active engagement involves the publication of messages, comments and notes within the community, while passive engagement can be simply reading posts and messages. The proposed system, called *Struts*, linearly combines the two criteria presented.

Another system, called *Swtruts*, has been proposed to measure trust in digital social networks (Jiang and Wang [2011]). This solution for digital social networking sites offers an answer to the following question: Can Bob trust Alice to use a particular service? The strategy is to spread Bob's question among contacts in the hopes of getting a response from a contact interacting with Alice already. In the event that this does not happen, the question is transmitted to contacts of contacts, and so on, until an answer is given. The authors propose to answer this question using the common interest shared between each pair of users. The task is then to generate a graph containing all the shortest paths between Alice and Bob. Arcs are weighted using the areas of interest of users, and a trust indicator is generated based on this graph.

Korovaiko and Thomo [2013] have proposed a large set of features that can participate to the evaluation of trust on e-marketing platforms. Such features can take into account the similarity of the ratings given by users to the same products, the similarity of categories that users review, etc. The authors have tested these features on the well known Epinions.com platform and have proven that they allow to improve the performances of the classification algorithms by 5 to 20% in regard to the state of the art.

The approach called *Iris* has recently been proposed to address the problem of directly assessing trust (Hamdi et al. [2012]). The proposed approach combines three important dimensions. The first aspect concerns the interactions between users, the second, the type of relationship, and the third, similarity of interest. This approach relies on the analysis of *Friend of a Friend* (FOAF) files to distinguish and assess the strength and type of relationship existing between users.

Algorithms for assessing the trust level of social networking site users pose many difficult constraints which must be resolved. One major constraint is the need for players to assign a score to the users of the platform. This makes it possible for malicious profiles to tamper with the indicator scores by integrating fraudulent votes. This type of behaviour is known as shilling attack, and a comprehensive survey on the detection of such attacks can be found in Gunes et al. [2012]. In addition, many users cannot actively participate in the assessment system, which limits the results. Note that, on the majority of social networking platforms, no feedback on interaction is possible, as no means of evaluation is made possible by the system. Note also that the evaluation of a user or an action by a user requires correct perception on the part of the player. While after receiving a product it is easy to measure the quality of the transaction, when it comes to evaluating the potential danger of a profile, the problem becomes much more complex. For example, a user could trust one of his or her friends who launches malicious actions that are not visible.

3 A social network analysis approach to modelling smartphones

This section is organized in two parts. First, we present existing works that have handled the problem of modelling smartphone data by introducing the ML-model into the equation. Then, we present the set of techniques that can be used to build the inter-layer connections of such a model. Note that a model and metrics such as this would allow us to measure and evaluate the interaction between the smartphone user and his or her set of contacts over multiple social networking sites (e.g. Twitter, Facebook) and traditional communication media (e.g. SMS, mails, phone calls). The techniques presented for identifying inter-layer connections will permit the ML-model to be built as well as overlap features to be established. Such features allow us to measure the contacts of the user who appear to share close links not only in terms of interactions in a given social network but also in a series of media accessible from the smartphone. These contacts play an important role and can be used to measure the level of trust as detailed in the next sections.

3.1 Modelling and analysis of smartphone data

A few works have proposed ways of modelling and analysing smartphone data.
Dellutri et al. [2009] have proposed representing the phone contacts of a smartphone user as a graph and have used web data analysis to calculate the strength of the ties between the contacts. This work has contributed to a better understanding of the social network of a phone user.
Some research has focused on the analysis of the multiple social networks of a given user. Hossmann et al. have proposed an analysis that takes into account the mobility, social relationship and communication patterns of a user. The goal of this approach is to highlight the correlation between heterogeneous data (i.e. Address Book contacts, SMS, geolocation and Facebook).
Recently, Catanese et al. [2013] have presented a tool called *LogAnalysis* for performing a forensic analysis of phone calls. *LogAnalysis* allows to represent, filter and monitor the call logs.

Magnani and Rossi [2011] have recently proposed a multi-layer model (called the ML-model) that may contribute to unifying the multiple social faces of a social network user. This model has been applied and tested by the authors on the FriendFeed and Twitter social networks. In this work, we propose applying and extending this model so that it may be applied to a smartphone. Our approach is motivated by the fact that smartphones are used for interacting with friends throughout many distinct forms of social media. More specifically, we propose using smartphone data to extend the application of this model to a larger number of networks, laying the foundation for a theoretical approach to overlap metrics.

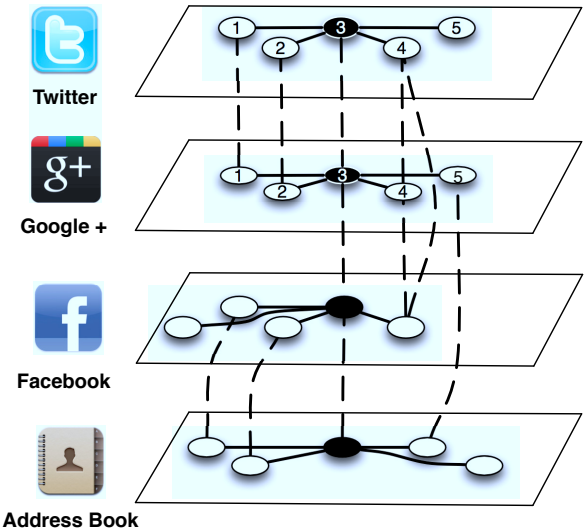

Fig. 1 The ML-model of a smartphone user

The multi-layer model is defined by a set L of K layers that are connected throughout a set of matching matrices. Each layer L_i corresponds to a social network that is represented as graph $G_i = (N_i, E_i)$. N_i is the set of nodes (i.e. profiles) and E_i the set of edges (i.e. relationships). The connections between the different layers are modelled by the matching matrices. Figure 1 shows an example of a multi-layer network that can be extracted from the user's smartphone (identified with black nodes). In the case of the multi-layer network of a smartphone user, as represented in the figure, each of the layers is a star network. In other words, the only information available on the smartphone is the contact list of the user on the multiple social networks.

There exist two types of connections in such networks: (1) the intra-layer connections, which are connections between users of a given social network, and (2) the inter-layer connections, which represent relationship between nodes of distinct social networks. The intra-layer connections are identified by the social network considered. For example, if the layer considered is Facebook, then the nature of the relation is identified by friendship. The inter-layer connections of the model, represented by dashed lines on the figure, require a matching condition to be verified. In this work, we propose matching two nodes if their corresponding profiles belong to the same individual. Although a great deal of data is available on a smartphone, the inter-layer connections are often not directly accessible on most of the devices. In the following subsection, we present the existing techniques that can aid in the identification of such connections.

3.2 Entity resolution

Entity resolution aims to find whether two profiles from different social networks belong to the same entity (Raad et al. [2010]). One can identify two types of approaches: direct matching approaches and indirect matching approaches. Below we present both types of approaches. We end this section with a discussion on the applicability of these approaches in a mobile context.

3.2.1 Inverse functional property-based approaches

The direct matching approach is based on the unique identifiers of a user on multiple social networks. These approaches are usually related to the mode of representation of a user profile. Among the most common profile representations is the Resource Description Framework (RDF), a metadata model for

representing any type of information as a subject-predicate-object expression. This framework has been enriched in the domain of social relationships by two ontologies, Friend of a Friend (FOAF) (Bojars et al. [2008], Brickley and Miller [2007]) and SIOC (Semantically Interlinked Online Communities) (Bojars et al. [2008]). These frameworks contain rich specifications that permit relationships to be made between individuals and their respective profiles. The description format is very rich and contains many unique identifiers that can be used to directly identify an entity over multiple platforms. These identifiers are referred to as an inverse functional property (IFP) and are defined as follows: *wherever you see the (subject) linked to an (object) by this particular (predicate), then the (subject) is the one and only (subject) with that (object) connected by the (predicate). If you ever see another subject linked to the object by the predicate, you'd know that the 'other' subject is actually the same subject.*

The work by Ding et al. [2005] relies on the use of the *mbox_sha1sum*, *foaf:homepage* and *foaf:name* to match profiles. The *mbox_sha1sum* is the result of the SHA1 mathematical function applied to email. The underlying assumption is that the profiles of the same individual over multiple social platforms contain the same email address. The homepage (*foaf:homepage*) is also used as a direct matching identifier between multiple entities. Although this could perform well, there is no guarantee that the user has indicated his homepage in the profiles. Finally, as the name of the user (*foaf:name*) is also used as an identifier, this approach can perform well, but only if the user precisely indicates his personal name in all of his digital profiles.

