LoTrust: A Social Trust Level Model based on Time-Aware Social Interactions and Interests Similarity

Ahlem Kalaï
MIR@CL Laboratory
SFAX University, Tunisia
ahlem.kalai@gmail.com

Abdelghani Wafa
MIR@CL Laboratory
SFAX University, Tunisia
abdelghani_wafa@hotmail.fr

Corinne Amel Zayani
MIR@CL Laboratory
SFAX University, Tunisia
corinne.zayani@isecs.rnu.tn

Ikram Amous
MIR@CL Laboratory
SFAX University, Tunisia
ikram.amous@isecs.rnu.tn

***Abstract*—With the immense growth of online social applications, trust plays a more and more important role in connecting users to each other, sharing their personal information and attracting him to receive recommendations. Therefore, how to obtain trust relationships through mining online social networks became a critical issue. To calculate the level of trust between two users, many computational trust models are proposed which mainly rely on the social network structure, the explicit trust from user to another, the users' behaviors, or the users' similarity, etc. However, the majority of these models ignored the temporal factor. In this paper, we propose a trust relationship detection mechanism from an egocentric social network in order to compute the trust level between an active user and his directed friends. We propose a Level of social Trust model, that we called LoTrust, which is suitable for personalized recommendation purpose. This computational model founded on novel trust metric which is based not only on the users' interests similarity according to their semantic social profiles (RDF/FOAF), but also takes into account the time factor of the users' active interactions (e.g comments, share photo, wall posts, messages). We perform experiments on real life dataset extracted from Facebook. The experimental results demonstrated how our LoTrust model produces satisfactory results than other computational models.**

I. Introduction

The Web has dramatically evolved to an interactive and social environment called Web -based social networks (e.g Facebook[1], Twitter[2]). These Online Social Networks (OSNs) provide a space in which people can share information and can connect with one another. In this open environment, the user-generated content (e.g discussion, social profiles, video and photo feeds, reviews and ratings of anything) is very tremendous [11] and created by the different users' activities or behaviors. This content can be reliable or untrustworthy to the users. Despite all measures taken for privacy and security in OSNs, there is no certainty of trust [34]. For this reason, trust [10] [9] plays an important role in addressing both information overload and credibility problems [52] [37]. Trust is a filed research which has recently been attracting scientists from many domains including sociology, psychology, economics, and computer science [33]. In our research context, we are interested how detect and measure trust in OSNs. With so much user-interaction and user-generated content, the establishing of online trust mining mechanisms [52] is emerged in recent years. If trust can be detected accurately, the user can then use this trust to make decisions.

In social Web, trust is a complex concept influenced by many factors (personality and social) which online systems cannot yet model it completely [52]. In this context, some research work proposed a computational trust models [33] which can improve the social recommender systems [49]. Other existing work proposed a mining trust mechanisms from OSNs [52] [48]. The majority of these researches only rely on the network structure in order to generate trusted graph like TidalTrust [10], SWTrust [17], or based on the explicit trust like TrustWalker [16], Epinions[3]. For this reason, the accuracy trust inferring cannot be guaranteed due to lack of some relevant and proper information. Reputation of one another [19] [46], profile similarity [50] [5] [12], explicit rating (e.g. TidalTrust [30]) are frequently used information as influence factors which affect the trust between users. Since various OSNs support different types of social activities or interactions (e.g. tag photo, post comment, write on friend's wall, send message) which are performed by the users, some research studies [24] [22] [42] [29] [31] have then used these interactions as another factor to compute the social trust. One shortcoming of all of the above studies that they have neglected the time factor.

In reality, every interaction between two friends occurs at a given time, in a given situation (or context) and in a particular location. Therefore, the interactions change over time. Hence, the time is an important factor to capture the change in the behavior of an individual. Josang et al. [18] proposed to rank the friends by age of their social friendships and they considered the newer friends as the most trustworthy. On the contrary, Moghaddam et al. [27] are considered the older friends more trusted than newer ones. We think that these assumptions are not always valid depending on the

[1]http://www.facebook.com
[2]http://www.twitter.com
[3]http://epinions.com

interactions' type and its frequency for a period of time. Indeed, social trust level between two friends is influenced (increase or decrease) by their time aware- interactions degree. Some friends who used to be very close may no longer be and vice versa.

Different from the previous mentioned researches, we propose in this paper a trust level detection mechanism from an egocentric social network between the ego-user and his directed friends. This mechanism is based on social trust computational model that we called LoTrust. This model takes into account not only the common interpersonal interests which are extracted from the FOAF-based social profiles of the users, but also the temporal factor of their interactions.

The rest of this paper is organized as follows. Section 2 introduces a background of the trust concept (definition, properties, metrics, impact factors and computational models of trust). Section 3 exposes the three steps of our proposed social trust detection mechanism. Section 4, 5 and 6 details each step of trust detection mechanism. Section 7 exposes some experiments and the obtained results. Finally, we conclude by outlining our future works.

II. Related Work

Trust is a research field which has recently been attracting scientists on specific domains (i.e academic, computer science [33], sociology and psychology [24], etc.). The trust relationships between users is often utilized as an important basis for many applications, such as distributed systems, social recommender system, and in social web applications (e.g Web based social networks, online social media sites). In this paper, we are interested in trust in OSNs. In this section, we introduce an overview of some definitions, properties of trust and the existing metrics from the literature. Next, we will present some impact factors and trust computational models.

A. Trust Definitions

Many definitions have been developed by different research works but no definitive model has prevailed. In [18], trust is defined as *the belief of a person named confident that another called credible who has a competence and willingness to cooperate to accomplish a task in favor of confidence*. In [51], trust is defined as *a universal rating associated to the user to measure his reliability or his usefulness*. The definition given in [41] is *trust which is a cumulative value inferred from several interactions*. In [33], trust is *a measure of confidence that an entity will behave in an expected manner, despite the lack of ability to monitor or control the environment in which it operates*.

