AAAI Technical Report SS-12-04
Intelligent Web Services Meet Social Computing

Which Social Networks Should Web Services Sign-Up In?

Noura Faci
Université Lyon 1, LIRIS, Lyon, France

Zakaria Maamar
Zayed University, Dubai, UAE

Parisa Ghodous
Université Lyon 1, LIRIS, Lyon, France

Abstract

This paper deals with the sign up issue in social networks populated with Web services. These social networks can be used for example, to ease the discovery of Web services. Based on Web services' functionalities three social networks are built: competition, substitution, and collaboration. In competition and substitution social networks, Web services offer homogeneous functionalities. In the collaboration social network, Web services that offer heterogeneous functionalities. In this latter type, Web services can be put together to develop composite services. Prior to joining a social network, a Web service through a third-party, named social Web service, should evaluate the pros and cons of being member in this network. A set of quality criteria for assessing these pros and cons are proposed. These criteria are, but not limited to, privacy, trust, fairness, and traceability. Policies for managing the sign up are, also, provided in this paper. The adoption and efficiency of these policies are monitored and assessed with respect to the values that these criteria take. In response to this sign up's outcomes, these policies are fine-tuned.

1 Introduction

Web services (WSs) are recognized for their capacity in developing loosely-coupled, cross-organization inter-operable applications. To sustain this recognition over other distributed computing technologies like CORBA, pending issues such as efficient discovery and better semantic matching that continue to hinder WSs acceptance need to be addressed. In a previous work (Maamar et al. 2011a), we embraced Social Networks (SNs) principles to put forward new solutions to address these issues and hence, boost the operation of WSs. The result is Social Web Services (SWSs) that can, for instance establish contacts with peers and count on privileged ones to help satisfy users' needs, e.g., recommending to expand their compositions with additional WSs. Based on WSs' functionalities three SNs are built (Maamar et al. 2011a): competition and substitution SNs are populated with WSs that offer homogeneous functionalities and collaboration SN is populated with WSs that offer heterogeneous functionalities. In this latter type, WSs can be put together to develop composite services. A brief overview of SNs development is given later.

In this paper we continue the efforts put into SWS development by examining criteria that can influence the sign up decision of a WS in a certain SN. After signing up, a SWS would like to avoid unfortunate events (e.g., attacks from competing peers) that could negatively impact its operation or to maximize its exposure to the external community. For this purpose we define four criteria namely *privacy*, *trust*, *fairness*, and *traceability* that allow a WS to assess the attractiveness of a SN in terms of safety and utility. These criteria characterize the quality of a SN. To assess these criteria we study different policies adopted in existing social networking online sites like Facebook for reducing the risks of exposure of their members. We define similar policies to cater for the particular needs, requirements, and characteristics of WSs.

Section 2 gives a brief overview of SNs and discusses SNs development. Section 3 addresses how SWSs select which SNs to sign up in, which policies are required for managing this sign up, how these policies are fine-tuned in response to this sign up's outcomes, and how these policies are illustrated. Prior to concluding some related works are provided in Section 4.

2 Background

2.1 Social Web services brief overview

Our research work on SWSs looks into the overlap between social computing (Web 2.0, (Kwak et al. 2010)) and service-oriented computing (WSs). Current research either considers WSs as services for user-centric SNs or develops WS-centric SNs.

In the user-centric SNs, we identify different approaches. Xie et al. propose a composition framework that relies on social based recommendations of semantic WSs (Xie, Du, and Zhang 2008). Wu et al. rank WSs using run-time non-functional properties and invocation requests (Wu et al. 2009). Ranking takes into account the popularity of a WS, considered as a social element and analyzed by users. Maaradji et al. propose an event-driven social composer to assist users take actions in response to events such as selecting a given WS (Maaradji et al. 2010). Lastly, Nam Ko et al.

discuss the way the social Web (exemplified by the well-known networking sites such as Facebook) contributes to create social applications without having to build social networks (Nam Ko et al. August 2010).