The problem with straight matching in terms of the personal name is that it can lead to 'no match' profiles should any difference exist between the names indicated. A set of measures have been proposed to overcome this limitation. The proposed measures aim to capture the degree of similarity not only between two strings (Elmagarmid et al. [2007]), but also, and more specifically, between two personal names (Christen [2006]). We present below a few ways of measuring similarity that allow such a task to be performed.

The Levenshtein distance is measured as the number of basic transformations needed to transfer the first chain to the second one (Levenshtein [1966]). The basic operations permitted are insertion, deletion and substitution. The Damerau-Levenshtein distance extends this measure by allowing transposition to be performed (Damerau [1964]).

The q-gram distance computes the number of subsequences of length q (called q-grams) in common between the two personal names (Kukich [1992]). Normalization is performed based on either the number of q-grams in the shortest string, the number of q-grams in the longest string, or the average of both. Note that the positional q-grams enable the distance between the matching q-grams to be taken into account in measuring similarity.

The Jaro metric computes the similarity between two strings by taking into account the order and number of common characters (Jaro [1989]). The Wrinkler measure improves the Jaro measure by integrating the fact that fewer errors occur at the beginning of personal names. It thus gives more importance to the first characters of the personal names. The sorted Winkler measure proposes sorting alphabetically the words that constitute the strings (e.g. name and surname) before computing the Wrinkler measure (Porter et al. [1997], Yancey [2005]).

Note that more complex measures exist for analysing similarity, such as indexes that are based on the phonetics of the personal names (e.g. Soundex by Zobel and Dart [1996]). The reader can refer to Christen [2006] and Elmagarmid et al. [2007] for an exhaustive list of these metrics.

3.2.2 Beyond IFP

A few approaches have been carried out to indirectly resolve the problem (without the use of a unique IFP). Attribute-based approaches aim to identify the similarity of two profiles based on their characteristics, such as their personal names, websites, interests or social circles (Raad et al. [2010], Singla and Domingos [2005]).

As an example, Raad et al. [2010] have propose using a large list of attributes available in FOAF files to performs the work of identity disambiguation. In this work, an adapted similarity measure is applied for each given attribute.

A different solution, based on the analysis of the entity labels, has also proven its efficiency in the case of an open source community (Shi et al. [2008]).

The framework called Flink proposes matching the identity of a user on multiple social networks with the use of multiple data sources (Web, Semantic Web, emails, publications) (Mika [2005]). The merging of the profiles is based on name matching and object identification, which are based on the IFPs.

Other approaches extend the set of characteristics analysed by integrating the characteristics of both profiles as well as the characteristics of their contacts. The work by Rowe and Ciravegna [2008] uses on the analysis of the social data and

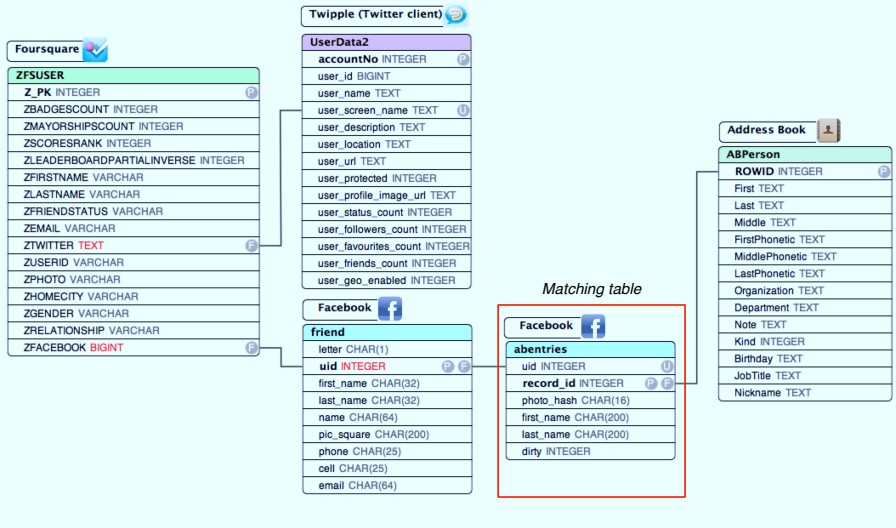

Fig. 2 SQLite databases of social applications retrieved on an iPhone 3GS. The connections that one can retrieve for carrying out matches are identified by full lines. Note that, under certain conditions, a matching table may be available and that all social networks allow the first and last name of contacts to be retrieved.

the identification of social circles for to perform the identity disambiguation.

Some approaches have proposed using the activity of the users as a solution to the problem of entity resolution (Melnikov and Schönwälder [2010], Chen and Hong [2007], Bergadano et al. [2002]). In the case of online game play activity, Chen and Hong [2007] have shown that activity distribution over the time can be a good representation of a user and could be used as an identifier.

3.2.3 Applicability to the mobile context

Smartphones store a great deal of information on the multiple interactions of a user. In this section we discuss the applicability of entity resolution in a smartphone context in order to identify the inter-layer connections of a multi-layer network.
Smartphone data are usually managed with the SQLite embedded relational database management system, which allows any application to store data locally on a smartphone. The SQLite system is now available on smartphone operating systems (e.g. iOS, Android) (Kreibich [2010], Newman [2004]). Note that the FOAF profiles of users are not directly accessible on mobile devices. This makes approaches such as Raad et al. [2010] not applicable in this context. However, a basic approach to performing a match could consist in the analysis of the local databases. As an example, some applications allow one's Facebook and Twitter contacts to be included and matched with the Address Book contacts. On an iPhone 3GS running firmware 4.3.5, we have observed that this operation leads to the matching data to be stored. The matching table is called *abentries* and contains pairs of matches between the Address Book and Facebook user's identifiers. Figure 2 represents the links that can be created between the Address Book, Facebook, Foursquare and Twipple (a Twitter client application). This figure only contains tables relevant to the purpose of this paper; however, many other tables exist for each social application. The figure highlights the connections that one can directly identify between the contacts found on the multiple platforms.

If no specific matching data is already present and available on the smartphone, one will have to apply classic approaches in order to carry out matching. It is clear that only inverse functional property-based approaches can be performed on the device, since no other data can be directly accessed on it. In this paper, we propose relying on the unique information that can be retrieved in any social network layer (i.e. name and surname of users). Although in real life the name and surname might not be enough to identify an individual, one can assume that, in a specific set of single user contacts, it is sufficient. Similarity measurements such as those of Levenshtein, Jaro and Winkler, which in most cases outperforms the two first measures, are adapted solutions that have proven their efficiency (Christen [2006]).

4 Proposed features

In this section, we propose a formalization of the matching function and the overlap features that are at the core of our proposal.

4.1 Node-matching function

Below we formalize the node-matching function that defines the inter-layer connections of the model. Given an individual u, encountered at least in one of the layers, we denote with u_k the node representing this user on layer L_k. Two nodes, u_k and v_l, match if we are able to detect that these nodes belong to the same individual in terms of the approaches presented in the previous section. To the contrary, the two nodes are considered as non-matching.

Definition 1: The node-matching function
Given two nodes, $u_k \epsilon L_k$ and $v_l \epsilon L_l$, and given a parameter $\theta \epsilon \mathbb{N}$, the function of node-matching is defined by:
$\forall k \neq l \epsilon \{1, , K\}$,

$$O^{\theta}(u_k, v_l) = \begin{cases} 1, if\ u_k\ and\ v_l\ match\ regarding\ \theta \\ 0, otherwise \end{cases}$$

The θ factor represents the maximum number of intermediate nodes that can be identified as two matching nodes by transitivity. For example, if a Twitter profile (T) matches with a Facebook profile (F) and this profile matches with a Google+ profile (G), but no match is directly identified between the Twitter and Google+ profiles, then:
$O^0(T, F) = 1$, $O^0(F, G) = 1$ and $O^1(T, G) = 1$.

Note that the matching function as stated in definition 1 is binary (i.e. a match exists or does not). However, in real-life application, entity disambiguation rarely allows two entities to be identified as matching with certitude. Instead, a measure of similarity is performed and pairs of entities that are above a given threshold are identified as a match. Thus, the challenge lies in the ability to select a good threshold. For this purpose, it is common to use a reference dataset with known matches and non-matches and to calculate from such dataset the threshold that allows the most accurate results to be obtained. This threshold is then used for predicting if a match exists between two profiles.