According to these definitions, trust is a subjective notion which is represented by a value and can change over time. It depends on the users' interactions and reflects their competences, their willingness, their reliabilities and their usefulness. The value of trust was measured in several ways depending on the properties which are considered. The next section points out to the important properties of trust.

B. Trust Properties

Although there is no precise definition in the literature, there is an agreement on the properties of trust which play an important role in trust modeling. We enumerate in this paper some properties, such as:

- Personalization or Subjectivity. Trust is considered a personal opinion [9] which based on various factors. Hence, the subjective nature of trust leads to personalize the trust computation, where the preferences and the interactions among users have a direct effect on the trust level value.
- Asymmetry/Symmetry. Trust is naturally asymmetric [14] [49] which means that for two persons involved in a relationship, trust is not necessarily identical in both directions. This is evident in our real life because the individuals have different experiences, psychological background, histories. It reflects a specific type of personalization. However, when both persons are trustworthy, they will converge to high mutual trust after repeated interactions [33].
- Transitivity or Propagation) /Non-transitivity. Because of trust is propagative nature [9], trust information can be passed from one member to another in a social network, creating trust chains. In other words, if a user X accepts a user Y to recommend him some items, so, why would not X accepts Y to recommend him/her a friend Z that he considers trustworthy. In addition, the trust transitivity can work in two ways [9]: a person can maintain two types of trust in another person: (i) trust in the person, and (ii) trust in the person's recommendations of other persons. However, in [46] trust is not perfectly transitive because a user X can not trust the stranger Z (i.e the latter who do not has a direct link with a user X).
- Explicit/Implicit. Explicit trust denotes the trust values explicitly indicated by their users [30] [9] [16]. Each time two users interact, they exchange their friends lists. Hence, we find that asking a user to evaluate each member of the network may be a tedious task. Moreover, the experience actually shows that few users feel bothered to accomplish this task. While, the implicit trust refers to the trust inferred from some evidence such as feature similarity among users [50] [5], their behaviors [24] [31], the age of their relationships [18] [27].
- Direct/Indirect or Recommended/Hybrid. Direct trust is based on the direct experience or interactions of the member with other party [47]. The indirect trust is based on experiences of other members in the social network with the other party. For example, A trusts B and B trusts C, we can infer that A trusts C. In this level, indirect trust based on the propagative property [9]. Recently, [47] propose a hybrid trust degree model which combine the direct and indirect relationship in social network.
- Dynamic. A user trusts in another only reflects his beliefs at a static point in time [49]. In fact, trust is not a static concept which changes (increase or decrease) over

time [35]. This change is often called trust dynamics [45]. Then, trust may decay with users interactions or observations [28] [33].

- Context-dependency. Trust level towards an individual can be varied based on time, situation, experience, and also a specific domain [48]. In [35] [33], trust is specified in a particular context which any information that can be used to characterized the situation of an entity. Suppose a user X in the community trusts another user Y for a given purpose (e.g. recommendation of movies). This does not automatically mean that X trusts Y for a different purpose or at a different time (recommendation of restaurant, heart surgery). Furthermore, the trust value between two persons can be different in different contexts [23] [44].
- Generic/specific-situation. Trust differs according to each individual in a certain situation. In the multi-agent research area, [24] proposed two types of trust concept: (i) A general trust on the evaluated agent without taking into account any situational hint, (ii) A situational trust depends on the situation in which the agent is evaluated. The latter has the most importance in the cooperative situations. In e-business field, [40] proposed a computational trust model for business agents in order to better assist them in the selection of partners decision in global marketplaces.

In the next section, we will present the types of the values and metrics of trust.

C. Trust Measurement

In social network scenario, trust relationship is based on the social connection between trustor and trustee. There are various ways to the different degrees of trust [14] [19]. In [4] a good state of the art related to different measurement are detailed. Thereafter, we cite two measures: (i) The trust value can be a set of binary values 0 and 1; or (ii) a continuous range like [0,1]. The binary values indicate that the person be trusted another or he untrusted to him like in Epinions site. We think that the choice of these values is very restrictive and we can not be used to rank the trust degree between people. This type of trust values does not give a precision degree for the trusted friend. However, other researches [24] [30], FilmTrust [9] proposed scaling trust in continuous range [0..1].

In addition, there are trust metrics which compute how much a user should trust another user, based on the other trust relations between other users in the network. Two types of trust metrics exist in the literature [32] [30] [9]. These metrics are classified in global and local metrics. (i) A global trust computes a universal trust value for each person in the network. Regardless of who asks for a trust recommendation, the same answer is given. It is defined as a value representing the reputation of a user. Hence, the trust value is computed without taking into account the personal bias but require the entire trust network information. Otherwise, (ii) a local trust calculates the trust from the perspective of the person asking for the trust recommendation. Essentially, the results are personalized for each user [25]. It is defined as a value assigned by a person to another according to ones knowledge to the latter. This knowledge is generally the result of interactions and differs from a user to another. Hence, the local metric returns a subset of the most trustworthy peers from the point of view of the trustor by taking into account the personal bias.

In our research work, we are interested in local trust metric in order to provide more personalized results. The proposed metric can be exploit in the purpose for any domain (e.g. Service computing, E-Learning, E-Commerce, E-Health, etc.) of social recommender system to make recommendation of any thing (i.e, friend, product, resource, service, media). The latter is part of our future works which related to Web Service recommendation in order to enhance our previous work [20]. In the next section, we will present some indicators that influence in the trust computation.

D. Trust Impact factors

In the social Web, trust is a composite [12] [4] or complex [35] relationship which is based on a wide range of factors [9]. Between two individuals, trust may be affected by their history of interactions, similar in preferences, interests, demographics information, etc. [52] identified four qualitative factors that influence the social trust formation such as the personality, relationship, knowledge, similarity and reputation. These factors can be mapped into some measurable feature values that can be used to compute or predict future trust relations. In addition, we have paid attention to the time as another factor that influence the trust level between users. A description of these factors is shown as follows.

