	SocEDA ***Cloud based platform for large scale social aware EDA*** ANR-10-SEGI-013	

Document name:	**Social Service Modeling – Overview of Activities, Proposed Framework, and Models of Social Concepts and Trust**
Document version:	**1.0**
Task code:	**2.1**
Deliverable code:	**D2.1.1**
WP Leader (organisation):	**LIRIS / INSA Lyon**
Deliverable Leader (organisation):	**LIRIS / INSA Lyon**
Authors (organisations):	• **Omar HASAN (LIRIS / INSA Lyon)** • **Sonia BEN MOKHTAR (LIRIS / INSA Lyon)** • **Lionel BRUNIE (LIRIS / INSA Lyon)**
Date of first version:	**2011-10-01**

Change control

Changes	Author / Entity	Code of version
Creation of the document	• **Omar HASAN** (LIRIS / INSA Lyon) • **Sonia BEN MOKHTAR** (LIRIS / INSA Lyon) • **Lionel BRUNIE** (LIRIS / INSA Lyon)	

Table of Contents

1. Introduction

The objective of the Task 2.1 (Social-Aware Event Modeling and Matching) is to establish a novel set of parameters based on social aspects that can be utilized by services for event subscription and event matching. The task can be subdivided into two activities: 1) Modeling social relationships between services and inferring trust between them based on these relationships. 2) Augmenting existing event processing models such that they allow services to use social and trust information for event subscription and event matching.

The aim of the first activity is to model the social relationships between services and to infer trust between them by analyzing their social relationships. We propose the following sub-activities to accomplish the goals of this activity: 1) modeling social relationships between services; 2) modeling trust between services; 3) developing a trust inference engine that utilizes the available social information to infer trust between services. We model the concepts of social networks, social relationships, and trust by identifying the various attributes that characterize them.

Some of the important characteristics of a social relationship that have been previously identified include: 1) the roles that are associated with the relationship; 2) the valence or the sentiments attached with the relationship, such as like or dislike; 3) the frequency of contact; 4) the duration or span of the relationship; 5) the trust or confidence that the nodes place in each other within various contexts; 6) the overlap in the social networks of the nodes.

We argue that trust is one of the most important indicators of the strength of a social relationship. Trust inherently accounts for many aspects of a social relationship such as the roles in the relationship, duration of the relationship, frequency of contact, valence etc. Trust can thus serve as a primary indicator of the strength of the social relationship between two services. We therefore propose to develop a trust inference engine that harnesses social information to infer the trust between services.

There are a number of methods that can be used to infer trust from information provided by others. These techniques include: 1) Trust recommendation and propagation, which takes advantage of the possible transitivity of trust. 2) Trust negotiation, which establishes trust between entities based on their properties. For example, the properties may include an individual's employer, their age, their membership in certain organizations, etc. 3) Reputation, which is the general opinion of the community about the trustworthiness of an entity.

The goal of the second activity is to enable services to subscribe to events and match events based on the aspects of their social relationships. The social and trust infrastructure established in the first activity would allow us to create novel parameters based on social relationships for event subscription and matching.

2. Overview of Activities

In this section we present an overview of the activities that are to be undertaken as part of this task.

2.1. Activity 1: Inferring trust between Services from their Social Relationships

This activity corresponds to the deliverable D2.1.1 of this task. The aim of the activity is to infer trust between services by analyzing their social relationships. We propose the following sub-activities to accomplish the goals of this activity: 1) modeling social relationships between services, 2) modeling trust between services, 3) developing a trust inference engine that utilizes the available social information to infer trust between services.

2.2. Activity 2: Social and Trust based Event Subscription and Matching

This activity corresponds to the deliverable D2.1.2 of this task. Our goal in this activity is to enable services to subscribe to and match events based on social parameters. The social and trust infrastructure established in the first activity would allow us to create the social parameters to be used by services for event subscription and matching.

3. The Proposed Framework

3.1. General Framework

Our proposed framework that demonstrates the interaction between different elements is presented in Figure 1.

Our first step is to develop a model for social relationships between services. This model would allow us to describe the social relationships between services and to evolve a rich social network. We argue that trust is an important indicator of the strength of social relationships. Trust inherently accounts for many aspects of a social relationship such as the roles in the relationship, duration of the relationship, frequency of contact, valence etc. We therefore propose to extract trust information from the social network of services. We propose to develop a *trust inference engine* that would infer the trust between any given services. The trust inference engine may be more generally termed as the *social relationship strength inference engine* or concisely as the *social filter*.

As shown in Figure 1, the social filter would translate a social network into a web of trust thus inferring the amount of trust between all adjacent nodes in the social network. As shown in Figure 2, the social filter may also perform the more specific task of inferring trust between specified pairs of nodes. The social filter would take as input the identity of a *source* node and a list of *target* nodes. The social filter would then operate on the social network that contains the specified nodes and would compute the following results: 1) the ranking of the target nodes in terms of the amount of trust that the source node holds in them; 2) the set of top k target nodes in terms of the amount of trust that the source node holds in them, where k is a predefined constant less than the size of the list of target nodes; 3) the quantified trust of the source node in each of the target nodes; 4) a binary value corresponding to each target node suggesting whether the source node should trust that target node or not.