We introduce binary matching matrices as the adjacency matrices of the graphs that connect pairs of layers.

Definition 2: Matching matrices
The matching matrices of index θ are defined by:

$$\forall k \neq l \epsilon \{1, ..., K\}, M^{\theta}_{u_k, v_l} = O^{\theta}(u_k, v_l).$$

The matching matrices provide important insights into the behaviour of the smartphone user on social networking sites (Girard and Fallery [2009]). Such matrices give direct indications of the way that the user organizes his digital life. For a smartphone user, a zero matrix means that the intersection between two of a user's contact lists is null. One can interpret this fact as the desire on the part of the user to separate his or her digital faces. To the contrary, a matrix that is mostly composed of '1' indicates that a close relationship exists between the considered pair of social networks. In other words, the user's audience in both social networks is very similar. As an example, for figure 1, the matching matrix between the Twitter and Google+ layers is given below. Note that the order of the nodes is indicated by their identifier number.

$$M^0(Twitter, Google+) = \begin{pmatrix} 1&0&0&0&0 \\ 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&0 \end{pmatrix}$$

4.2 Overlap features

This section focuses on the concept of overlapping to enrich the current ML-model. Note that the ML-model includes two variants: the pillar model and general model. On the one hand, in pillar ML-model, if a node belongs to a certain layer, it cannot be connected with multiple nodes of another layer. On the other hand, in the general model, this is possible. In the following section, we adapt the definition with regard to the two possible variants of the ML-model.

In regard to the general model, the overlap of a node u_k into a layer L_l, denoted $O^{\theta}_G(u_k, L_l)$, is defined below. This feature is equal to the ratio of nodes of the layer matching this node to the total number of nodes of the layer.

Definition 3: Overlap of a node in a layer (general model)
The overlap of a node u_k into a layer L_l, for a given $\theta \epsilon \mathbb{N}$, is defined by:

$$\forall k, l \epsilon \{1, , K\}, O^{\theta}_G(u_k, L_l) = \frac{\sum_{v_l \epsilon N_l} O^{\theta}(u_k, v_l)}{|N_l|}.$$

In the case of a pillar model, the overlap of a node u_k into a layer L_l is denoted $O^{\theta}_P(u_k, L_l)$. Definition 4 states that this feature is equal to the number of nodes of the layer matching said node. Basically, the definition takes into account the fact that a given node cannot match with more than

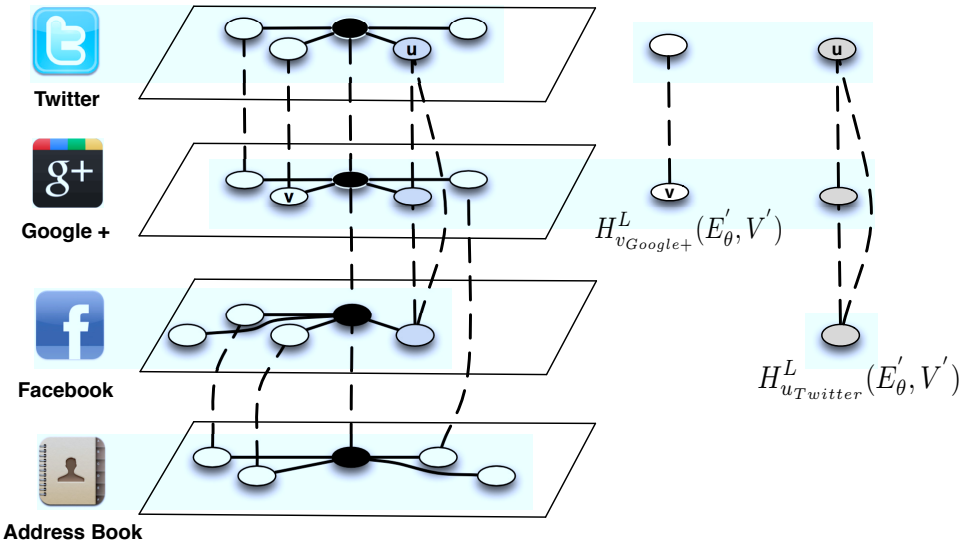

Fig. 3 Identity graphs obtained from the analysis of inter-layer connections of the multi-layer social network.

one node belonging to a distinct layer.

Definition 4: Overlap of a node in a layer (pillar model)
The overlap of a node u_k into a layer L_l, for a given $\theta \epsilon \mathbb{N}$, is defined by:

$$\forall k, l \epsilon \{1, , K\}, O^\theta_P(u_k, L_l) = \sum_{v_l \epsilon N_l} O^\theta(u_k, v_l).$$

We illustrate the overlap between a node and a layer using the node u of the figure 3. This node, belonging to the Twitter social network, is identified in both the Google+ and the Facebook layer. Using the pillar model, one can observe the following results:

$$O^0_P(u_{Twitter}, Google+) = 1$$
$$O^0_P(u_{Twitter}, Facebook) = 1$$
$$O^0_P(u_{Twitter}, AddressBook) = 0$$

The basic observation is that the given node u, has a certain presence in the digital life of the smartphone owner.

To measure this presence more precisely, we define the overlap of a node in a set of layers. Definition 5 illustrates the fact that the overlap of a node in a set of layers increases as its presence in multiple layers is observed. A node that belongs to any of the layers considered will get a high rate of overlap. Specifically, in the case of the smartphone-based ML network, this means that this node can access the information published by the smartphone user, whatever the communication channel may be.

Definition 5: Overlap of a node in a set of layers (general model)
The overlap of a node u_k into a set of layers $S \subset L$, for a given $\theta \epsilon \mathbb{N}$, is defined by:

$$\forall L_k \notin S, u_k \epsilon L_k, O^\theta_G(u_k, S) = \frac{\sum_{l \epsilon S} O^\theta_G(u_k, l)}{\sum_{l \epsilon S} |N_l|}.$$

Definition 6 proposes an adaptation of this feature in the case of a pillar model:

Definition 6: Overlap of a node in a set of layers (pillar model)
The overlap of a node u_k into a set of layers $S \subset L$, for a given $\theta \epsilon \mathbb{N}$, is defined by:

$$\forall L_k \notin S, u_k \epsilon L_k, O^\theta_P(u_k, S) = \frac{\sum_{l \epsilon S} O^\theta_P(u_k, l)}{|S|}.$$

In the example given in figure 3, regarding the pillar model, the node u is observed in three of the four layers analysed, and thus:

$$O^0_P(u_{Twitter}, L) = 0.75$$

It is important to notice that friend recommendation and management systems strongly encourage users to enlarge their number of friends. For example, Twitter offers a service that enables you to find your Facebook contacts in order to follow them. Some services also offer extending your Address Book with Facebook contacts. Many solutions also exist that let you import all your Facebook contacts into your Google+ social network.

Finally, we propose extending the notion of overlap to a given pair of layers of the model. The overlap between two layers gives an idea of the similitude between any pair of layers. For both models, this overlap is equal to the number of connections identified between these two layers divided by the number of maximum connections allowed by the model.

Definition 7: Overlap between two layers (general model)
The overlap of a layer L_k into a layer L_l is defined as follows:
$\forall \theta \epsilon \mathbb{N}, \forall k \neq l \epsilon \{1, , K\}$,

$$O_G^\theta(L_k, L_l) = \frac{\sum_{u_k \epsilon N_k} O_G^\theta(u_k, L_l)}{|N_k|}.$$

For the pillar model, the number of connections allowed is equal to the minimum number of nodes between the two layers.

Definition 8: Overlap between two layers (pillar model)
The overlap of layer L_k in layer L_l is defined as follows:
$\forall \theta \epsilon \mathbb{N}, \forall k \neq l \epsilon \{1, , K\}$,

$$O_P^\theta(L_k, L_l) = \frac{\sum_{u_k \epsilon N_k} O_P^\theta(u_k, L_l)}{min(|N_k|, |N_l|)}.$$

In the example provided, one can observe that the Twitter and Google+ layers possess five nodes. Thus, the expected maximum number of connections equals five. Among these five possible links, three connections are observed. This means that: $O_P^0(Twitter, Google+) = 0.6$. Similarly, one can deduce the following scores for each of the other pairs of layers.