- Personality factor refers to the users' individual traits that lead to expectations about the ones trustworthiness, like trust propensity [1], user gregariousness [52]. If an online user has a high tendency to trust others in general, this disposition is likely to positively affect his or her trust in a specific trust party.
- Relationship factor refers to the trust building mechanism which relies on qualitative assessments based on connections found in OSNs.
- Reputation factor refers to the trust building mechanism in which trustee behavior in the whole system affect the amount of his trustworthiness. In [33], the reputation utilize the user experience as the main source of trust information. The experience describe the perception of the members in their interactions with each other and it may affect the attitudes or behaviors of users. In [52], the reputation reflects the user popularity which is based on the positive and negative links that the user receives from others in trust network structure. In [8] proposed to calculate trust values on the basis of the actions performed by the user in OSN, and the type of content being posted. Thereby, the user is responsible for his/her reputation in the OSN world. This will enable the users to decide which content is reliable and which user is credible.
- Knowledge factor refers to the trust building mechanism where individuals get to know each other through in-

teractions and then predict others behaviors based on the information they obtain from this interactive process. Therefore, trust depends on the individual's behavior [29] [33] which is identified by patterns of interactions (or activities/actions). There are two types of interactions: *active* and *passive* [29] or *positive* and *negative* [39].The active interactions include having a large number of friends like commenting, liking, sharing a post, and tagging on an image, posting a video and so on. The passive interactions include reading posts or articles, regular visits to the community, etc. Therefore, the frequency and the type of interactions are important indicators of social trust between friends in the social networks [31] . [24] proposed a trust model which is based only on the direct interactions between two agents.

- Similarity factor refers to the trust building mechanism which implies that trust is established based on social similarities [2] such as common characteristics the trustor perceives of the trustee. These characteristics can be mined from the users' profiles which include the information related to interests, preferences, and demographic [12]. In [50], there is a strong correlation between trust and interest similarity. In fact, the users prefer suggestions come from others with similar tastes, preferences, interests and affinities. Likewise, they prefer in priority the recommendations that come from closest friends [30] [16] who have for example: a proximity in age, live (i.e same country), hobbies (i.e listen to the same music). Different metrics such as Cosine, Pearson Correlation, Jaccard Coefficient can be exploited.
- Time factor refers to the trust changes over time owing to experience from the outcome of interactions between the trustor and trustee. Therefore, trust is a dynamic concept [35] [43] [45] [33] (See section II-B). This dynamicity can be capture through the variation users' interactions according the time. For example, [18] introduced a forgetting factor and affirmed that the old feedback may irrelevant and become obsolete with time; and they assigned a less weight to the old feedback. [27] proposed a novel approach for measuring trust among users which is based on the friendship age. They believe that older friends are more trusted than newer ones. [22] are also considered the time difference between two users respective actions which form the connection. [3] apply a time window concept on the interactions between users.

In our Work, we are interested in three factors such as the interaction-based knowledge factor, the time factor and the interests-based similarity factor. In the next section, we discuss some computational trust models which are proposed in literature.

E. Computational Trust Models

Trust has been applied to enhance the decision-making process in various domains (e.g. Artificial Intelligence, Human-Computer, Interaction, Networking and Network Security, etc.) [4]. [24] addressed the issue of formalizing trust as a computational concept. His proposed model is complex and it is highly theoretical difficult to implement. In [14], modeling trust for computation use is difficult, particularly when working in the OSNs. In literature, various computational trust models have been proposed and they can be categorized into three general groups such as trust evaluation, trust propagation and trust prediction models [52].

- Trust evaluation models have been popular in estimating the users trustworthiness in large-scale distributed systems such as P2P application by developing the trust scoring system. The evaluation model can be categorized on three models [33], such as as Network-based trust model (i.e exploits the social network structure) [51], Interaction-based (i.e exploits the users' interactions patterns) [22] [29] and Hybrid model (i.e uses both users' interactions and network structure) [39] to compute social trust.
- Trust propagation models focused on developing a trust inference model which propagates trust values through a Web of Trust (WoT) [13]. Transitivity property of trust is considered as a base for trust calculation in these models especially in the OSNs [14] [25].
- Trust prediction models represent a body of trust model research that used existing prediction methods to assign trust class labels and weights to candidate user pairs [22] [52] [7]. Trust prediction based on classification techniques is relatively under explored in contrast with much research works already have been done in trust propagation. Statical techniques (Bayesian systems, beliefs models) and machine learning (Artificial Neural Networks, Hidden Markov Model) [52] focus on providing a mathematical model for computing and predicting trust. But, both of these solutions are highly complex.

In our work, we are interested in trust evaluation model which is based on three impacts factors previously presented (See section II-D). In the next, we will detail our proposed mechanism for capturing social trust from egocentric (i.e. personnel) OSN (e.g Facebook).

III. Social Trust Detection Mechanism

Generally, the OSNs are widely used by the large public and provide, therefore, a large volume of data (personal information (age, country), interactions (messages, comments), interests (music, sport), preferences, etc.). The majority of trust mining research from OSNs neglect these data and they based only on the network structure similarity by using the distance metric [30] [16]. However, in our work, we proposed to exploit the richness of user- generated content and users' interactions to detect or capture the social trust.

To perform this mechanism, we proposed in the first level, the knowledge extraction process from social data [38] which is detailed in the experimentation level (See section VII-A). In the second level, we apply our trust detection mechanism from an egocentric social network of an active user. This mechanism

takes as input the user-ego 's profile and it based on three steps that we we will detail in the next sections.