Our models of social concepts and trust are presented in sections 4 and 5 respectively. We would continue to further enrich the models with additional characteristics that may be learned from the use cases studied over the course of the project.

The presence of social and trust information about services would allow us to create novel parameters based on this information for event subscription and matching. Complex event processing modules can use these parameters to enhance the selection and composition of events. As shown in the third part of Figure 1, a complex event processing module may use the inferred trust information as a parameter in the selection and composition of events. This functionality would be studied as part of the second activity of the task which corresponds to the deliverable D2.1.2.

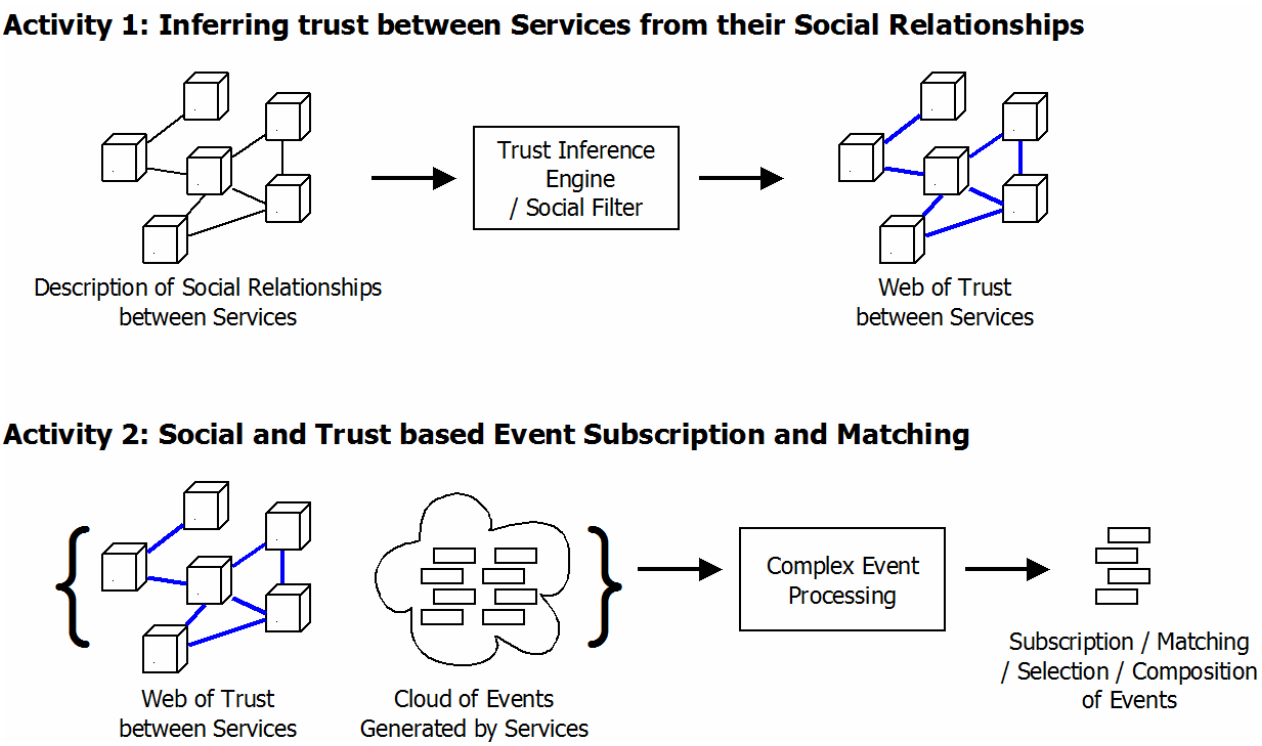

Figure 1: General Framework

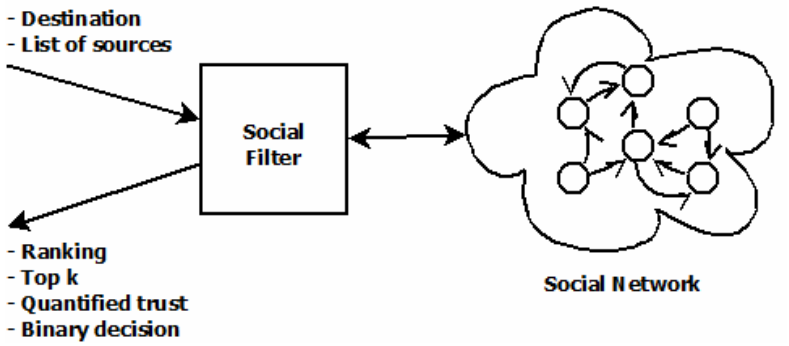

Figure 2: Inputs and Outputs of the Social Filter

3.2. Architecture of the Social Filter

In Figure 3, we sketch the architecture of the social filter. The social filter provides a web service interface for external components. A client submits a pair of source and target nodes. The social filter client would be an external component in the SocEDA architecture, such as the Event Cloud and the Filters sub component (described in D1.2.1). The social filter web service provides the strength of the relationship (trust) of the source node in the target node. This version of the