In the WS-centric SNs, we mention our previous works in (Maamar et al. 2011b) and (Maamar et al. 2011c). In the first reference we introduce a method for engineering SWSs. This engineering requires identifying relationships between WSs, mapping these relationships onto SNs, building SNs of SWSs, and setting the social behaviors of SWSs. In the second reference we weave the principle of SNs into WS discovery. SNs differ in the way they enable developers to describe situations in which WSs engage in, for instance collaboration and recommendation. We emphasize that WSs should not be treated as stand-alone components that respond to user queries, only. On the contrary, WSs permanently face competition and collaboration situations during selection and composition, respectively.

2.2 Turning Web services into social

Developing SNs of SWSs require six steps that range from identifying the components of a social network to working out the means that allow to navigate through this network (Maamar et al. 2011a). As stated earlier, there are three types of SNs: collaboration, substitution, and competition. The analysis of the last two in term of selection criteria is given in (Maamar, Faci, and Loo 2012). In this paper, we focus on the collaboration SN.

Step 1 - *Identification of a social network's components*

A SN's components refer to nodes and edges that respectively, correspond to WSs and interactions between WSs. A collaboration edge means that a WS that is part of an ongoing composition recommends to a service engineer to include extra peers in that composition. The service engineer either accepts or rejects the recommendation.

Step 2 - *Matching analysis of Web services*

To establish the collaboration relationship between WSs, their respective functionalities are matched. These functionalities describe a WS's profile in terms of preconditions and effects. WS_i and WS_j are potential collaborators (i.e., complementary) when WS_j's preconditions match WS_i's effects. We adopt Min et al.'s approach to establish the Degree of Complementary (DC) between two WSs (Min et al. 2009).

Step 3 - *Management of the social network*

The completion of this step requires a special type of node, which we denote by Web service root. It is defined with respect to two stages defining the life-cycle of a SN.

- Building stage: Any WS that will join a SN can be treated as a root. So, the selection is random. The rest of SWSs in the SN will be connected to this root.
- Exploitation stage: When a SN is built, and for a certain composition, any component WS in this composition can be a root. The objective is to look for its potential collaborators.

When a SN is built for first time SWSs are grouped into two clusters known as no-complementary and complementary. This happens according to the DC that a SWS has with the SWS root: when $0 \leqslant DC \leqslant 0.49$ for example, the SWS is placed in the no-complementarity cluster, otherwise the SWS is placed in the complementarity cluster (e.g., $0.5 \leqslant DC \leqslant 1$). It is noted that a cluster might already be populated with other SWSs. This placement process continues as long as SWSs are made available and agree to be part of a SN. While the clustering is in progress, the connection of the SWSs together in the SN is in progress as well, which leads to extending the SN.

Step 4 - *Initial evaluation of edge weights*

The initial value of the Weight of an Edge (WE) between SWS_i and SWS_j, where SWS_i is the SWS root, corresponds to the complementary degree between them.

Step 5 - *Navigation through the social network*

Appropriate means are required to help a SWS navigate through a SN. Each SWS root is an entry point to a SN. Looking for collaborators in a SN requires factors such as previous experiences and user needs.

Step 6 - *Ongoing evaluation of edge weights*

The ongoing evaluation reflects the role of the collaboration SN in discovering collaborator WSs. This happens by updating the edge weights each time a collaborative peer is discovered using this SN. Updating these weights can be based on reward-based price formulas (Yu et al. 2004) (Equation 1).

$$WE_{t+\delta t}(SWS_i, SWS_j) = WE_t(SWS_i, SWS_j) + \alpha \times \left(\frac{|SWS_j\ selection_{t+\delta t}|}{|SWS_i\ collaboration_{t+\delta t}|} - WE_t(SWS_i, SWS_j)\right) \quad (1)$$

where α is a constant between 0 and 1, δt represents the update period, $|SWS_j\ selection_t|$ is the number of times that SWS_j and SWS_i were engaged in collaboration following the use of SWS_i's collaboration SN at time t, and $|SWS_i\ collaboration_t|$ is the number of times that SWS_i was engaged in collaborations at time t.