1) The egocentric social network analysis consists in analyzing the user's profile in order to extract the useful information.
2) The trust level computation consists in calculating for the active user (ego) the level of social trust with his directed friends based on the trust model that we called *LoTrust*.
3) The trusted friends filtering consists in selecting dynamically the most trusted friends for an active user according to the dynamic trust threshold that we defined.

Finally, our mechanism returns a trusted egocentric network which represented by a Trust Matrix. The latter can be used as the main input into a social recommender system [21] [15] [36] that we envisage to integrate it in our previous works [20].

IV. Egocentric Social Network Analysis

With the emergence of the Web 2.0, many users can interconnect together in OSNs and make social relationships (coworkers, family relationship, friendship, financial transactions, common interest). These relations are created on the basis of the users interactions (chat, share media, tagging, etc). From, this step we propose to analyze the user's social profile [26] in order to extract the useful information. In [6], two approaches of the Social Networks Analysis (SNA) are distinguished. The *socio-centric* approach (or complete network) focuses on all actors and all the links. The *ego-centric* approach (or personal network) focuses on the network surrounding one actor (ego) and his links. In this paper, we focus on egocentric analysis to detect and calculate the social trust from the individual' side. In this section, we identify the egocentric social network structure in the first part. In the second part, we detail the social profile modeling.

A. User's Profile Modeling

In general, a user's social network is viewed as a graph of *nodes* and *edges* where the nodes represent the users. Each user's node is described by its profile that contains information about the user's characteristics. The edges represent the links which define the type of social relation (e.g friendships) between the users. From this profile two types of information could be extracted. The *permanent* information which refers to the personal data (e.g. name, age, country, city). The *dynamic* information which refers to evolved data such as interests, preferences, links that define the social relationships (e.g. friendship, business) between users or groups' interactions (e.g social activities), etc.

B. User's Profile Representation

From our research, some languages exist to represent the structure of social networks such as RDFa[4], Microformats[5], XFN (XHTML Friends Network). Nevertheless, the concepts of WoT [13] or FOAF (Friend-Of-A-Friend)[6] has become a widely accepted vocabulary to describe people (personal information, links between them, any things they create) in many large OSNs like Facebook, Live Journal[7]. In addition, it is used to produce Semantic Web profiles for their users [13]. Indeed, in our work, we opted for RDF/FOAF as a common representation of the users' social profiles which represent the personal and the structural data. Moreover, we choose to represent the users' interactions by a vector which contains the type of each interaction (e.g. message, comment or post, etc.), the date and the involved friends. In the next section, we will detail the trust computation step.

V. LoTrust Model

This step consists in computation for an ego user his trust value towards his directed friends according to the Level of social Trust model, that we called LoTrust. We detail in this section the properties, the impacts factors and the proposed metrics to calculate the trust level.

A. Properties and Influence Factors

To perform the trust model, we have based on some properties: trust is personalized, asymmetric, non-transitive and dynamic. We adopt a local metric which varies from one user to another. We also propose that the trust level is a quantified value which is correlated with two impact factors as follow.

1) **Time-aware interaction** (See section V-B1). The OSNs enable the users to communicate via various social activities, such as sending messages, posting comments, wall posts, sharing photo, etc. Therefore, we consider that these active interactions according to time factor can provide information on the relationship strength between a pair of users and can reflect how much they are close in the period of time.
2) **Interests similarity** (See section V-B2). Trusting someone does not necessarily mean sharing the same preferences or interests with him [50]. Indeed, trust may include some information about personal identity and depends on the users' profiles similarity for evaluation. Therefore, we consider that the personal interest is a key point that keeps online users to form a connected group in the OSNs. Hence, the users who share common interests are more inclined to form trust relationships.

B. Proposed metric

We define the social trust level as measured value of trust to discriminate between trusted and untrusted friends from an egocentric network. Our LoTrust model is an aggregating of two values which are defined above (See Section V-A). Compared to the existing models [29] [31], our model takes into account the temporal factor to compute the interaction degree between users. In this section, we detail the metric for each factor and the trust global measure.

[4]http://www.w3.org/MarkUp/2009/rdfa-for-html-authors
[5]http://microformats.org/wiki/what-are-microformats
[6]http://xmlns.com/foaf/spec/
[7]http://www.livejournal.com

1) Time-aware Interaction Degree: Based on the egocentric network analysis of each ego-user (See section IV), we propose to represent by a vector all the types of social interactions by specifying the activity type (comment, message, etc.), the date and the involved friends who have direct connection with the ego. We rely on the assumption that the closest users frequently interact. Therefore, we use the interaction degree between users as a relevant value. To take into account the time factor influence, we suggest calculating, in the first level, the number of interactions (NI_f) between the ego and his friend u_j in the period of time Δ_t (e.g. for each month, year) according to equation (1).

$$NI_f(ego, u_j, \Delta_t) = \sum_{a_{ego,u_j}(\Delta_t) \in VA} k \tag{1}$$

Second, we calculate the total number of interactions (NI_{all}) of the ego, with all his friends in the same period Δ_t according to equation 2.

$$NI_{all}(ego, \Delta_t) = \sum_{u_l \in F(ego)} NI_f(ego, u_l, \Delta_t) \tag{2}$$

Finally, The time-aware interaction degree measure $DoI(ego, u_j)$ is calculated according to equation 3.

$$DoI(ego, u_j)_{\Delta_t} = \frac{NI_f(ego, u_j, \Delta_t)}{NI_{all}(ego, \Delta_t)} \tag{3}$$

where Δ_t is the period between the first interaction date and the current date between ego and u_j.

2) Interests Similarity Degree: In social network, each user is usually characterized by his semantic social profile (i.e RDF/FOAF ontology). Indeed, we utilize a SPARQL Query language in order to extract the interests for each friend from his/her profile. the obtained list are used to compute the degree of similarity $DoS_{interest}$ between two users by using the Jaccard similarity coefficient. This measure is based on the comparison of the common interests of ego and u_j. We count the number of common interests in both users and the total number of interests. For each pair of nodes (ego,u_j), the degree of similarity $DoS_{interest}(ego, u_j)$ can thus be calculated as shown in equation 4.

$$DoS_{interest}(ego, u_j) = \frac{\left\| interests_{ego} \cap interests_{u_j} \right\|}{\left\| interests_{ego} \cup interests_{u_j} \right\|} \tag{4}$$

With $DoS_{interest}(ego, u_j)$ is in interval of [0,1].