$O_P^0(Twitter, Facebook) = 0.2$
$O_P^0(Twitter, AddressBook) = 0.0$
$O_P^0(Google+, Facebook) = 0.4$
$O_P^0(Google+, AddressBook) = 0.2$
$O_P^0(Facebook, AddressBook) = 0.6$

Such observations make it possible to highlight how close the two social networks of a given user are. On the one hand, highly overlapped pairs of layers can reveal the possible similar uses of the two social networks. On the other hand, completely non-overlapped layers can reveal a voluntary boundary created by the user among two of its digital faces. In the example, Twitter and the Address Book are completely non-overlapping, while Facebook and Address Book overlap significantly.

4.3 Identity graph

We have introduced a set of indicators that allows the multiple aspects of overlapping inside social networks to be identified. We propose modelling such indicators with an *identity graph (IG)*. The identity graph (see definition 9) allows the degree of a contact's overlap in a set of layers to be visualized easily. It is defined as a graph that contains nodes that match each other as well as their corresponding inter-layer connections. Note that if a contact is represented on a single layer, the corresponding identity graph is a single node.

Definition 9: Identity Graph
The identity graph of a node u_k belonging to a layer k, into a set of layers $S \subset L$, is denoted: $H_{u_k}^S(E_\theta^{'}, V^{'})$,
where: $E_\theta^{'}(H_{u_k}^S) = \{v_l \epsilon N, l \epsilon S \,|\, O^\theta(u_k, v_l) = 1\}$
and: $V^{'}(H_{u_k}^S) = \{(u, v) \epsilon E_\theta^{'} \times E_\theta^{'} \,|\, O^\theta(u, v) = 1\}$.

A common way to build the IG of a person is to cross the inter-layer connections with $\theta = 0$, starting with one of his or her identified profiles. The resulting graph of such an operation is noted $H_{u_l}^S(E_\theta^{'}, V^{'})$, where u is the start node and S the set of layers taken into account. In figure 3, regarding the pillar model, we have represented the two following identity graphs $H_{u_{Twitter}}^S(E_\theta^{'}, V^{'})$ and $H_{v_{Google+}}^S(E_\theta^{'}, V^{'})$. One can easily verify that the indicators proposed are directly related to the IG characteristics of social networks (e.g. given a node u belonging to a layer k and a set of layers $S \subset L$, $O_P^0(u_k, S) = \frac{|V'(H_{u_k}^S)|}{|S|}$). The overlap of the corresponding person is proportional to the number of nodes of such a graph. Note also that one could evaluate the reliability of the match based on the average degree of the graph.

5 Application

On social platforms, an important privacy issue is related to the notion of friendship. The security policy of the social platform considers all the contacts of a user as trustworthy, and thus gives them access to the data published. However, can one be sure that all of his or her contacts are trusted individuals? Some studies have shown that this security issue can be used to extract a significant

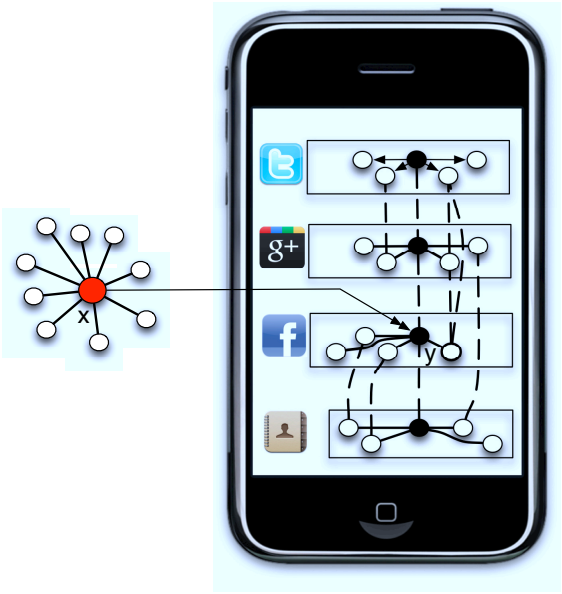

Fig. 4 Multi-layer network of a smartphone user. The x node represents a Facebook profile that is evaluated and the y node represents the smartphone user profile. Our approach aims to identify the similarity of x and y given only the data represented on the figure.

amount of Facebook users' private data (Nagle and Singh [2009]). This study has been furthered by some other works that have proven that a friendship request, even coming from a stranger, has an important rate of success (Acquist et al. [2007]). Smartphones, which natively integrate social networks, increase the potential impact of this risk since one can publish photos, texts and videos with a simple click.

In this section, we present an example of application of how overlap features can be applied to evaluate the trustworthiness of contacts. The proposed trust evaluation system relies on the link prediction problem. Figure 4 illustrates the situation. We want to impart a trust score to the contacts of a smartphone user on a given social network such as Facebook or Twitter. The information we intend to use is that of the ML network of the smartphone user and the friends of the tested contacts.

5.1 Current techniques

The link prediction problem involves the identification, given a snapshot of a social network, of the connections that will appear in the future. Most of the approaches rely on the measurement of a similarity score between each pair of nodes. The nodes with the highest similarity score are the ones that are assumed to be the most relevant to the prediction. One can identify three broad groups of similarity measurement between nodes: the one based on globally-based indices, the one based on quasi-locally based indices and the one based on locally-based indices (Lü and Zhou [2011]). The present work can be viewed as an adaptation of the problem as follows: given the multi-layer network of a smartphone user, which connections (i.e. future or existing friends) appear to be the most legitimate? Given this context, one can only consider the locally-based features in order to address the problem, since no other information is assumed to be available on a smartphone. In this section, we aim to present the main similarity indexes.

Multiple local similarity features have been proposed and an exhaustive list can be found in Lü and Zhou [2011] and Liben-Nowell and Kleinberg [2007]. We denote by x and y two given social network profiles. The sets of friends of x and y are denoted $\Gamma(x)$ and $\Gamma(y)$. Their respective number of friends is denoted k_x and k_y. Table 2 presents an overview of the similarity functions between a given pair of nodes x and y.

The most common local similarity measurement between a node x and a node y is the common neighbours (CN) index, which basically counts the number of common neighbours between the pair of nodes. On a social network, this means that two profiles that share many common friends are considered more likely be friends than two profiles that do not share many common contacts. The Facebook social network uses this assumption to recommend friends to a user (Facebook [2013a]).

The Jaccard (JA) index counts the number of common friends but ensures the normalisation of the similarity score. It takes into account the union of the two sets of neighbours for this purpose.

The Salton (SA) index is widely used in the literature and is often referred to as the cosine similarity, or Ochiai coefficient, in biology. This index is basically equal to the cosine similarity between the two vectors of neighbours. To perform such calculations, each neighbour vector should be represented as a binary array.

The Sørensen (Sø) index, also referred to as Dice's coefficient, gives a similarity score that is equal to twice the shared contacts over the total number of contacts.

The hub promoted and hub deprecated indexes (HPI and HDI, respectively) provide a way of giving more or less importance to links that are adjacent to hubs (Ravasz and Barabási [2003]). On Facebook, using the HDI to predict friendships allows a profile's similarity with that of a celebrity, which has a very high number of contacts, to be deprecated.

The preferential attachment (PA) index assumes that the similarity between two nodes is propor-

Indices	Formula
Common Neighbours	$\lvert\Gamma(x) \cap \Gamma(y)\rvert$
Salton Index	$\frac{\lvert\Gamma(x)\cap\Gamma(y)\rvert}{\sqrt{k_x * k_y}}$
Jaccard Index	$\frac{\lvert\Gamma(x)\cap\Gamma(y)\rvert}{\lvert\Gamma(x)\cup\Gamma(y)\rvert}$
Sørensen Index	$\frac{2\lvert\Gamma(x)\cap\Gamma(y)\rvert}{k_x+k_y}$
Hub Promoted Index	$\frac{\lvert\Gamma(x)\cap\Gamma(y)\rvert}{min\{k_x,k_y\}}$
Hub Deprecated Index	$\frac{\lvert\Gamma(x)\cap\Gamma(y)\rvert}{max\{k_x,k_y\}}$
Leicht Holme Newman Index	$\frac{\lvert\Gamma(x)\cap\Gamma(y)\rvert}{k_x * k_y}$
Preferential Attachment Index	$\lvert\Gamma(x)\rvert \, . \, \lvert\Gamma(y)\rvert$
Adamic Adar Index	$\sum_{z\epsilon\Gamma(x)\cap\Gamma(y)} \frac{1}{log(\Gamma(z))}$
Resource Allocation Index	$\sum_{z\epsilon\Gamma(x)\cap\Gamma(y)} \frac{1}{k_z}$

Table 2 List of local prediction metrics tested in this work.

tional to the product of their degree. This underlying model is used to generate scale-free networks that follow a power-law degree distribution. Applying such a model to social networks implies that famous profiles will more likely create connections than non-famous profiles. For the same reason, these connections will more likely involve other famous profiles.