3 Should Web services sign up into the collaboration social network?

3.1 Selection criteria

To support the sign-up decision we consider *privacy*, *trust*, *fairness*, and *traceability* criteria that WSs should take into account on top of the functionality criterion (other criteria can be used as well). We assume that an authority component (SN_{auth}) manages the SN that connects new SWSs to existing members in the network, assesses the weights of edges in the network, enforces the management policies of the network, etc. Policies are discussed in the next section.

By being part of a collaboration SN, a SWS knows the peers that it likes to work with in case compositions are to be built.

1. **Privacy**. A SWS needs to ensure that appropriate means in this network permit to secure its private details (e.g., non-functional properties (QoS)) since some of these details can be revealed by some un-trustworthy

members in the network. This puts the SWS in a vulnerable position when these details are revealed to other (competing) peers by these members. We measure the privacy level of a collaboration SN ($Privacy_{Col}$) by:

$$Privacy_{Col} = \min_{i \in [1,n]} (1 - \frac{|focussedRevelations_{SWS_i}|}{|Revelations|}) \quad (2)$$

where $|focussedRevelations|$ represents the total number of revelations that SWS_i was subject to and $|Revelations|$ is the total number of revelations affecting the SN.

2. **Trust**. A SWS needs to make sure that the peers it recommends for appending into ongoing compositions behave and operate as expected. We measure the trust level of a collaboration SN ($Trust_{Col}$) by:

$$Trust_{Col} = \min_{i \in [1,n]} (\frac{successfulRec_{SWS_i}}{Rec_{SWS_i}}) \quad (3)$$

where $successfulRec$ represents the number of recommendations that SWS_i made for other peers that accepted and behaved as expected and Rec is the total number of recommendations by SWS_i.

3. **Fairness**. Since SWSs are complementary, fairness is not relevant.

4. **Traceability**. It permits to keep track of the SWSs' operations and interactions so that the SN_{auth} can hold them accountable for these operations' and interactions' outcomes in case of conflicts (e.g., exchanging contradicting details) or irregularities (e.g., flooding the network with unnecessary details). The SN_{auth} can, also, analyze these outcomes to verify the quality of SWSs' self-details. This would increase the confidence level of the SN_{auth} in the SWSs in the network as well as the trust among these SWSs. Traceability process runs according to a certain frequency and for a certain duration over operations (op) and/or interactions (int). We measure the traceability level of a collaboration SN ($Trace_{Col}$) by:

$$Trace_{Col} = \frac{1}{2} * (\beta_{op} * freq_{op} + \beta_{int} * freq_{int}) * d \quad (4)$$

where $\beta \in \{0, 1\}$, $\beta_{op} + \beta_{int} = 1$, and $freq$ and d are frequency and duration parameters, respectively. Traceability value can be ranked as low, average or high with respect to some min and max values. For instance high traceability means that a SWS can rely on the SN_{auth} to generate an accurate trace of the operations that were executed. When the SN_{auth} detects irregularities, traceability permits for instance to pin down the responsible SWSs.

3.2 Management policies

In Section 3.1 we mentioned briefly the role of a SN_{auth} in enforcing the implementation of this network's management policies. This enforcement requires making the SWSs aware of the policies so they can first, avail of the network's benefits and second, comply with the policies to avoid violations and hence, penalties (Section 3.3). In this section we propose some policies per criterion for the collaboration SN.

Privacy ($privacyCol$). It aims at protecting the SWSs from the collaborator peers that attempt to collect their details in order to share them with unauthorized peers. The following policies propose ways of achieving this aim.

1. $P_{privacyCol,1}$: a SWS should label its details (e.g., with whom it collaborates heavily) as either private, protected, or public.
2. $P_{privacyCol,2}$: a SWS should only share the details that the collaborator peer needs before this peer is appended into a composition.
3. $P_{privacyCol,3}$: a SWS is penalized by the social network's SN_{auth} when it reveals details to non-members of this SN.

Trust ($trustCol$). It aims at ensuring that the SWSs have full confidence in the peers they recommend to append into ongoing compositions. The following policies propose ways of achieving this aim.