If $DoS_{interest}(ego, u_j)$= 1, it indicates that the user u_j is similar to his friend ego while $DoS_{interest}(ego, u_j)$ = 0 indicates that the user u_j completely different to his friend ego.

3) Global Trust Score: The social Trust level $LoT(ego, u_j)$ is calculated by equation 5. $LoT(ego, u_j)$ in interval of [0,1] denote the trust value that user ego assigns to friend u_j. If $LoT(ego, u_j)$= 0, it indicates that user ego completely distrusts his friend u_j while $LoT(ego, u_j)$=1 indicates that user ego completely trust his friend u_j. Once the level of social trust applied to all the friends of the user ego, the obtained values of trust will be stored in a Trust Matrix (Users $\times$ Users).

$$LoT(ego, u_j) = \alpha \times DoI(ego, u_j)_{\Delta_t} + \beta \times DoS_{interest}(ego, u_j) \tag{5}$$

where $DoI(ego, u_j)_{\Delta_t}$ is the interaction degree over time, and $DoS_{interest}(ego, u_j)$ is the interest similarity degree, with α and β are in the interval of [0,1] and β= 1-α.

VI. Trusted Friends Filtering

We propose, according to the obtained values in the previous step (See section V-B3), to select only the most trustworthy ego's friends. We know that the trust between two friends is dynamic since it depends on the change in their interaction frequency in time. In fact, in the recommendation purpose, the list of trusted friends differs from a user to another. For this reason, we propose a dynamic threshold γ that adapts to each user instead of using one static threshold (e.g. [20]) that will be used for all the users. Hence, the best trusted friends of the user-ego will be recommended where the level of social trust $LoT(ego, u_j) \geq \gamma$, and the threshold γ is calculated according to equation 6.

$$\gamma = \frac{\sum_{distinct(t_j) \in T_i} t_j}{j} \tag{6}$$

with T_i is the list of trust values of u_i to all his friends and distinct(t_j) is the list of distinct values in T_i

In the next section, we will detail the experiments and the obtained results.

VII. Experiments

In our work, we proposed a novel social trust model (LoTrust) based on the interest similarity and the degree of social interaction that depends on the time factor. In our experimentation, we choose the messages as more active interaction between the users in OSNs. The trust level between users that we proposed is implicitly calculated and does not require the user's intervention. We conducted two different types of evaluation:

- *Subjective evaluation.* Our goal is to validate, on the one hand, the contribution of aggregating social interactions and interest similarity by evaluating the choice of the best parameters α and β. On the other hand, intend to evaluate the contribution of using dynamic threshold γ rather than static threshold.
- *Objective evaluation.* Our purpose is to calculate the precision and recall of obtained results by our trust detection mechanism which performs the LoTrust.

In next subsections, we describe the used dataset and evaluation metrics.

A. Social Data Extraction

Access to data from OSNs is one of the main challenge of SNA. We use Facebook as a popular real-world social network.

Nevertheless, the Facebook API [8] is increasingly regulated and data collection options become very limited. For this reason, we have used another solution that we permit to download an archive file[9] of social data for each friend under his permission. This file contains the HTML Web pages of various types of information about each user. The user' information describe his/her permanent data (e.g name, age, country, etc.), his/her dynamic data like: interests (e.g music, sport, etc.), preferences, social activities (e.g messages, comments, loved pages, etc.), network structure data (user's friends list) and confidential data (e.g address, phone number, message content, notification setting, active session). Then, we apply the Web mining technique to extract useful data such users' interests and interactions.

For evaluation purpose, we choose an egocentric social sub-network for an user from Facebook which contains in total 1326 nodes (direct and indirect friends). From this sub-network, we have the opportunity to collect the social data for only 20 users. After that, we invited each user to connect in our social trust detection system in order to select and save his real trusted friends. Finally, we conducted a comparison between obtained results by using some metrics which are provided below.

B. Accuracy Metrics

We used three popular metrics, such as Recall, Precision and F-measure. In our context, the recall corresponds to the number of trustworthy friends who are returned by the system compared to the total number of real trustworthy friends who are identified by each user as shown in equation 7.

$$Recall = \frac{Nb_{returnedtrustedfriends}}{Nb_{Realtrustedfriends}} \quad (7)$$

The precision is the number of real trustworthy friends who are returned by the system compared to the total number of returned friends as shown in equation 8.

$$Precision = \frac{Nb_{returnedRealtrustedfriends}}{Nb_{returnedfriends}} \quad (8)$$

The F-Measure is a combination of the two previous metrics as shown in equation 9.

$$F - Measure = \frac{2 \times Recall \times Precision}{Recall + Precision} \quad (9)$$

C. Experimental Results

In this section, we analyze the obtained results by subjective and objective evaluations.

1) Setting parameters α and β: The social trust level is based on the time-aware interaction degree and the interest similarity between the users (See equation 5). In figure 1, we found that the best value of F-measure is the one with parameters: $\alpha = 0,8$ and $\beta = 0,2$. This mean that the temporal factor of the users' interactions has an important influence on the trust level. Consequently, we observe that if parameter α is closer to 0 and parameter β is closer to 1, the trust level decrease over time.