The Leicht-Holme-Newman (LHN) index gives a high similarity score for two nodes possessing a large set of common neighbours with regard to the expected number of such neighbours in the configuration model (Leicht et al. [2006]). The configuration model defined in Molloy and Reed [1995] is a randomized realization of a particular network. This model proposes cutting each edge into two parts and bringing about a new random distribution of obtained stubs. In such model, the denominator $k_x * k_y$ is logically the expected number of common neighbours.

The Adamic-Adar (AA) index counts the common neighbours by giving the less connected nodes more weight (Adamic and Adar [2001]). This can be interpreted as the insignificance of sharing a common friend that is a celebrity on the network. Contrarily, getting a common friend with a low quantity of contacts will be weighted more heavily. This helps illustrate the fact that a person with a low quantity of friends may select his or her contacts more carefully than a famous person who may accept the friendship of many people.

The resource allocation (RA) index adds the inverse of the number of its contacts for each common neighbour z. This index, as indicated by its name, is closely related to the physical process of resource allocation (Zhou et al. [2009]). The similarity evaluates the amount of information that can be sent from x to y via their common neighbours. Each common neighbour, is identified as a transmitter possessing a resource that it will equally distribute to all of his neighbours. The total amount of resources received by y from x corresponds to the similarity score.

5.2 Overlap-based indicator

Online social networks usually do not distinguish the multiple types of relationships that one can possess (e.g. family, workmates). Thus, each contact is treated equally in terms of permissions and importance. For example, the Facebook friend recommendation system called *People You May Know* is based mainly on the number of common neighbours and the work and education information of users (Facebook [2013a]). This model is clearly not a sufficient means of ensuring the level of trustworthiness of a given number of contacts in the network. To overcome this limitation, a possible solution would be to integrate the number of contacts of the common neighbours into the evaluation of contacts. This observation, as integrated into the indices presented, allows the nodes to be distinguished depending on their degree. Although this seems to be a good solution, it is clear that the degree of a contact is not enough to determine its importance. For example, on Facebook, many contacts may be ignored by an individual because their presence among his or her set of friends may be passive, accidental or not significant. To the contrary, family members of the user may be identified as more important and thus would affect the similarity score more heavily. To overcome this limitation, which applies to any of the presented similarity features, we propose enriching the resource allocation index by establishing overlap as a parameter of information allocation between a pair of nodes. The underlying assumption is that important transmitters are more likely to be profiles

that are highly overlapped in the multi-layer social network. The proposed smartphone-weighted resource allocation index is defined in equation 1:

Definition 10 : smartphone-weighted resource allocation (SWRA) index

Given a smartphone user y and a tested profile x, the SWRA index is computed as:

$$s_{xy}^{SWRA} = \sum_{z \epsilon \Gamma(x) \cap \Gamma(y)} \frac{O_P^{\theta}(z, L)}{k_z}. \quad (1)$$

Where:

L is the set of social network layers,
k_z the degree of z,
θ a given natural number,
x the tested user,
y the target user (smartphone owner),
$O_P^{\theta}(z, L)$ is the overlap of z in L.

6 Evaluation of the approach

We tested our approach on a set of social network layers (AddressBook, Twitter, Google+ and Facebook) extracted from smartphones and a set of contacts (friends and non-friends) extracted from Facebook and Twitter. The overlap network extracted from the multi-layer network of a given user is represented in figure 5. Each connected component of the graph represents the identity graph of a Facebook contact among the four layers. The strategy used for harvesting data on the smartphone is based on an analysis of the synchronization files, but alternatives do exist (Bader and Baggili [2010]), and a smartphone-embedded solution will be presented later in this paper.

We illustrate two of the four reference datasets in figure 6. These represent the graphs extracted from a level-two depth-first traversal on the Twitter (a) and Facebook (b) social networks. These graphs have been represented with Gephi software (Bastian et al. [2009]) by performing the Fruchterman-Reingold visualization algorithm. In the case of Facebook, the graph contains 25,230 nodes connected by 29,521 edges. The measured clustering coefficient is equal to 0.636 and the average path length is equal to 4.48. In the case of Twitter, the graph contains 15,088 nodes and 17,236 edges. The clustering coefficient is 0.247 and the average path length is 3.2.

To evaluate the approach, it is necessary to assume that a subset of existing links are not known. Thus, the efficiency of each algorithm relies on the ability to predict such *non-observed* (but existing) connections. Basically, a good classifier is expected

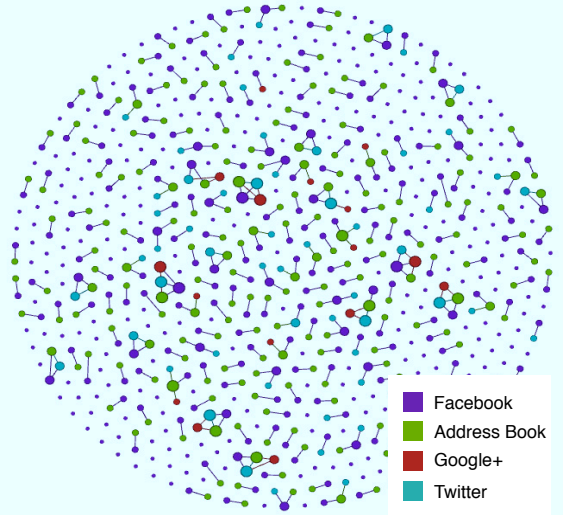

Fig. 5 Identity graphs, extracted from a smartphone, illustrating the overlap of Facebook contacts among the three other considered layers.

to give more weights to *non-observed* links than to *non-existing* links. In our case, the edges are connections that illustrate *a verified friendship* between the smartphone user and his contacts. A verified friendship is identified as a friendship that is certified as trustworthy by the concerned person and validated by an expert. This has been done by directly asking the smartphone owner to label his or her social network friends as trustworthy or not. A detection of potential malicious activities of the labelled trustworthy profiles (e.g. publishing malicious URLs) is also performed to certify that such profiles are not performing malicious activities (Perez et al. [2011]). If this is the case, such profiles are removed from the list of contacts and are considered as *non-existing* links. Such preprocessing ensures that the performance of each approach is based on its capability to detect certified trustworthy relationships.

Here we evaluate the efficiency of our proposed smartphone-weighted resource allocation index in regard to the other similarity measures presented using the area under the ROC curve (AUC) metric (Hanley and McNeil [1982]). The AUC score is calculated based on n independent comparisons between a *non-observed* and a *non-existing* pair of links. The number of times that the algorithm gives a *non-observed* link a higher score than a *non-existing* link is equal to n' (and n'' if they have the same score).

Given these parameters, the AUC is calculated as in the following equation:

$$AUC = \frac{n' + 0.5n''}{n}.$$

The accuracy of the prediction is as high as the AUC number is close to one. Contrarily, a random

Indices	Facebook		Twitter	
	Dataset 1	*Dataset 2*	*Dataset 3*	*Dataset 4*
CN	0.908	0.892	0.782	0.755
Salton	0.910	0.889	0.640	0.610
Jaccard	0.907	0.897	0.547	0.540
Sørensen	0.907	0.892	0.465	0.525
HPI	0.905	0.891	**0.935**	**0.905**
HDI	0.918	0.886	0.670	0.675
LHN	0.913	0.878	0.552	0.575
PA	0.535	0.559	0.500	0.535
AA	0.901	0.833	0.732	0.740
RA	0.886	0.843	0.715	0.745
SWRA	**0.983**	**0.921**	0.695	0.750

Table 3 AUC values for the datasets (best results shown in bold and worst results underlined)

