Effective Design of Trust Ontologies for Improvement in the Structure of Socio-Semantic Trust Networks

Nima Dokoohaki[1], Mihhail Matskin[2]

***Abstract*—Social ecosystems are growing across the web and social trust networks formed within these systems create an extraordinary test-bed to study relation dependant notions such as trust, reputation and belief. In order to capture, model and represent the semantics of trust relationships forming the trust networks, main components of relationships are represented and described using ontologies. This paper investigates how effective design of trust ontologies can improve the structure of trust networks created and implemented within semantic web-driven social institutions and systems. Based on the context of our research, we represent a trust ontology that captures the semantics of the structure of trust networks based on the context of social institutions and ecosystems on semantic web.**

***Index Terms*—Semantic Trust, Trust Networks, Trust Ontology, Semantic Social Networks, Ontology Engineering, Structural Analysis.**

I. INTRODUCTION

Semantic web is described to be a web of knowledge having properties such as heterogeneity, openness and ubiquity. In such an environment where everyone has the ability to contribute, trustworthiness of these people and their contributions are of great importance and value. As stressed, trust plays a crucial role in bringing the semantic web to its full potential.

A trust network can be seen as a structure capturing metadata on a web of individuals with annotations about their trustworthiness. Considering social network as our context, a trust network can be seen as an overlay above the social network that carries trust annotations of the metadata based on the social network, such as user profiles and information. Social networks are gaining increasing popularity on the web while semantic web and its related technologies, are trying to bring social networks to their next level. Social networks are using the semantic web technologies to merge and integrate the social networking user profiles and information. Such efforts are paving the path toward semantic web-driven social ecosystems. Merging and integrating social networking data and information can be of business value and use to web service consumers as well as to web service providers of social systems and networks. Ontologies, at the core of semantic-web driven technologies lead the evolution of social systems on the web. Describing trust relations and their sub-components using ontologies, creates a methodology and mechanism in order to efficiently design and engineer trust networks.

"Structure of a given system is the way by which their components interconnect with no changes in their organization" according to [1]. Determining the structure of a society of agents on a trust network structure within a semantic social system, can help us determine the organizational structure of a system. Having this capability we can determine an organization's certain factors such as flexibility, change capacity, etc.

In this paper we investigate how effective design of trust ontologies can improve the structure of trust networks created and implemented within semantic web-based social systems. To address the efficient design of trust networks on semantic web-driven social systems, we have engineered and analyzed a trust ontology [2]. Our trust ontology is based on the main concept of *Relationship*, that models the main element of trust networks, and two concepts of *Main Properties* and *AuxiliaryProperties*, which model properties of relationships.

In order to effectively design an ontology for trust, we have introduced a framework for comparing and evaluating trust ontologies. As an experiment, several ontologies of trust have been evaluated according to our framework. To understand the process of engineering the ontology itself, all phases and steps taken during the process of building our proposed trust ontology have been mentioned in details. As an experiment, we have studied the structure of the trust network to describe how a trust ontology can serve as the framework for engineering efficient and scalable trust networks. Same experiment data have been used to create network of other similar works structure-wise to get a deeper knowledge of the

[1]Nima Dokoohaki is a PhD candidate at Department of Electronics, Computer and Software Systems (ECS), School of Information and Communications Technology (ICT), Royal Institute of Technology (KTH), Stockholm, Sweden. Email: nimad@kth.se

[2]Mihhail Matskin is a professor at Department of Electronics, Computer and Software Systems (ECS), School of Information and Communications Technology (ICT), Royal Institute of Technology (KTH), Stockholm, Sweden and professor II (adjunct professor) at Norwegian University of Science and Technology, (NTNU), Trondheim, Norway. Email: misha@imit.kth.se

network structure with respect to ontology design disciplines. The contents of this paper are organized as follows: following the background study and discussion on related research in section 2, state of art in trust ontologies is presented in section 3, our trust ontology is introduced in the section 4, in section 5 trust networks analysis is presented and discussed. Finally we conclude in section 6 and we discuss the future research in section 7.

II. BACKGROUND

Within the context of social semantic systems, there has been an extensive amount of efforts based on both academic and practical approaches in order to design and engineer trust networks, but none of the existing works in the field were designed bearing structural and design issues in mind. In this section we introduce the technologies that we have incorporated and considered in our approach.