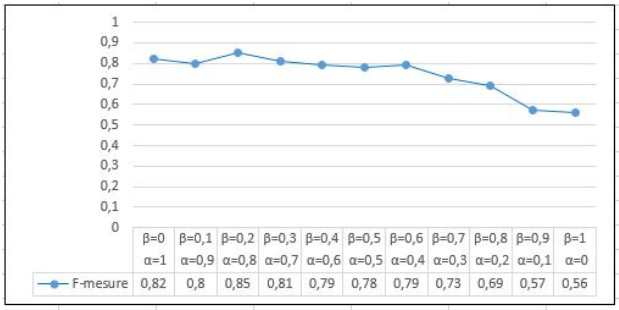

Fig. 1. Obtained results of F-measure with variation of α and β parameters.

2) Impact of dynamic trust threshold γ: We suggest that the accuracy of the returned results depends highly on the chosen threshold. In our social trust detection mechanism, we used three static thresholds (λ=0,5, 0,6 and 0,7) and the proposed dynamic threshold γ to filter the current user's friends. In figure 2, we observe that every time we increase λ (=0.6 or 0.7), the chance of selection of trusted friends (i.e number of friends) is reduced. Otherwise, if we decrease λ (=0.5), some friends will be chosen and recommended to the ego user. According to these results, we observe that for the majority of users, the selection of trusted friends by γ is much better than λ.

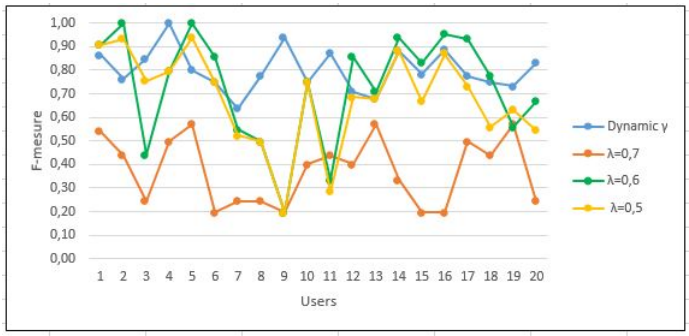

Fig. 2. Obtained results of F-measure with variation of static threshold (λ=0,5, 0,6 and 0,7) compared to the dynamic threshold γ

In addition, we note that static threshold has better results for some users and less for others. Thus, we proved with this assessment the interest of using a dynamic threshold in order to select the trusted friends from a large number in social network.

3) Comparison with other trust models: We compared the obtained results of our LoTrust model with some of two other models. The first model called Temporal Trust [27] which was proposed to rank the user' friends according to the age of their relationship by considering the newest friends as the most trustworthy. The second model called Closest Friends [31] which is based on social interactions between friends without considering the time factor. In general, the results obtained in terms of precision and recall show better results by taking into

[8]https://developers.facebook.com/docs/marketing-api/using-the-api
[9]https://www.facebook.com/help/131112897028467/

account the temporal factor on the users' interactions and the interests similarity (See figure 3 and 4).

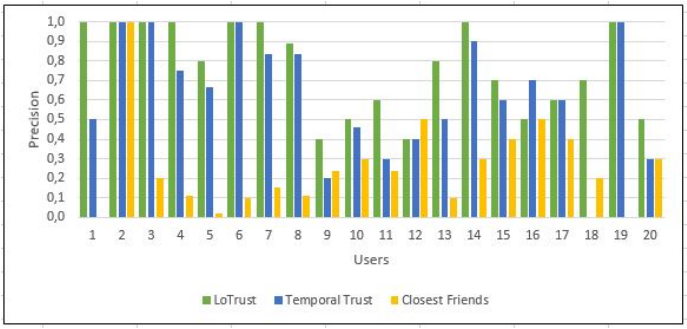

Fig. 3. Comparison of obtained results of our LoTrust model in terms of precision with two models: Temporal Trust model and Closest Friends model.

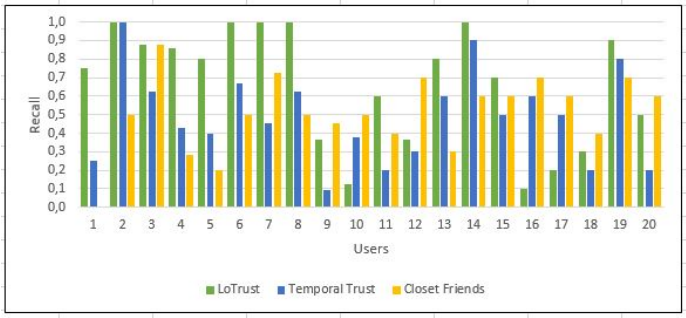

Fig. 4. Comparison of obtained results of our LoTrust model in terms of recall with two models: Temporal Trust model and Closest Friends model.

In figure 3, we found that the precision of the obtained results by the Closest Friend model is very low (precision average= 25,85%) than LoTrust model (= 76,94%) and Temporal Trust model (= 62,72%). This justifies our hypothesis that the non-consideration of the time factor may recommend to the user ego the friends who were considered trusted in the past and they are no longer. In addition, our model LoTrust gives better precision values than those obtained by the Temporal Trust model with a difference of 14,22% of the average precision. This first justifies that our model detect and recommend for each user the real trusted friends who are identified by each user, and second, the time- aware of the social interaction degree has a very strong impact than the age of relation (newest or oldest) which is taken into account in Temporal Trust model.

In figure 4, we found that the recall average of the obtained results by our LoTrust model is much better (=66,17%) than the Closest Friend model (= 50.71%) and Temporal Trust model (= 48.58%). This justifies that our model detects and recommends the trusted friends from the real trusted friends who are identified by each user.

VIII. Conclusion and Future work

In this paper, we presented a method for capturing trust relationships automatically from OSNs. We have proposed a new model called Level of social Trust (LoTrust) to compute the trust level between users by taking into account the social data extracted from the egocentric network for a given user. Our proposed trust metric is a local score which computed from the values of two measures: time-aware interaction degree and the interests similarity degree. According to the LoTrust model, our detection mechanism can recommend to an ego user only his best directed trusted friends.