architecture takes the basic input of a single pair of source and target nodes and provides the basic output of the relationship strength. However, we note that these basic inputs and output are sufficient as a foundation for the more complex inputs and outputs (such as ranks, top *k*, etc.) discussed in the previous section. The relationship strength engine uses various techniques for trust / relationship strength inference which are discussed in Section 5.3. The engine operates on social network data which is maintained in a local database. The local social network data is updated by the social network manager component. The social network manager interfaces with external components such as the event cloud to monitor changes in the social relationships between services.

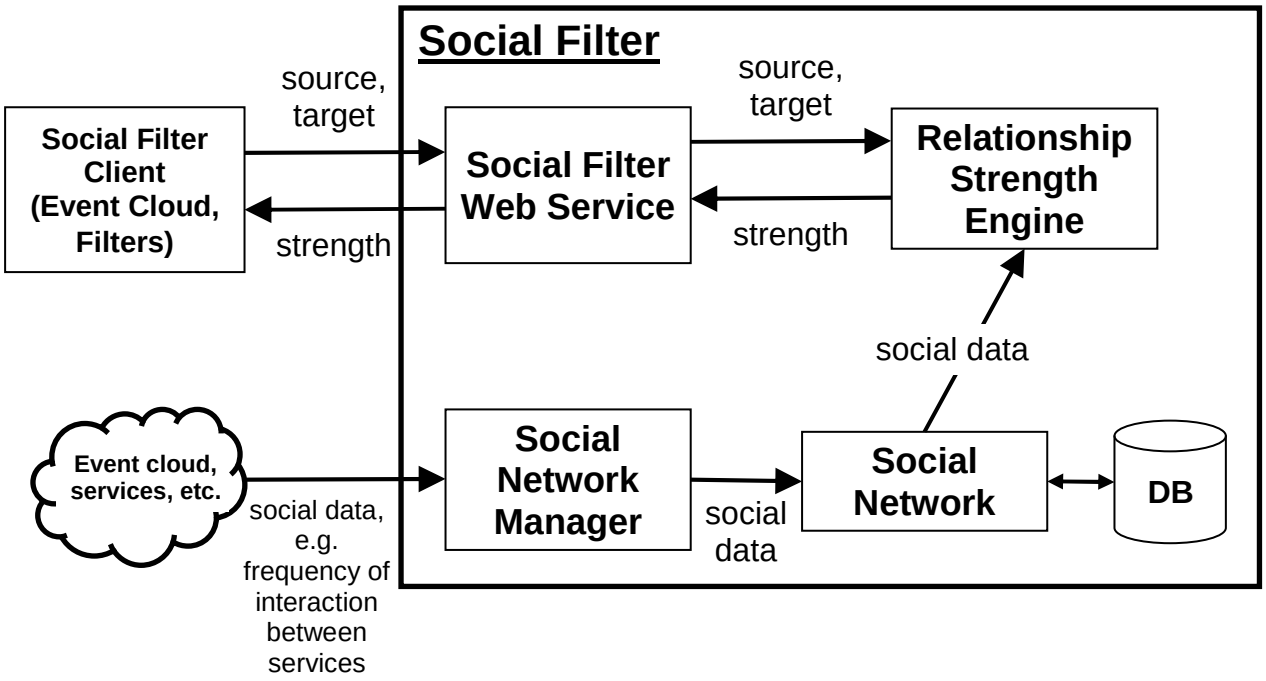

Figure 3: Architecture of the Social Filter

Figure 4 shows a sequence diagram for the interaction of the *SocialFilterWS* component with the external *EventCloud/Filters* component. The *EventCloud/Filters* invokes the *SocialFilterWS* by submitting the IDs of a source node and a target node. The *SocialFilterWS* calls the *RSEngine*. The *RSEngine* in turn retrieves related social network information from the *SocialNetwork* component and runs the social filter algorithms to compute the strength of the relationship between the source and the target node. The *RSEngine* returns the relationship strength to the *SocialFilterWS*, which conveys it to the *EventCloud/Filters*.