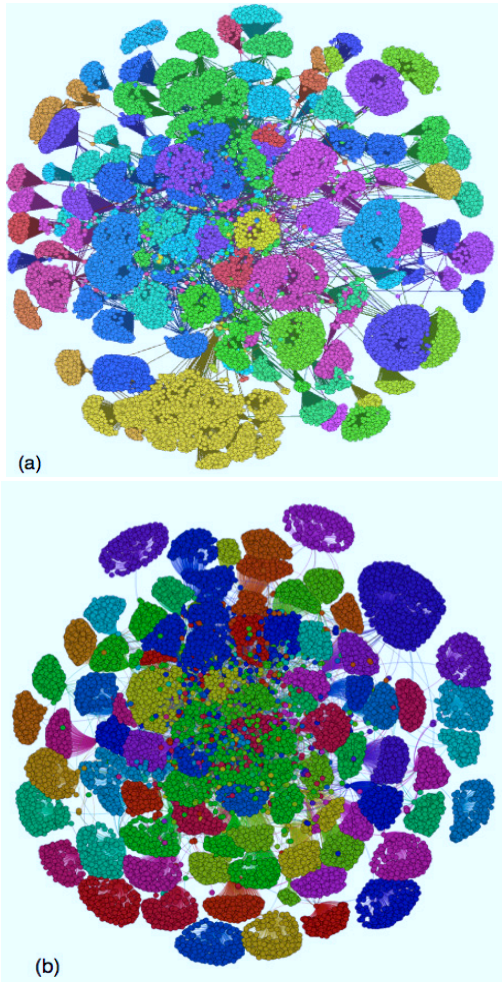

Fig. 6 Facebook (a) and Twitter (b) graphs extracted from a level-two depth-first traversal. Nodes belonging to the same community have the same colour.

algorithm is assumed to have an AUC value that is close to 0.5.

The results obtained for the indices are presented in table 3 for the Twitter and Facebook datasets.

Regarding Facebook, we observe that the proposed SWRA index obtains the best results for both datasets. The preferential attachment index is less efficient in predicting the relationship of two contacts on the Facebook network. This means that the relationship is not well described if only the number of contacts in profiles is taken into account. We can also observe that the common neighbour based indices perform relatively well. However, it is possible that the distinction between these approaches and the SWRA feature proposed in this paper occurs in sensitive cases. In other words, the overlap feature lets one discriminate a pair of nodes that could not be identified as legitimate based on the unique common neighbour score. Regarding the Twitter datasets, we can observe that our proposed approach does not obtain the best results. This allows us to suppose that the nature of connections is not based principally on the identity of the people. Indeed, as already stated, Twitter relationships are based more on the information than on the people. We note that the hub promoted index is the only indicator that performs significantly well. This means that users connect to people that already possess many connections on the network. This observation reflects the fact that on Twitter the degree of a node is often seen as a level of prestige and trust. This phenomenon is further backed by the fact that Twitter bases its contact recommendation system on this principle. The Gayo Avello [2011] work has proven that malicious Twitter profiles obtain a high centrality score when applying the most common centrality algorithms (PageRank, HITS, NodeRanking, etc.). Lee et al. [2010] has identified that this is mainly due to the fact that legitimate users follow a large amount a spammers. These observations reveal a very important security issue. Based on the facts presented, the creation of a relationship

on Twitter is based mainly on a feature that is not capable of ensuring trustworthiness. This aspect calls for deep investigation in further works. We have observed that, for information-centred social networks such as Twitter, the presented approach does not perform well. This is mainly due to the fact that our approach relies on the modelling of a personal device based on user-centred types of layers (e.g. SMS, Mail, Phones). A possible solution to the identification of a trustworthy relationship on Twitter could be to adapt the overlapping feature so that it can capture the level of importance of a given topic in the ML network of the smartphone user. With such a solution, each layer would be represented by a graph in which nodes are topics (or interests) instead of people. This could allow the important interest of the user to be identified based on his or her activity (i.e. content of messages) on the multiple online social networks and traditional communication media. A combination of both profile-based and topic-based overlapping features could also offer interesting perspectives for the same purpose (Tchuente et al. [2013]). However, for user-centred social networks, overlapping would appear to be a complementary tool for the existing approaches to better distinguish the illegitimate and legitimate contacts. This confirms the fact that legitimate connections between Facebook users are more likely to appear if they share friends that have a significant overlap in the ML network. In other words, the scores illustrate the fact that the data available on the smartphone of a user can be used to discriminate between trustworthy and non-trustworthy contacts on user-centric networks.

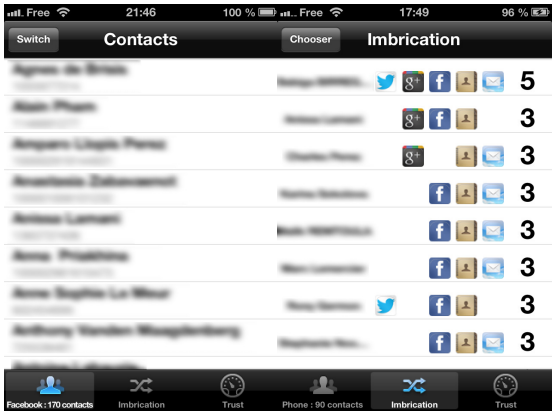

Fig. 7 Contact list and overlap screens

Fig. 8 Common friends overlap and trust score screens

7 Prototype

We have developed an iOS application for illustrating the feasibility of our approach in a mobile context. This application, called *Socializer*, works on iPhone and iPad running on iOS6. A updated trial version of the application can be requested by contacting the corresponding author. It analyses the following five layers: Facebook, Twitter, Google+, Mail and Address Book (referred as Phone in the rest of this section). The integration of Facebook and Twitter is simplified with the native integration of these social networks into iOS6. The application provides three main screens. The first screen, shown on the left side of figure 7, displays the multiple contacts of the user on the distinct social layers considered. The user can change layers easily with the top-left menu item, called *Switch*.

The second screen, on the right side of figure 7, shows the result of the analysis of the overlap (not normalized and in the pillar model) among contacts in reference to the layers that one wants to take into account. By default, the application displays the overlap regarding all layers that contains a non-null list of contacts. The user can change this setting and activate or deactivate any of the layers.

The third screen, on the left side of figure 8, displays the trust score given to each Facebook contact. It integrates the possibility of displaying the common friends and their respective overlap score for a selected contact. The common friend overlap is illustrated on the right side of figure 8. Finally, to perform a large-scale analysis, the application allows the results of the extraction to be exported and sent by e-mail.

We present below the results of the overlap and trust scores collected from the application. Although they are not required for the validation of our approach, we think that such results are valuable and can help give new insight into social network uses and the relative level of security of user data (Vorvoreanu [2010]). A total number of thirty individuals have participated in the experiment. All of these users own an iPhone or an iPad device and use the Facebook social network.

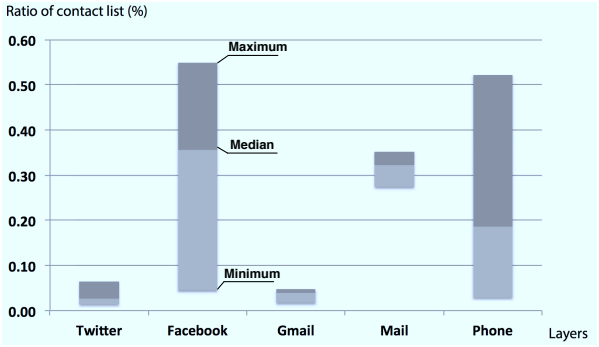

Fig. 9 Ratio of contacts for each social network

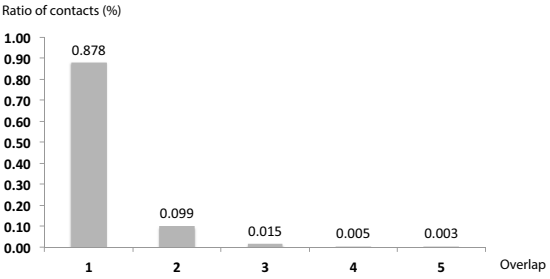

Fig. 10 Average overlap of profiles over the five layers

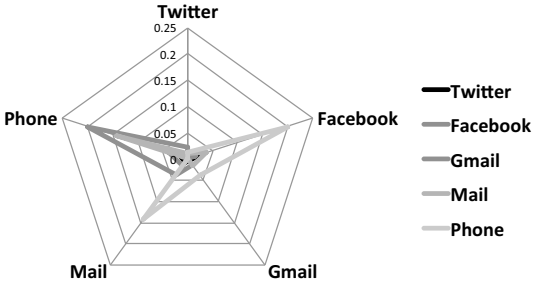

Fig. 11 Average overlap between each pair of layers

Although non-exhaustive, these results give some insight into the possible perspectives of this work and illustrate the feasibility of our proposed approach.