The empirical results show that our proposed metric produces satisfactory results especially the consideration of time factor which has a positive influence on the trusted friends detection. In addition, the use of a dynamic threshold to discriminate between the users' friends produces more results than the use of a static threshold. Meanwhile, our LoTrust can be used in the social recommender system for different domains (E-commerce, Web service, etc.).

In our future work, we would like to improve our LoTrust model by taking into consideration another impact factor such as the Context of Trust.

References

[1] C. J. A, S. B. A, and L. J. A, "Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance." *Journal of applied psychology*, vol. 92, no. 4, p. 909, 2007.

[2] C. G. Akcora, B. Carminati, and E. Ferrari, "User similarities on social networks," *Social Netw. Analys. Mining*, vol. 3, no. 3, pp. 475–495, 2013.

[3] H. Charif, B. Anne, and R. Azim, "Time-aware trust model for recommender systems," International Symposium on Web AlGorithms, 2015, poster.

[4] J. Cho, K. S. Chan, and S. Adali, "A Survey on Trust Modeling," *ACM Comput. Surv.*, vol. 48, no. 2, p. 28, 2015.

[5] D. J. Crandall, D. Cosley, D. P. Huttenlocher, J. M. Kleinberg, and S. Suri, "Feedback effects between similarity and social influence in online communities," in *14th International Conference on Knowledge Discovery and Data Mining*, Las Vegas, Nevada, USA,, August 2008, pp. 160–168.

[6] A. D'Andrea, F. Ferri, and P. Grifoni, *Computational Social Network Analysis: Trends, Tools and Research Advances*. London: Springer London, 2010, ch. An Overview of Methods for Virtual Social Networks Analysis, pp. 3–25.

[7] T. DuBois, J. Golbeck, and A. Srinivasan, "Predicting Trust and Distrust in Social Networks," in *Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and Third International Conference on Social Computing (SocialCom)*, Boston, MA, USA, October. 2011, pp. 418–424.

[8] M. Gambhir, M. N. Doja, and Moinuddin, "Action-Based Trust Computation Algorithm for Online Social Network," in *Fourth International Conference on Advanced Computing Communication Technologies*, 2014, pp. 451–458.

[9] J. golbeck, "Computing with Trust: Definition, Properties, and Algorithms," in *Second International Conference on Security and Privacy in Communication Networks and the Workshops, SecureComm*, Baltimore, MD, Aug. 28 - September 1 2006, pp. 1–7.

[10] J. Golbeck, "Trust on the World Wide Web: A Survey," *Foundations and Trends in Web Science*, vol. 1, no. 2, pp. 131–197, 2006.

[11] J. Golbeck, Ed., *Computing with Social Trust*, ser. Human-Computer Interaction Series. Springer, 2009.

[12] J. Golbeck, "Trust and nuanced profile similarity in online social networks," *TWEB*, vol. 3, no. 4, 2009.

[13] J. Golbeck and M. Rothstein, "Linking Social Networks on the Web with FOAF: A Semantic Web Case Study," in *Twenty-Third Conference on Artificial Intelligence AAAI*, Chicago, Illinois, USA, July 13-17 2008, pp. 1138–1143.

[14] M. Golbeck, "Computing and Applying Trust in Web-based Social Networks," *Doctoral Dissertation, University of Maryland, College Park*, 2005.

[15] I. Guy and D. Carmel, "Social recommender systems," in *20th International Conference on World Wide Web, WWW (Companion Volume)*, Hyderabad, India,, March 28 - April 1 2011, pp. 283–284.

[16] M. Jamali and M. Ester, "TrustWalker: a random walk model for combining trust-based and item-based recommendation," in *International Conference on Knowledge Discovery and Data Mining*, Paris, France, June 28 - July 1 2009, pp. 397–406.

[17] W. Jiang and G. Wang, "SWTrust: Generating Trusted Graph for Trust Evaluation in Online Social Networks," in *10th International Conference on Trust, Security and Privacy in Computing and Communications TrustCom*, Changsha, China, 16-18 November 2011, pp. 320–327.

[18] A. Jøsang and R. Ismail, "The Beta Reputation System," in *15th Bled Electronic Commerce Conference*, 2002.

[19] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[20] A. Kala, C. A. Zayani, and I. Amous, "User's Social Profile - Based Web Services Discovery," in *8th IEEE International Conference on Service-Oriented Computing and Applications, SOCA*, Rome, Italy, October 19-21 2015, pp. 2–9.

[21] I. King, M. R. Lyu, and H. Ma, "Introduction to social recommendation," in *Proceedings of the 19th International Conference on World Wide Web, WWW*, Raleigh, North Carolina, USA, April 26-30 2010, pp. 1355–1356.

[22] H. Liu, E.-P. Lim, H. W. Lauw, M.-T. Le, A. Sun, J. Srivastava, and Y. A. Kim, "Predicting Trusts Among Users of Online Communities: An Epinions Case Study," in *Proceedings of the 9th ACM Conference on Electronic Commerce*, ser. EC '08. New York, NY, USA: ACM, 2008, pp. 310–319.

[23] X. Liu, *Towards Context-Aware Social Recommendation via Trust Networks*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 121–134.

[24] S. Marsh, "Formalizing trust as a computational concept," *Ph.D, Department of Mathematics and Computer Science, University of Stirling, Scotland*, 1994.

[25] P. Massa and P. Avesani, "Controversial Users Demand Local Trust Metrics: An Experimental Study on Epinions.com Community," in *The Twentieth National Conference on Artificial Intelligence and the Seventeenth Innovative Applications of Artificial Intelligence Conference*, Pittsburgh, Pennsylvania, USA, July 9-13 2005, pp. 121–126.

[26] M. Mezghani, C. A. Zayani, I. Amous, and F. Gargouri, "A user profile modelling using social annotations: a survey," in *the 21st World Wide Web Conference, WWW (Companion Volume)*, Lyon, France, April 16-20 2012, pp. 969–976.