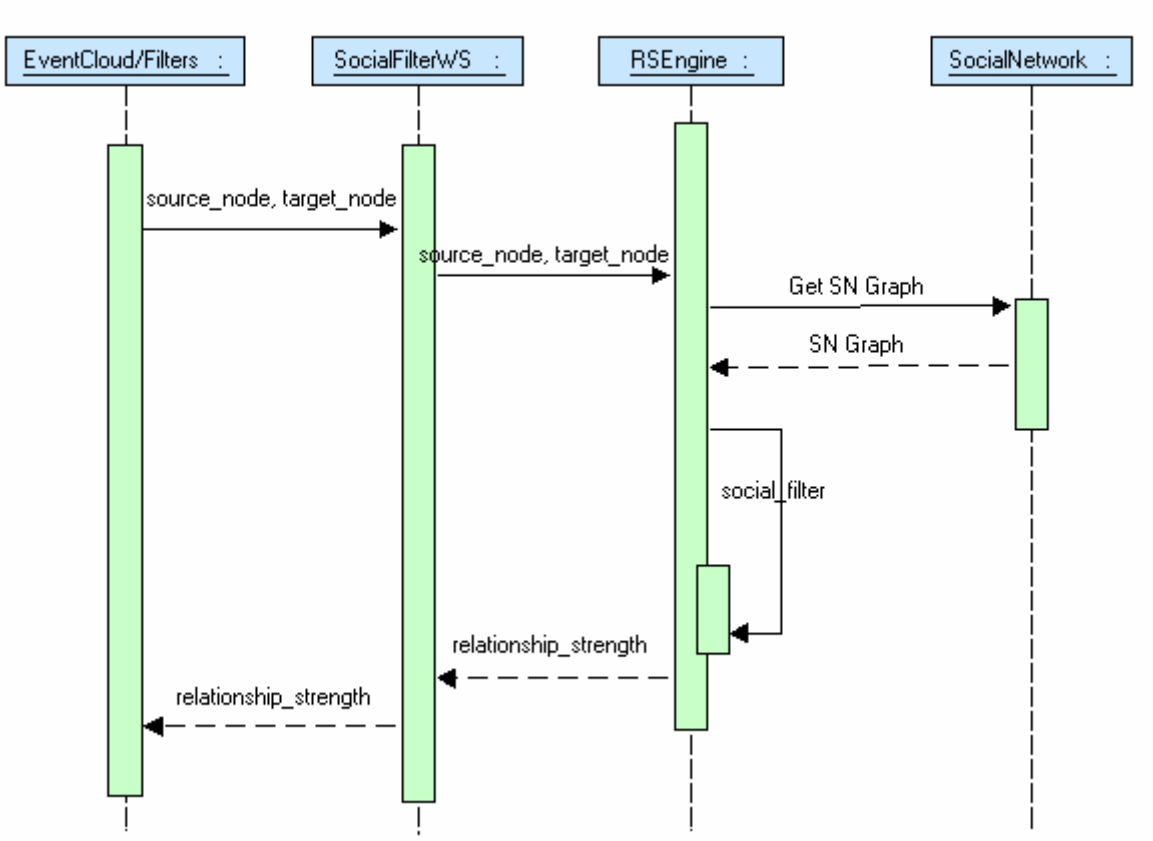

Figure 4: Sequence Diagram

4. Social Networks and Relationships

We take a look at the key social concepts of social networks and social relationships. In particular, we discuss the nature of social relationships by identifying the various attributes that characterize them.

4.1. Social Networks

A social network is a composition of nodes and the relationships between them. The nodes in a social network may be individuals or collectives of individuals. The relationships between nodes are founded on human ties such as friendship, membership in the same family or organization, mutual interests, common beliefs, trade, exchange of knowledge, geographical proximity, etc.

4.2. Characteristics of Social Relationships

The most commonly discussed characteristics of social relationships include *roles*, *valence*, *provenance*, *history*, and *strength* [Mika2011].

- **Roles.** A social relationship is defined by the roles that are associated with it. For example, the roles of employer and employee define the relationship of employer--employee in a professional setting. The same pair of nodes may take on different roles in a parallel relationship. For example, a employer--employee relationship may be complemented by a neighbor--neighbor relationship.
- **Valence.** A social relationship can have positive, negative, or neutral sentiments associated with it. For example, an individual may like, dislike, or be apathetic towards another individual.
- **Provenance.** Some attributes of a social relationship may be asymmetric, that is, perceived differently by the individual participants of the relationship. For example, a sentiment of *like* from one node may not be reciprocated by the other node in the relationship.
- **Relationship history.** Social relationships have a temporal dimension. A social relationship may evolve with time through interactions or the absence thereof. The history of a social relationship can be considered as an indicator of the current and future status of the relationship. For example, a long positive relationship in the past is likely to be followed by a positive relationship in the present and in the near future.
- **Strength.** Strength of a tie (or social relationship) is a quantifiable property that characterizes the link between two nodes [Petroczi2007]. The notion of tie strength was first introduced by sociologist Mark Granovetter in his influential paper ``The strength of weak ties" [Granovetter1973] published in 1973. He defined the strength of a tie as a ``combination of the amount of time, the emotional intensity, the intimacy (mutual confiding), and the reciprocal services which characterize the tie" [Granovetter1973]. The strength of a social relationship is a complex construct, which is itself composed of

several properties of social relationships. We discuss the strength of social relationships in detail in the following section.