Figure 9 shows the average distribution of contacts over the social media of smartphone users. On such a map, one can observe the minimum, maximum and the median scores for each layer. The Twitter and Google+ layouts are the least represented among the individuals involved in the experiment. However, the mail layout represents an average 40% of the total contacts. The Facebook and Phone contact lists are usually well represented, but their ratio is very sparse. Based on these observations, we can state that, in most cases, at least three layers (Facebook, Mail and Phone) are available on the smartphone. The two other layers are not represented per se, and this could reduce the thoroughness of the approach.

Figure 10 illustrates the distribution of overlap scores (not normalized) over the five dimensions. We have observed that more than 10% of contacts have an overlap of greater than one. These are the most overlapping digital entities and are assumed to share a close relationship with the smartphone owner. The highest score in terms of the results of our approach was for the identification of these contacts. Only a very few contacts possess an overlap of up to three, and this matches with the results for the distribution of contacts.

In figure 11, we show the average overlap between pairs of layers. For better visualization, we have set the overlap of a layer with itself to null. One can see that Twitter hardly overlaps with any other layer taken into consideration. The main reason is that Twitter is not a person-oriented system, but rather an information-oriented system (Boyd and Ellison [2007]). Thus, the nature of the layer is fundamentally different. One can observe that the Phone layer is well overlapped with the Facebook, Google+, and Mail layers. However, this overlap does not exceed 20% for the Phone and Facebook pair, and is only 15% for the Phone and Mail pair of layers. The significant overlap of the Facebook layer over the other layers is a sign of the success of our proposed approach.

The distribution of computed trustworthiness to contacts as a ratio of the maximum amount is illustrated in figure 12. Such a representation allows the distinct types and ratios of the contacts of a given Facebook user to be evaluated. We can see that about 30% of a person's contacts can be assumed to be trustworthy, since they possess between 70% and 100% of the highest maximum trust. About 35% possess a score that varies from 30% to 70% of the maximum trust, and these contacts are not connected by a key person but instead share a significant amount of common contacts considered as trustworthy. Approximately 25% of contacts are located in the 10% to 20% range. This result proves that one may possess a set of contacts that only have a few contacts in common. Finally, about 15% of contacts have a very low score of trustworthiness. Such contacts appear among a person's social network contacts but with no legitimacy a priori. Such contacts are completely disconnected from the observed interaction of the user in the four other layers. These people can access a person's private and personal data without any legitimacy.

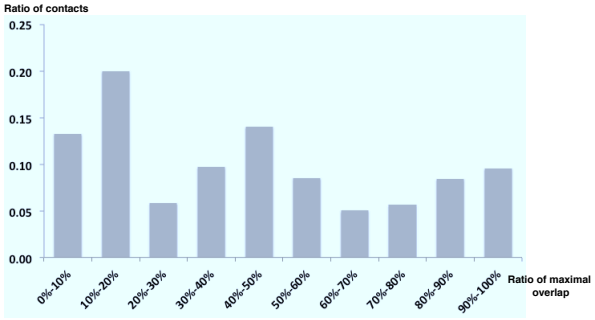

Fig. 12 Trust repartition among contacts

8 Conclusion

In this paper, we have proposed a novel approach to addressing the issue of evaluating the trustworthiness of the contacts of a social network user. The method relies on the multi-layer graph, which models the multiple interactions of a smartphone user with its multiple social media. Such a model, improved by overlap metrics, allows important contacts to be identified and to integrate such contacts into the evaluation of trust. Applying this model to Facebook has proven the efficiency of our approach, and the deployment of the *Socializer* application has illustrated its feasibility. To the best of our knowledge, this approach is the first attempt to analyse the trustworthiness of social networking site users based on smartphone modelling. The direct integration of such an approach into smartphones has many advantages. The evaluation of the trust score does not require any user participation and it only relies on data available locally on the smartphone. The analysis is performed on the user's smartphone; no rule of confidentiality is violated and no special access to information is required. In future work, we plan to integrate the weights of the edges in the model such as the temporal aspect of the interaction between the smartphone user and its contacts. Also, we plan to analyse the impact of the software on the users' behaviour.

9 Acknowledgment

This work is part of the CyNIC (Cybercrime, Nomadism and IntelligenCe) CPER project supported by the Champagne-Ardenne region and European Regional Development Fund (ERDF).

References

Saeed Abu-Nimeh, Thomas M. Chen, and Omar Alzubi. Malicious and spam posts in online social networks. *IEEE Computer*, 44(9):23–28, 2011.

Alessandro Acquist, Elisabetta Carrara, Fred Stutzman, Jon Callas, Klaus Schimmer, Maz Nadjm, Mathieu Gorge, Nicole Ellison, Paul King, Ralph Gross, and Scott Golder. Security Issues and Recommendations for Online Social Networks, October 2007.

Lada A. Adamic and Eytan Adar. Friends and neighbors on the web. *Social Networks*, 25:211–230, 2001.

Mona Bader and Ibrahim Baggili. iPhone 3GS Forensics: Logical analysis using Apple iTunes Backup Utility. *Small scale digital device forensics journal*, 2010.

Mathieu Bastian, Sebastien Heymann, and Mathieu Jacomy. Gephi: An Open Source Software for Exploring and Manipulating Networks. In *International AAAI Conference on Weblogs and Social Media (AAAI)*, 2009.

Fabricio Benevenuto, Gabriel Magno, Tiago Rodrigues, and Virgilio Almeida. Detecting spammers on Twitter. In *Proceedings of the 7th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS)*, 2010.

Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security*, 5(4):367–397, November 2002.

Uldis Bojars, Alexandre Passant, Richard Cyganiak, and John Breslin. Weaving SIOC into the Web of Linked Data. In *Proceedings of the WWW 2008 Workshop Linked Data on the Web (LDOW), Beijing, China*, 2008.

Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. The socialbot network : When Bots Socialize for Fame and Money . In *the 27th Annual Computer Security Applications Conference (ACSAC)*, page 93, New York, New York, USA, 2011. ACM Press.

Danah Boyd and Nicole B Ellison. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1-2), 2007.

Dan Brickley and Libby Miller. The Friend Of A Friend (FOAF) Vocabulary Specification. Technical report, November 2007.

Barbara Caci, Maurizio Cardaci, and MarcoE. Tabacchi. Facebook as a small world: a topological hypothesis. *Social Network Analysis and Mining*, 2(2):163–167, 2012.

Salvatore Catanese, Emilio Ferrara, and Giacomo Fiumara. Forensic analysis of phone call networks. *Social Network Analysis and Mining, 3(1):15-33*, 2013.

Kuan-Ta Chen and Li-Wen Hong. User Identification based on Game-Play Activity Patterns. In *Proceedings of the 6th ACM SIGCOMM workshop on Network and System Support for Games (SIGCOMM)*, pages 7–12. ACM, 2007.

Peter Christen. A comparison of personal name matching: Techniques and practical issues. In *Workshop on Mining Complex Data (MCD), held at IEEE ICDM'06, Hong Kong*, pages 290–294, 2006.

Fred J. Damerau. A technique for computer detection and correction of spelling errors. *Communication of the ACM*, 7(3):171–176, March 1964.

Fabio Dellutri, Luigi Laura, Vittorio Ottaviani, and Giuseppe F Italiano. Extracting social networks from seized smartphones and web data. *Information Forensics and Security, 2009. (WIFS)*, pages 101–105, 2009.

Li Ding, Lina Zhou, Timothy W Finin, and Anupam Joshi. How the Semantic Web is Being Used: An Analysis of FOAF Documents. In *Hawaii International Conference on System Sciences (HICSS)*, 2005.

Ahmed K. Elmagarmid, Panagiotis G. Ipeirotis, and Vassilios S. Verykios. Duplicate record detection: A survey. *EEE Transactions on Knowledge and Data Engineering*, 19(1):1–16, January 2007.

Facebook. People you may know, sep 2013a. URL `https://www.facebook.com/help/www/501283333222485/`.

Facebook. Adding friends & friend requests, sep 2013b. URL `https://www.facebook.com/help/www/360212094049906`.

Ian Fette, Norman Sadeh, and Anthony Tomasic. Learning to detect phishing emails. In *Proceedings of the 16th international conference on World Wide Web (WWW)*, pages 649–656, New York, NY, USA, 2007. ACM.

Daniel Gayo Avello. All liaisons are dangerous when all your friends are known to us. In *Proceedings of the 22nd ACM conference on Hypertext and hypermedia (HT)*, pages 171–180, New York, NY, USA, 2011. ACM.