1. $P_{trustCol,1}$: a (collaborator) SWS should take part in a composition as agreed upon between the recommending peer, this SWS, and the SN_{auth}.
2. $P_{trustCol,2}$: a (collaborator) SWS should operate properly as expected by the recommending peer and SN_{auth}.

Fairness ($fairnessCol$). As fairness is not relevant to a collaboration SN, policies are not required.

Traceability ($traceCol$). It aims at tracking the SWSs' operations for quality assurance purposes. The following policies propose ways of achieving this aim.

1. $P_{traceCol,1}$: a SWS will be probed regularly by the SN_{auth} as part of the monitoring operations that this component performs.
2. $P_{traceCol,2}$: a SWS will be informed by the SN_{auth} about any necessary action that it has to take in response to this probing.

3.3 Linking criteria to policies

The purpose of linking criteria for SNs selection to policies for SNs management is to monitor and assess the adoption and efficiency of these policies with respect to the values that these criteria take (Equations 1−3). Indeed a low value for a certain criterion in a certain network can indicate the inappropriateness of other policies or the lack of compliance with some policies. Corrective actions are deemed appropriate such as reviewing some existing policies or developing new ones. In the following, we discuss the links between the aforementioned criteria and policies per type of criterion:

1. Privacy criterion is associated with three policies that refer to labeling SWSs' collaboration details, sharing these details between recommending and recommended (collaborator) SWSs, and penalizing recommended (collaborator) SWSs. A poor privacy level

(i.e., $Privacy_{Col}$ close to zero) raises issues like the appropriateness of these details for not disturbing the composition progress as stated in $P_{privacyCol,2}$ and the efficiency of the means that prevent revealing these details as stated in $P_{privacyCol,3}$. To improve the privacy level corrective actions consist of identifying the necessary details to share and guaranteeing that recommended peers are trustworthy.

2. Trust criterion is associated with two policies that refer to confirming the participation of recommended SWSs in compositions and guaranteeing the proper functioning of these recommended SWSs. A poor trust level (i.e., $Trust_{Col}$ close to zero) raises concerns about the confidence that the recommending SWSs have in the recommended peers as stated in $P_{truCol,1}$. To improve this level corrective actions consist of checking that recommended peers are trustworthy. We define two additional policies for penalizing the collaborators as follows:
   - $P_{trustCol,3}$: a (collaborator) SWS is penalized by the SN_{auth} when it deviates from its expected functioning.
   - $P_{trustCol,4}$: a (collaborator) SWS is penalized by the SN_{auth} when it does not take part in a composition as expected.
3. Fairness criterion is not related to any policy.
4. Traceability criterion is associated with two policies that refer to probing and advising SWSs by the SN's SN_{auth}. A poor traceability level (i.e., $Trace_{Col}$ close to zero) raises concerns about the quality of the monitoring means that this SN_{auth} uses as stated in $P_{traceCol,1}$ as well as the willingness of these SWSs in implementing the advices of this SN_{auth} as stated in $P_{traceCol,2}$. To improve the traceability level corrective actions consist of improving the monitoring means and warning the SWSs. We define two additional policies for punishing and promoting SWSs, respectively, as follows:
   - $P_{traceCol,3}$: a SWS is penalized by the SN_{auth} when the corrective actions (or advices) it recommends are not implemented by this SWS.
   - $P_{traceCol,4}$: a SWS is rewarded by the SN_{auth} when the corrective actions (or advices) it recommends are implemented by this SWS.

3.4 Illustration

The previous parts of the paper worked out three main elements that are, how SWSs use criteria to select which SNs they can sign up in (Section 3.1), how SWSs need to comply with the policies that manage these networks (Section 3.2), and how the assessment of these criteria permits reviewing these policies (Section 3.3). In the following we illustrate how all these elements are put into action a collaboration SN. We, also, adopt some techniques discussed thoroughly in the related-work section to address issues raised during this network use.