4.3. Strength of Social Relationships

Granovetter proposed four dimensions of tie strength: *amount of time*, *intimacy*, *intensity*, and *reciprocal services* [Granovetter1973] [Gilbert2009]. A number of researchers (including Burt [Burt1995], Wellman and Wortley [Wellman1990], Lin et al. [Lin1981], Marsden [Marsden1984]) have since studied the dimensions of tie strength and have refined and expanded the original list of four. The existing literature suggests seven dimensions of tie strength: *intensity*, *intimacy*, *duration*, *reciprocal services*, *structural factors*, *emotional support*, and *social distance* [Gilbert2009].

In a study on predicting tie strength between individuals based on their exchanges on social networking sites [Gilbert2009], Gilbert and Karahalios have identified a number of indicators that predict tie strength belonging to each of the seven dimensions. In a study with similar goals, Petroczi et al. [Petroczi2007] have developed a set of questions that they pose the members of a virtual social network in order to establish the strength of ties between them. In the following list, we discuss each of the seven dimensions of tie strength as well as some associated indicators and questions that yield tie strength.

- **Intensity.** The indicators of the intensity of a tie strength include the *frequency of contact* and the *amount of information exchanged* between two nodes.

  Homans presented the argument in his 1950 book ``The Human Group'' that ``the more frequently the persons interact with one another, the stronger their sentiments of friendship for one another are apt to be'' [Homans1950] [Granovetter1973].

  Gilbert and Karahalios [Gilbert2009] use the amount of information exchanged (for example, the number of words and messages exchanged) on a social networking site as an indicator of the intensity of the tie strength between individuals.

- **Intimacy.** Mutual confiding (or trust) is an indicator of the intimacy and the strength of a social tie [Granovetter1973] [Marsden1984] [Petroczi2007]. Sociologist Diego Gambetta [gambetta00] characterizes trust as contextual and quantifiable as subjective probability.

  Petroczi et al. [Petroczi2007] ask the members of an online discussion forum the following question in order to determine the trust and consequently the tie strength between them: ``Which participants do you trust (for example they know your real name, email address, password to your introduction sheet)?''.

  Gilbert and Karahalios [Gilbert2009] use the variable ``Relationship status'', with the possible values of *single*, *in relationship*, *engaged*, and *married*, as an indicator of the intimacy of two individuals. Other variables that they use as indicators of intimacy

include ``Distance between hometowns", ``Appearances together in photos", and ``Days since last communication".

- **Duration.** The duration or the span of the relationship is considered as an indicator of the strength of the relationship.

  Gilbert and Karahalios [Gilbert2009] use the variable ``Days since first communication" on social networking sites as a proxy for the length of the relationship between two individuals.

- **Reciprocal services.** A social relationship is stronger if it is reciprocated by both participants. For example, a sentiment of *like* shared by both nodes would result in a strong social relationship.

  Gilbert and Karahalios [Gilbert2009] use *the number of links and applications mutually shared* between friends as variables quantifying reciprocal services on social networking sites.

- **Structural factors.** Ronald Burt proposed that structural factors shape tie strength, factors like network topology and informal social circles [Burt1995] [Gilbert2009].

  A structural factor that Gilbert and Karahalios [Gilbert2009] use to predict tie strength is the ``Number of mutual friends". They also use structural factors such as membership in common interests groups, and association with the same institutions, organizations, or geographical locations (for example, graduation from the same university, employment in the same company, or residence in a common city, etc.).

- **Emotional support.** Wellman and Wortley argue that providing emotional support, such as offering advice on family problems, indicates a stronger tie [Wellman1990] [Gilbert2009].

  To determine the emotional support between the members of a virtual social network, Petroczi et al. [Petroczi2007] ask the members which other members they have requested or they feel they could request for a favor or help.

  Gilbert and Karahalios [Gilbert2009] monitor emotion words (as identified by the Linguistic Inquiry and Word Count (LIWC) dictionary [Pennebaker2001], for example, *birthday*, *congrats*, *sweetheart*) exchanged between the members of a social networking site as indicators of emotional support.

- **Social distance.** Lin et al. show that social distance, embodied by factors such as socioeconomic status, education level, political affiliation, race and gender, influences tie strength [Lin1981] [Gilbert2009].

Gilbert and Karahalios [Gilbert2009] measure social distance by considering parity in age, occupation, education, political, and religious views of the individuals.

4.4. Description of Social Relationships between Services

The use cases for the SocEDA project (such as the one described in the deliverable D5.3.1) consider an Internet of Services, with the assumption that the services involved can publish their events and create event clouds.