Saptarshi Ghosh, Bimal Viswanath, Farshad Kooti, Naveen Sharma, Gautam Korlam, Fabricio Benevenuto, Niloy Ganguly, and Krishna P Gummadi. Understanding and combating link farming in the twitter social network. *Proceedings of the 21st international conference on World Wide Web (WWW)*, 2012.

Aurélie Girard and Bernard Fallery. Digital Social Networks: literature review and research perspectives. In *Association Information and Management*, June 2009.

Jennifer Golbeck. Trust on the world wide web: a survey. *Foundations and Trends in Web Science*, 1(2), January 2006.

Ihsan Gunes, Cihan Kaleli, Alper Bilge, and Huseyin Polat. Shilling attacks against recommender systems: a comprehensive survey. *Artificial Intelligence Review*, pages 1–33, November 2012.

Sana Hamdi, Alda Lopes Gancarski, Amel Bouzeghoub, and Sadok Ben Yahia. IRIS: A Novel Method of Direct Trust Computation for Generating Trusted Social Networks. In *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 616–623, 2012.

James A Hanley and Barbara J McNeil. The Meaning and Use of the Area under a Receiver Operating (ROC) Curvel Characteristic. *Radiology*, 143(1):29–36, 1982.

Theus Hossmann, Franck Legendre, George Nomikos, and Thrasyvoulos Spyropoulos. Stumbl: Using Facebook to Collect Rich Datasets for Opportunistic Networking Research. *Information Forensics and Security, (WIFS),2009.*

Matthew A Jaro. Advances in record-linkage methodology as applied to matching the 1985 census of Tampa, Florida. *Journal of the American Statistical Association*, 1989.

Wenjun Jiang and Guojun Wang. SWTrust: Generating Trusted Graph for Trust Evaluation in Online Social Networks. In *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011*, pages 320–327. IEEE Computer Society, 2011.

Mucheol Kim, Jiwan Seo, Sanghyun Noh, and Sangyong Han. Identity management-based social trust model for mediating information sharing and privacy enhancement. *Security and Communication Networks*, 5(8):887–897, 2012.

Jon Kleinberg. The small-world phenomenon: an algorithm perspective. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 163–170, New York, NY, USA, 2000. ACM.

Nikolay Korovaiko and Alex Thomo. Trust prediction from user-item ratings. *Social Network Analysis and Mining*, 3(3):749–759, 2013.

Jay A. Kreibich. *Using SQLite*. O'Reilly Media, 1st edition, 2010.

Karen Kukich. Techniques for automatically correcting words in text. *ACM Computing Surveys*, 24(4):377–439, December 1992.

Kyumin Lee, James Caverlee, and Steve Webb. The social honeypot project. In *Proceedings of the 19th international conference on World wide*

web (WWW), page 1139, New York, New York, USA, 2010. ACM Press.

Ryong Lee and Kazutoshi Sumiya. Measuring geographical regularities of crowd behaviors for Twitter-based geo-social event detection. In *Proceedings of the 2nd ACM SIGSPATIAL International Workshop on Location Based Social Networks (SIGSPATIAL)*, pages 1–10, New York, NY, USA, 2010. ACM.

E. A. Leicht, Petter Holme, and M. E. J. Newman. Vertex similarity in networks. *Physical Review E*, 73(2):026120, February 2006.

Vladimir Levenshtein. Binary codes capable of correcting deletions, insertions, and reversals. *Soviet Physics Doklady*, 10(8):707–710, 1966.

David Liben-Nowell and Jon Kleinberg. The link-prediction problem for social networks. *Journal of the American Society for Information Science and Technology*, 58:1019–1031, 2007.

Linyuan Lü and Tao Zhou. Link prediction in complex networks: A survey. *Physica A: Statistical Mechanics and its Applications*, 390(6): 1150–1170, March 2011.

Matteo Magnani and Luca Rossi. The ML-Model for Multi-layer Social Networks. In *Advances in Social Networks Analysis and Mining (ASONAM)*, pages 5–12. IEEE Computer Society, 2011.

Paolo Massa and Paolo Avesani. Trust Metrics on Controversial Users. *International Journal on Semantic Web and Information Systems*, 3(1): 39–64, 2007.

Nikolay Melnikov and Jürgen Schönwälder. Cybermetrics: user identification through network flow analysis. In *Proceedings of the Mechanisms for autonomous management of networks and services, and 4th international conference on Autonomous infrastructure, management and security (AIMS)*, pages 167–170. Springer-Verlag, 2010.

Peter Mika. Flink: Semantic Web technology for the extraction and analysis of social networks. *Web Semantics: Science, Services and Agents on the World Wide Web*, 3(2-3):211–223, October 2005.

Michael Molloy and Bruce Reed. A critical point for random graphs with a given degree sequence. *Random Structures Algorithms*, 6(2-3):161–180, March 1995.

Frank Nagle and Lisa Singh. Can Friends Be Trusted? Exploring Privacy in Online Social Networks. In *International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pages 312–315. IEEE, 2009.

Surya Nepal, Wanita Sherchan, and Cecile Paris. STrust: A Trust Model for Social Networks. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pages 841–846, 2011.

Chris Newman. *SQLite (Developer's Library)*. Sams, Indianapolis, IN, USA, 2004.

Charles Perez, Marc Lemercier, Babiga Birregah, and Alain Corpel. SPOT 1.0: Scoring Suspicious Profiles on Twitter. In *2011 International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pages 377–381. IEEE, 2011.

Charles Perez, Babiga Birregah, and Marc Lemercier. The Multi-layer Imbrication for Data Leakage Prevention from Mobile Devices. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pages 813–819. IEEE, 2012.

Edward H. Porter, William E. Winkler, Bureau Of The Census, and Bureau Of The Census. Approximate string comparison and its effect on an advanced record linkage system. In *Advanced Record Linkage System. U.S. Bureau of the Census, Research Report*, pages 190–199, 1997.

Elie Raad, Richard Chbeir, and Albert Dipanda. User Profile Matching in Social Networks. In *13th International Conference on Network-Based Information Systems (NBiS)*, pages 297–304. IEEE, 2010.

Erzsébet Ravasz and Albert-László Barabási. Hierarchical organization in complex networks. *Physical Review E*, 67(2):026112, February 2003.

Matthew Rowe and Fabio Ciravegna. Disambiguating identity through social circles and social data. In *1st International Workshop on Collective Semantics: Collective Intelligence & the Semantic Web (CISWeb)*, 2008.

Lian Shi, Diego Berrueta, Sergio FernÃ¡ndez, Luis Polo, and Silvino Fernandez. Smushing rdf instances: are alice and bob the same open source developer? In *ISWC2008 workshop on Personal Identification and Collaborations: Knowledge Mediation and Extraction (PICKME)*, October 2008.

Parag Singla and Pedro Domingos. Object identification with attribute-mediated dependences. In *Proceedings of 9th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD)*, pages 297–308, 2005.

Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. Detecting spammers on social networks. In *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC)*, pages 1–9. ACM Request Permissions, 2012.

Dieudonne Tchuente, Marie-Francoise Canut, Nadine Jessel, Andre Peninou, and Florence Sedes. A community-based algorithm for deriving users' profiles from egocentrics networks: experiment on facebook and dblp. *Social Network Analysis and Mining*, 3(3):667–683, 2013.

Mihaela Vorvoreanu. Managing identity across social networks. *Poster session at the 2010 Conference on Computer Supported Cooperative Work*, 2010.

Alex Hai Wang. Don't follow me: Spam detection in twitter. In *Conference on Security and Cryptography (SECRYPT)*, 2010a.

Alex Hai Wang. Detecting spam bots in online social networking sites: a machine learning approach. In *Proceedings of the 24th annual IFIP WG 11.3 working conference on Data and applications security and privacy (DBSec)*, pages 335–342, Berlin, Heidelberg, 2010b. Springer-Verlag.

William E. Yancey. Evaluating string comparator performance for record linkage. 2005.

Tao Zhou, Linyuan Lü, and Yi-Cheng Zhang. Predicting missing links via local information. *The European Physical Journal B*, 71(4):623–630, October 2009.

Justin Zobel and Philip Dart. Phonetic string matching: lessons from information retrieval. In *Proceedings of the 19th annual international ACM SIGIR conference on Research and development in information retrieval (SIGIR)*, pages 166–172, New York, NY, USA, 1996. ACM.