We divide the foundation of our work into two main topics, namely: semantic social networks and trust. In this section we also give a detailed and thorough overview into each field. Each overview is divided into subsections where each of the substantial topics is further studied and discussed.

A. Socio-Semantic Ecosystems Overview

In 1967, Stanley Milgram introduced "Small World Hypothesis" [3], which was published by American Sociologist. Social networks became popular in 1990s. A social network is generically defined as a set of people gathered together through connections or links, according to [5].

Web has become a ground for bringing the notion of society of people into life. A web-driven social network needs to be accessible using a web browser and within this network people should be able to explicitly (or implicitly) state their connections and their links to individuals or group of individuals, according to [21].

Web-based social networks continue to evolve, while what is most important today is that connections on these networks, are not single dimensional anymore and today you can model and state different aspects of relationships, such as trust.

In 2005, according to [21], there were 115,000,000 accounts within social networks scattered across about 18 online networking communities. It's important to consider that not all these accounts correspond to a single individual. Many people have multiple memberships across multiple networks, at the same time.

Size of the social networks will continue to grow everyday as people realize the "hidden" values of social networking day by day [8]. This growth will continue in size aspect of web grounded social networks and will not stop and as many have predicted [7] [8], the so called "email scenario" will take place, where the number of advertisements and SPAM messages will increase so drastically that by some point of time these networks will literally collapse.

There is a strong and growing demand for fusion of the data from different social networks on web. Many are interested in sharing their profiles, while others are interested in merging their data from multiple networks.

Two main reasons can be stated and discussed here:

First and foremost, great amount of this data which is scattered throughout all these sites are not shareable and are inaccessible from other networks. Second, as stated many users have different accounts across different networks and if their data merge, then many of these accounts might become a single account.

In addition to individuals and users on the web, social networks have become the target of the businesses and industries. There are many businesses and enterprises which sell packages of social networking capable software to their users. So the value of social networking exceeds beyond the borders of individuals and businesses now.

1) Vision of semantic web-driven social institutions

Social metadata fusion, in the form of sharing or integration brings business value to entities living within such ecosystems. The vision of "Semantic Social Network (SSN)" [4], describes the fusion and integration of social data across social networks, located on a web of semantics.

This vision is based upon two important dimensions:

First, semantic descriptions of social data about people available on the web in public, expressed in a formal metadata language such as XML or RDF, with explicitly described links to other people on same or different networks.

Second, semantic references to those descriptions described and stored in a formal metadata language such as RDF or XML [4] [5].

There were several attempts to bring this vision into life. One of the most important and influential ones is FOAF (friend-of-a-friend) project [6].

2) FOAF and SIOC: bringing the vision into life

FOAF project creates an RDF vocabulary for describing people and the relationship between them. In this way it can be used as the "glue" in between semantic web and social ecosystems, according to [10].

As described, current Web communities are distributed all around the web, with no links in between them, according to [11].

In order to bring semantics to online communities, SIOC [12] (Semantically-Interlinked Online Communities) tries to create the so called "glue" through SIOC ontology [13] [14].

SIOC aims to enable the integration of Web community information and creates the possibility of describing and presenting the social web of data using RDF. We can think of FOAF as an enabler for describing semantic web of individuals, while SIOC enables describing semantic web of communities of individuals.

SIOC utilizes the FOAF vocabulary for expressing personal profile and social networking information [11].

3) Modeling social networks on semantic web

Social Network Analysis (SNA) [15] [16], is the science of studying and analyzing a networked setting and it has been applied to settings of networks of health, innovation, etc. Network analysis provides the theoretical as well as practical background for studying how to analyze the network participation effect on certain grounds such as an individuals or groups behavior.

Ontologies can be used to model and capture the structure of formal semantics of social networks.

Wennerberg [15] describes how the structure of a network can be modeled using a semantic web ontology. Ontologies model, present and document the concepts and properties of a certain domain. Having the social nature of the networks as the domain of the study, ontologies can capture the concepts of relationships, individuals and their respective properties. Inference mechanism gives ontologies the ability of inferring new information using rules which could be of great importance in social context.

A set of existing efforts on modeling social network on the semantic web could be mentioned here.