It is evident that social relationships exist between humans. However, we argue that social relationships can also exist between services. The characteristics that we have identified for social relationships between humans also apply to relationships between services. Let's consider each of the following characteristics previously discussed in Section 4.2 in the context of social relationships between humans:

- **Roles.** Roles also exist between services. At a fundamental level, the relationship between two services can be characterized by the role of consumer-provider or vice versa. More complex roles include composition, two services belonging to the same organization, etc.
- **Valence.** A service can have a positive, negative, or neutral opinion towards another service based on the quality of service that it has received.
- **Provenance.** Attributes of a relationship between two services can also be asymmetric. For example, one service can have a positive valence towards the other however the opposite may be true in the other direction.
- **Relationship history.** The relationship between two services also has a temporal dimension. The relationship can evolve with time through varying intensity of interactions.
- **Strength.** The strength of a relationship between two services is characterized by dimensions and indicators similar to those for social relationships between humans. For example: the *intensity* of the relationship as indicated by interaction frequency and the amount of information exchanged, the *intimacy* of the relationship as depicted by the recentness of interaction and the amount of declared trust; the *duration* of the relationship as measured by the time past since the first interaction; and *structural factors* such as the number of mutual nodes.

Our argument that social relationships exist between services is also supported by Qinyi et al. [Qinyi2009] and Maamar et al. [Maamar2011].

A preliminary model for the description of a social relationship between two services is given in Table 1.

Element	Data Type	Comments	Dimension of Tie Strength
source_node	Node ID		
target_node	Node ID		
role	Role ID		
interaction_count	{0,1,2,3,…}	Number of interactions between the two nodes	Intensity
amount_of_data_exchanged	{0,1,2,3,…}	Amount of data exchanged between the two nodes. The data unit can be considered as kilobytes, megabytes, etc.	Intensity
time_of_last_interaction	Timestamp	The time of the latest interaction between the two nodes	Intimacy
trust	[0,1]	A value representing the amount of subjective trust that the source node holds in the target node. 0: weak, 1: strong. The context of trust is the general integrity of the target node.	Intimacy
time_of_first_interaction	Timestamp	The time of the earliest interaction between the two nodes	Duration
mutual_nodes_count	{0,1,2,3,…}	The count of nodes that have relationships with both the source and the target nodes	Structural Factors

Table 1: Model for Description of a Social Relationship between Services

5. Trust

Trust is an important indicator of the strength of a social relationship. It inherently takes into account a number of other aspects of a social relationship.

5.1. Modeling Trust

Sociologist Diego Gambetta [Gambetta2000] proposes the following definition of trust:

> Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.

This is one of the seminal definitions that describe trust as a quantifiable construct. Gambetta observes that trust is an agent's degree of belief (the level of subjective probability) that another entity will perform an expected action. An additional important aspect of this definition is the recognition that trust is contextual.

The advantage of Gambetta's model of trust is its quantification of trust as subjective probability. It allows trust to be modeled as a mathematical construct and to be manipulated using the wide range of tools available in probability theory. Moreover, trust modeled with subjective probability is more intuitive than trust modeled with other theories such as subjective logic and fuzzy logic.

5.2. Characteristics of Trust

From Gambetta's definition, we infer that trust has the following characteristics:

- **Binary-Relational and Directional.** According to the definition, ``Trust … is a particular level of the subjective probability with which ***an agent*** assesses that ***another agent or group of agents*** will perform a particular action …". From this excerpt, it is evident that trust is a relationship between two entities. Moreover, it is also clear that trust is directional. The first entity is an agent who has trust in a second entity which may be another agent or a group of agents.
- **Contextual.** As given in the definition, ``Trust … is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform ***a particular action*** … ". We infer that trust is in the context of ``a particular action" that the second entity may perform.
- **Quantifiable as Subjective Probability.** ``Trust … is ***a particular level of the subjective probability*** with which an agent assesses that another agent or group of agents will perform a particular action, ***both before he can monitor such action (or independently of his capacity ever to be able to monitor it***) …. From this excerpt of the definition, we deduce that trust is quantifiable as subjective probability.

We discuss below some other characteristics of trust which are not evident from Gambetta's definition. We provide examples to support their validity as characteristics of trust. These characteristics have been previously identified by several authors (such as [Capra2004]).

- **Non-Reflexive.** An agent may or may not trust herself. For example, a patient Alice may trust her doctor to prescribe her the correct medicine, whereas she might not trust herself to do so.
- **Asymmetric.** If an agent Alice trusts an agent Bob, then Bob may or may not trust Alice. For example, in the context of car repair, a car owner Alice may trust her mechanic Bob, however Bob may not necessarily trust Alice.
- **Non-Transitive.** If an agent Alice trusts an agent Bob who in turn trusts an agent Carol, then Alice may or may not trust Carol. For example, an email server ***A*** might trust an email server ***B*** to not send spam. If ***B*** trusts an email server ***C*** in the same context, then ***A*** may or may not trust ***C*** depending on various factors such as its strength of trust in ***B***, the availability of additional evidence, etc.
- **Dynamic.** Trust may change with time. For example, let's say that an online shopper Alice has so far had good experiences with an online vendor Bob and therefore she has high trust in him. However, if her latest transaction with Bob is less than satisfactory, then her trust in Bob is likely to decrease instead of staying constant.