- Privacy is mainly assessed through the capacity of the collaboration SN to resist to attacks on SWSs' non-public details. Gao et al. discuss privacy breach attacks in the specific context of online social networks of persons (Gao et al. 2011). Breaches due to befriending users apply perfectly to SNs of SWSs. Indeed some malicious peers acting as friends require non-public details from a SWS. These peers may have some financial interests when revealing these details to other members of the SN. Gao et al. suggest to increase users' alertness concerning their acceptance of friend requests as a defense to these attacks, which seems to be appropriate for protecting non-public details of SWSs.
- Trust is mainly assessed through the capacity of the collaboration SN to recommend trustworthy SWSs. An untrustworthy SWS can alternatively increase and decrease confidence that other peers have in it, while keeping a reasonable reputation. Improvement measures could be (1) to inform members about this kind of oscillatory behavior or (2) to decrease the trust level of this untrustworthy SWS.
- Fairness criterion is not related to any policy.
- Traceability is mainly assessed through the capacity of the collaboration SN to provide accurate traces of all the operations and interactions that occur in this network. Inaccurate traces might lead into poor decisions made by the SWSs. Improvement measures could be (1) to increase the monitoring frequency and duration of the peers that are suspected to be the source of irregularities or (2) to apply probabilistic models for more accurate traces.

4 Related work

Characterizing SNs can be achieved through a new criteria-based model for assisting WSs decide whether or not they sign up in a SN. Similar models exist in other fields of research. They use $\mathcal{Q}$uality of $\mathcal{S}$ervice ($\mathcal{Q}$o$\mathcal{S}$) built upon non-functional properties. The literature review we carried out did not reveal explicit works on quality of SNs but rather aspects related to quality SN, software quality assessment using SNs, and relationship between quality of SNs and investment decisions.

In (Perego, Carminati, and Ferrari 2009) Perego et al. discuss the quality SN as part of a collaborative environment for personalizing Web access. The authors use social tagging to evaluate the quality of Web resources based on users' preferences and opinions. They examine safety and trustworthiness aspects of a SN. According to Perego et al., "*...the Web as a whole is still considered, by many, as a source of unreliable and untrustworthy information, thus preventing the exploitation of its full potentialities*". The quality SN provides end-users the possibility of associating labels with Web resources as well as using rates to express their dis/agreement on existing labels. The authors evaluate the members reachable through the networks but not the networks themselves.

In (Zuluaga 2010) Zuluaga analyzes the impact of the quality of SN on the educational decision making process. Though this work does not really fit into our vision of quality, it is worth mentioning that Zuluaga uses the schooling level and labor position of the members in a SN to establish the quality of the network. It was noted that the higher

the quality of the network, the higher the probability of investing in education will be. However, the authors do not consider the policies that regulate the SN and their impact on the quality of the SN.

In (Tonchev and Tonchev 2010) Tonchev and Tonchev look at SNs, e.g., Facebook and Twitter, from a quality perspective, which is in inline with our quality model. They insist that the popularity of SNs can sustain business growth subject to maintain a good $\mathcal{Q}o\mathcal{S}$. They address the notion of quality as applied to a SN and the way to evaluate this quality. The proposed set of criteria mainly includes conformance to specifications, access control and privacy. However, these criteria are not strictly formalized, through mathematical formulas for instance.

In (Dasgupta and Dasgupta 2010) Dasgupta and Dasgupta emphasize on the barriers that users have to overcome when they simultaneously sign up on different SNs. This leads to duplicate information, loss of privacy, and redundant information flow. Today's SN-based applications are almost the same in terms of features provided to users. To alleviate these negative consequences, Dasgupta and Dasgupta propose the Social Network as a Service (SNaaS) model considered as a kind of single counter offering specialized services such as blogging, mentoring, and community management. These services give access to specific SN-based applications, e.g., LinkedIn that concentrates on corporate SN aspects. However, users decide to sign up to specific SNs based only on functionality but not quality criteria.