[27] M. G. Moghaddam and A. Elahian, "A novel temporal trust-based recommender system," in *22nd Iranian Conference on Electrical Engineering (ICEE)*, May 2014, pp. 1142–1146.

[28] S. Nepal, C. Paris, S. K. Bista, and W. Sherchan, "A trust model-based analysis of social networks," *IJTMCC*, vol. 1, no. 1, pp. 3–22, 2013.

[29] S. Nepal, W. Sherchan, and C. Paris, "STrust: A Trust Model for Social Networks," in *10th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom*, Changsha, China, 16-18 November 2011, pp. 841–846.

[30] M. Paolo and A. Paolo, "Trust-aware recommender systems," in *ACM Conference on Recommender Systems, RecSys*, 2007, pp. 17–24.

[31] V. Podobnik, D. Striga, A. Jandras, and I. Lovrek, "How to calculate trust between social network users?" in *20th International Conference on Software, Telecommunications and Computer Networks, SoftCOM*, Split, Croatia, September 11-13 2012, pp. 1–6.

[32] J. Rouchier, "Cognition and Multi-Agent Interaction: from Cognitive Modeling to Social Simulation ," *J. Artificial Societies and Social Simulation*, vol. 10, no. 4, 2007.

[33] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, p. 47, 2013.

[34] M. M. Singh and T. Y. Chin, "Hybrid Multi-faceted Computational Trust Model for Online Social Network (OSN)," *International Journal of Advanced Computer Science and Applications, (IJACSA)*, vol. 7, no. 6, p. 11, 2016.

[35] S. Staab, B. Bhargava, L. Lilien, A. Rosenthal, M. Winslett, M. Sloman, T. S. Dillon, E. Chang, F. K. Hussain, W. Nejdl, D. Olmedilla, and V. Kashyap, "The Pudding of Trust," *IEEE Intelligent Systems*, vol. 19, no. 5, pp. 74–88, Sep. 2004.

[36] J. Tang, X. Hu, and H. Liu, "Social recommendation: a review," *Social Netw. Analys. Mining*, vol. 3, no. 4, pp. 1113–1133, 2013.

[37] J. Tang and H. Liu, "Trust in social computing," in *23rd International World Wide Web Conference, WWW (Companion Volume)*, Seoul, Republic of Korea, April 7-11 2014, pp. 207–208.

[38] D. Tchuente, C. M. Canut, N. Baptiste-Jessel, A. Péninou, and F. Sèdes, "Modèle et techniques de dérivation de profils utilisateurs à partir de réseaux sociaux égocentrés," in *Actes du XXXème Congrès INFORSID*, 2012, pp. 207–222.

[39] S. Trifunovic, F. Legendre, and C. Anastasiades, "Social trust in opportunistic networks," in *IEEE Conference on Computer Communications Workshops, INFOCOM*. IEEE, 2010, pp. 1–6.

[40] J. Urbano, A. P. Rocha, and E. C. Oliveira, "A Situation-Aware Computational Trust Model for Selecting Partners," *Trans. Computational Collective Intelligence*, vol. 5, pp. 84–105, 2011.

[41] P. Victor, C. Cornelis, M. D. Cock, and P. P. da Silva, "Gradual trust and distrust in recommender systems," *Fuzzy Sets and Systems*, vol. 160, no. 10, pp. 1367–1382, 2009.

[42] B. Viswanath, A. Mislove, M. Cha, and P. K. Gummadi, "On the evolution of user interaction in Facebook," in *Proceedings of the 2nd ACM Workshop on Online Social Networks, WOSN*, 2009, pp. 37–42.

[43] F. E. Walter, S. Battiston, and F. Schweitzer, "Personalised and dynamic trust in social networks," in *ACM Conference on Recommender Systems, RecSys*, New York, NY, USA, October 23-25 2009, pp. 197–204.

[44] Y. Wang, L. Li, and G. Liu, "Social context-aware trust inference for trust enhancement in social network based recommendations on service providers," *World Wide Web*, vol. 18, no. 1, pp. 159–184, 2015.

[45] Z. Yan, *Trust Modeling and Management in Digital Environments: From Social Concept to System Development*. Hershey, PA: Information Science Reference - Imprint of: IGI Publishing, 2010.

[46] B. Yu and M. P. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," in *Cooperative Information Agents IV, CIA The Future of Information Agents in Cyberspace*, Boston, MA, USA, July 7–9 2000, pp. 154–165.

[47] J. Zeng, M. Gao, J. Wen, and S. Hirokawa, "A Hybrid Trust Degree Model in Social Network for Recommender System," in *3rd International Conference on Advanced Applied Informatics (IIAIAAI),*, Aug 2014, pp. 37–41.

[48] Y. Zhang and T. Yu, "Mining Trust Relationships from Online Social Networks," *Computer Science and Technology*, vol. 27, no. 3, pp. 492–505, 2012.

[49] X. Zhou, Y. Xu, Y. Li, A. Jøsang, and C. Cox, "The state-of-the-art in personalized recommender systems for social networking," *Artif. Intell. Rev.*, vol. 37, no. 2, pp. 119–132, 2012.

[50] C. Ziegler and J. Golbeck, "Investigating interactions of trust and interest similarity," *Decision Support Systems*, vol. 43, no. 2, pp. 460–475, 2007.

[51] C. Ziegler and G. Lausen, "Paradigms for Decentralized Social Filtering Exploiting Trust Network Structure," in *On the Move to Meaningful Internet Systems: CoopIS, DOA, and ODBASE, OTM*, Agia Napa, Cyprus, October 25-29 2004, pp. 840–858.

[52] K. Zolfaghar and A. Aghaie, "Mining trust and distrust relationships in social Web applications," in *IEEE International Conference on Intelligent Computer Communication and Processing (ICCP)*, 2010, pp. 73–80.