5.3. Inferring Trust

There are a number of techniques that enable inferring trust between entities. The first technique that we describe is *direct interaction* that requires explicit input from nodes. The other three methods that we discuss aim to infer trust from existing information.

Our *trust inference engine / social filter* uses the techniques discussed here to infer the *trust / strength of the social relationship* between a given pair of nodes in a social network.

5.3.1. Direct Interaction

The primitive method of establishing trust in an unknown entity is to directly interact with it and observe its behavior in the desired context. However, this method requires that the entity be trusted at least once without any prior background on that entity. This approach is perhaps suitable for low-risk transactions and in situations when no other recourse is available. However, when reliance on an unknown entity may lead to substantial damage, the other approaches for trust establishment are clearly preferable, since they allow the truster to base his trust on some prior knowledge provided by others.

McKnight et al. [McKnight1998] introduce the notion of *initial trust*, which is described as the trust in an unfamiliar trustee -- a relationship in which the actors do not yet have credible information about, or affective bonds with each other [Bigley1998].

5.3.2. Trust Recommendation and Propagation

Establishing trust in an unknown entity through trust recommendation and propagation takes advantage of the possible transitivity of trust. Let's say that Alice wishes to establish trust in an

unknown individual, Carol. If another individual Bob trusts Carol then he could give a recommendation to Alice about Carol's trustworthiness. Taking Bob's trust recommendation and her own trust in Bob into account, Alice may establish a trust relationship with Carol. Thus a transitive path of trust that leads from Alice to Bob to Carol, enables Alice to develop trust in Carol. If Alice wishes to establish trust in Carol through Bob's recommendation, we say that Bob's trust in Carol has propagated to Alice.

Guha et al. [Guha2004] term the above described one-step propagation as *atomic propagation*. The term stems from the observation that the conclusion is reached based on a single argument, rather than a possibly lengthy chain of arguments. Guha et al. identify four types of atomic propagations: *direct propagation*, *co-citation*, *transpose trust*, and *trust coupling*. We briefly elaborate each of these types of atomic trust propagation:

- **Direct Propagation.** The example given in the first paragraph represents direct propagation. If ***i*** trusts ***j***, and ***j*** trusts ***k***, then a direct propagation allows us to infer that ***i*** trusts ***k***. Guha et al. refer to this particular atomic propagation as direct propagation since the trust propagates directly along an edge.
- **Co-Citation.** Let's consider that ***i1*** trusts ***j1*** and ***j2***, and ***i2*** trusts ***j2***. Under co-citation, it is concluded that ***i2*** also trusts ***j1***.
- **Transpose Trust.** In transpose trust, ***i***'s trust in ***j*** causes ***j*** to develop some level of trust towards ***i***. Let's say that ***i*** trusts ***j***, then transpose trust implies that ***j*** should also trust ***i***.
- **Trust Coupling.** Let's suppose that ***i*** and ***j*** both trust ***k***, then trust coupling leads us to infer that ***i*** and ***j*** should trust each other since they both trust ***k***.

Iterative propagation builds upon multiple atomic propagations to help establish trust in an unknown entity. Let's extend the example presented in the first paragraph: Alice trusts Bob and Bob trusts Carol. We further assume that Carol trusts Dave. Alice may establish trust in Dave as a result of the following two atomic propagations: 1) the first atomic propagation builds Bob's direct trust in Dave, and 2) now since Bob trusts Dave, Alice can establish trust in Dave through a second atomic propagation. This sequence of atomic propagations is referred to as iterative propagation.

5.3.3. Trust Negotiation

Trust negotiation is an approach that can enable strangers to electronically share sensitive data and services. Trust negotiation establishes trust between entities based not on their identities but their properties. For example, in the case of an individual, the properties that may be considered include their place of employment, age, membership in certain organizations etc. With trust negotiation, the trust between two entities is acquired through iterative requests for credentials and their disclosure.

An example from [Bertino2004]: *CARS* is an online car rental agency, which has an agreement with a company called *CORRIER* to provide rental vehicles free of charge to their employees, provided that they prove their employment status (which also implies that they are authorized to drive). Other customers (who are not employees of *CORRIER*) can rent a vehicle by showing a valid driving license and by providing a credit card for payment. Thus, *CARS* establishes trust in customers to be legitimate drivers through the exchange of multiple possible credentials.

Customer: Request a vehicle

CARS: Show digital employment ID from CORRIER

Customer: Not available

CARS: Show digital driving license

Customer: Digital driving license

CARS: Provide digital credit card

Customer: Digital credit card

CARS: Vehicle granted (vehicle info, pickup info, etc.)