5 Conclusion

This paper deals with the quality of social networks used to connect social Web services together. These social networks aim to improve the efficiency of Web service discovery. Prior to signing up in these networks, quality criteria were proposed such as privacy, trust, fairness, and traceability. These criteria can help Web services select the most appropriate social networks. We defined each criterion by emphasizing the intrinsic features of the collaboration social networks. Besides these criteria, we defined policies that guarantee the proper management of the social networks. Upon signing up in a social network, social Web services have to fully comply with these policies. The paper, also, discussed how the selection criteria of social networks and policies for their management are connected. The objective was to adjust the existing policies or call for new policy definition in some cases. Future work is to develop a proof-of-concept tool with several functionalities like simulate attacks and enforce policies per type of criterion.

References

Dasgupta, D., and Dasgupta, R. 2010. Social Networks using Web 2.0, Part 2: Social Network as a Service (SNaaS). Technical report, IBM, developerWorks.

Gao, H.; Hu, J.; Huang, T.; Wang, J.; and Chen, Y. 2011. Security Issues in Online Social Networks. *IEEE Internet Computing* 15(4).

Kwak, H.; Lee, C.; Park, C.; and Moon, S. 2010. What is Twitter, a Social Network or a News Media? In *Proceedings of the 19th International World Wide Web Conference (WWW'2010)*.

Maamar, Z.; Faci, N.; Krug Wives, L.; Badr, Y.; Bispo Santos, P.; and Palazzo M. de Oliveira, J. 2011a. Using Social Networks to Web Services Discovery. *IEEE Internet Computing* 15(4).

Maamar, Z.; Faci, N.; Krug Wives, L.; Yahyaoui, H.; and Hacid, H. 2011b. Towards a Method for Engineering Social Web Services. In *Proceedings of the IFIP WG8.1 Working Conference on Method Engineering (ME'2011)*.

Maamar, Z.; Krug Wives, L.; Badr, Y.; Elnaffar, S.; Boukadi, K.; and Faci, N. 2011c. `LinkedWS`: A Novel Web Services Discovery Model Based on the Metaphor of "Social Networks". *Simulation Modelling Practice and Theory, Elsevier Science Publisher* 19(10).

Maamar, Z.; Faci, N.; and Loo, A. 2012. "Towards a Quality of Social Network (QoSN) Model in the Context of Social Web Services. In *Third International Conference on Exploring Services Science, Lecture Notes in Business Information Processing*.

Maaradji, A.; Hacid, H.; Daigremont, J.; and Crespi, N. 2010. Towards a Social Network Based Approach for Services Composition. In *Proceedings of the 2010 IEEE International Conference on Communications (ICC'2010)*.

Min, L.; Weiming, S.; Qi, H.; and Junwei, Y. 2009. A Weighted Ontology-based Semantic Similarity Algorithm for Web Services. *Expert Systems with Applications* 36(10).

Nam Ko, M.; Cheek, G. P.; Shehab, M.; and Sandhu, R. August 2010. Social-Networks Connect Services. *IEEE Computer* 43(8).

Perego, A.; Carminati, B.; and Ferrari, E. 2009. The Quality of Social Network: A Collaborative Environment for Personalizing Web Access. In *Proceedings of the International Conference on Collaborative Computing: Networking, Applications, and Worksharing (CollaborateCom'2009)*.

Tonchev, A., and Tonchev, C. 2010. Social Networks: A Quality Perspective. Technical report, The Big $\mathcal{Q}$ Blog, http://www.juran.com/blog/?p=127.

Wu, Q.; Iyengar, A.; Subramanian, R.; Rouvellou, I.; Silva-Lepe, I.; and Mikalsen, T. 2009. Combining Quality of Service and Social Information for Ranking Services. In *Proceedings of ServiceWave 2009 Workshops held in conjunction with the 7th International Conference on Service Service-Oriented Computing (ICSOC'2009)*.

Xie, X.; Du, B.; and Zhang, Z. 2008. Semantic Service Composition based on Social Network. In *Proceedings of the 17th International World Wide Web Conference (WWW'2008)*.

Yu, B.; Li, C.; Singh, M.; and Sycara, K. 2004. A dynamic pricing mechanism for p2p referral systems. In *AAMAS'04: International Conference on Agents and Multi-Agent Systems*.

Zuluaga, B. 2010. Quality of Social Networks and Educational Unvestment Decisions. Technical report, Social Science Research Network (SSRN).