5.3.4. Reputation

Reputation is the general opinion of the community about the trustworthiness of an individual or an entity. A person who needs to interact with a stranger, may analyze her reputation to determine the amount of trust that he can place in her. In the physical world, reputation often comes from word of mouth, media coverage, physical infrastructure, etc. However, the reputation of a stranger is often difficult to observe in online communities, primarily due to their global scale, the cheap availability of anonymous identities, and the relative ease of acquiring high quality digital presence.

A reputation system computes the reputation of an entity based on the feedback (quantified trust) provided by fellow entities. Reputation systems make certain that users are able to gage the trustworthiness of an entity based on the history of its behavior. The expectation that people will consider one another's pasts in future interactions constrains their behavior in the present [Resnick2000].

6. Conclusion

In this document, we have modeled social relationships by identifying the various attributes that characterize them. The use cases for the SocEDA project consider an Internet of Services, with the assumption that the services involved can publish their events and create event clouds. We have argued that social relationships can also exist between services. Consequently, we have developed a model of social relationships between services based on the attributes that we identified for human social relationships. We also argued that trust is one of the main indicators of the strength of a social relationship. We provided a model of trust and discussed several techniques for inferring trust between a pair of given nodes. We proposed a social filter component that utilizes these techniques to infer the trust or the strength of the social relationship between services. Components in the SocEDA architecture such as the Event Cloud can invoke the social filter to find out the amount of trust between pairs of services.

7. References

[Bertino2004] E. Bertino, E. Ferrari, and A. C. Squicciarini. Trust-x: A P2P framework for trust establishment. IEEE Transactions on Knowledge and Data Engin., 16(7):827 - 842, July 2004.

[Bigley1998] G. A. Bigley and J. L. Pearce. Straining for shared meaning in organization science: Problems of trust and distrust. Acad. Management Rev.,23(3):405421, 1998.

[Burt1995] R. Burt. Structural Holes: The Social Structure of Competition. Harvard University Press, 1995.

[Capra2004] L. Capra. Engineering human trust in mobile system collaborations. In Proceedings of the 12th ACM SIGSOFT International Symposium on Foundations of Software Engineering, Newport Beach, CA, USA, 2004.

[Gambetta2000] D. Gambetta. Trust: Making and Breaking Cooperative Relatioins, chapter Can We Trust Trust?, pages 213 - 237. Department of Sociology, University of Oxford, 2000.

[Gilbert2009] E. Gilbert and K. Karahalios. Predicting tie strength with social media. In Proceedings of the Conferece on Human Factors in Computing Systems (CHI09), 2009.

[Granovetter1973] M. Granovetter. The strength of weak ties. American Journal of Sociology, 78:1360-1380, May 1973.

[Guha2004] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Propagation of trust and distrust. In Proceedings of the International World Wide Web Conference (WWW 2004), 2004.

[Homans1950] G. Homans. The Human Group. Harcourt, Brace, & World, New York, 1950.

[Lin1981] N. Lin, W. M. Ensel, and J. C. Vaughn. Social resources and strength of ties: Structural factors in occupational status attainment. American Sociological Review, 46(4):393 - 405, 1981.

[Maamar2011] Z. Maamar, P. Santos, L. Wives, Y. Badr, N. Faci, J.P.M. de Oliveira. Using Social Networks for Web Services Discovery. IEEE Internet Computing, July-Aug, 2011. Volume: 15, Issue:4, Pages: 48 - 54.

[Marsden1984] P. V. Marsden and K. E. Campbell. Measuring tie-strength. Social Forces, 63:482 - 501, 1984.

[McKnight1998] D. H. McKnight, L. L. Cummings, and N. L. Chervany. Initial trust formation in new organizational relationships. Acad. Management Rev., 23(3):473490, 1998.

[Mika2011] P. Mika and A. Gangemi. Descriptions of social relations. Technical report, Department of Business Informatics, Free University Amsterdam, The Netherlands, Retrieved February 17, 2011 2011.

[Pennebaker2011] J. W. Pennebaker, M. E. Francis, and R. Booth. Linguistic Inquiry and Word Count: LIWC2001. Erlbaum Publishers, Mahwah, NJ, 2001.

[Petroczi2007] A. Petroczi, T. Nepusz, and F. Bazso. Measuring tie-strength in virtual social networks. Connections, 27(2):39 - 52, 2007.

[Qinyi2009] Qinyi Wu, Arun Iyengar, Revathi Subramanian, Isabelle Rouvellou, Ignacio Silva-Lepe, Thomas Mikalsen. Combining Quality of Service and Social Information for Ranking Services. ICSOC 2009.

[Resnick2000] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation systems. Communications of the ACM, 43(12):4548, December 2000.

[Wellman1990] B. Wellman and S. Wortley. Diferent strokes from diferent folks: Community ties and social support. The American Journal of Sociology, 96(3):558 - 588, 1990.