Cantador et al. [17], model a social semantic network by utilizing ontology as a basis for clustering the user profiles in a social networking community. The ontology represents the domain of user's cognitive patterns, such as interests and preferences. Resulting ontological instances, take the shape of a semantic network of interrelated domain concepts and user profiles.

A similar effort [18] uses ontology at the core of a semantic web-enabled application. This ontology generates a social network of users and their interests. Generated ontological networks are used in order to detect and filter the Conflict of Interest (COI) relationships in an academic context, comprising authors and reviewers of papers.

In a similar effort with the same context, Mika [19] uses ontologies, in the context of a semantic web-driven application system and Flink [19], for modeling, capturing and visualizing the social network of researchers.

B. Trust overview

Being the key to any interaction procedure in human societies, trust has been the subject of studies to many fields of research and science such as sociology and psychology, as well as of course computer science.

Because of its importance and significance, trust has been harvested as a field of research in for example decentralized access control, public key certification, reputation systems for peer to peer networks, and mobile ad-hoc networks.

Despite the fact that there has been a variety of definitions for trust, there has not been an agreement on a generic definition of trust. Researchers mostly have defined trust, depending on the context and the orientation of the paper they have written or the experiments they have been conducting. As a matter of fact most of these definitions are specific to the context of the work being done.

Lack of consensus on generic trust definition makes us realize the importance of having a definition which is context-neutral and general enough to be applied to different fields of research and different contexts.

Trust is a complex issue, relating to fairness and straightforwardness, honesty and sincerity of a person or the service this person might offer.

Grandison [20] defines the trust in the following manner; "*Trust* is the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context". "Distrust may be a useful concept to specify as a means of revoking previously agreed trust or for environments when entities are trusted, by default, and it is necessary to identify some entities which are not trusted", according to [20].

Distrust is defined as "the lack of firm belief in the competence of an entity to act dependably, securely and reliably within a specified context" [20] [21].

1) Trust components, properties and sources

Trust is presented in the form a *relationship* between two parties. These two parties, often individuals or agents representing those individuals, are represented as *trustor* or *source*, which is defined to be the entity which seeks trust or trust related operations such as evaluation in other entity, *trustee* or *sink*, which is the entity that is trusted or it has been requested for trustworthiness-related evaluation. Trust is seen as having a *purpose* or a *context*. For instance, Alice trusts Bob as a doctor, but she might not trust Bob as a car mechanic, adopted from [20] [24]. In addition, a trust relation might also have a *trust metric*, which can be quantitative or qualitative, characterizing the degree to which the trustor trusts the trustee. This quality or quantity represents the *intensity* and *level* of trust. This quality and quantity can be evaluated by using an algorithm or *mechanism* which derives trust, according to the metric. For instance, Alice might trust

Bob as a doctor very much, while she only moderately trusts Martin as a doctor, adopted from [20] [24].

So far we have realized trust as a *computational value* depicted by a *relationship*, described inside a *specific context* and measured by a *metric* and is evaluated by a *mechanism*.

Some important properties of trust are stated and discussed [20] [24].

For instance, subjectivity (difference in judgments of two people on the same entity's trustworthiness) or transitivity (If transitive, when Alice trusts Bob and Bob trusts Cherry, Alice will trust Cherry, adopted from [20] [24]). One of the most important subjects of discussion on properties and components of trust is the difference being made between trust in performance and trust in recommendation [20] [24].

First, there is a difference between trust in an entity to perform an action (*trust in performance*), and trust in an entity to recommend other entities to perform that action (*trust in recommendation*). This is the distinction between Cherry trusting Bob as a dentist, and Cherry trusting Bob to recommend a good dentist, according to [20] [24].

Another difference is based on existence of recommenders. There is a difference between the trust that is directly observed by trustor from trustee and the trust that is conveyed and inferred from the recommenders' trust.

As a result, this difference can be sampled between Cherry trusting Bob as dentist, resulting from Cherry's own direct observation and evaluation from Bob, and Cherry trusting Bob as a dentist, based on the fact that she trusts Shawn as a recommender for a good doctor and on the fact that Shawn trusts (and perhaps recommends) Bob to be a good dentist, adopted from [20] [24].

During the observations made by [25], a set of sources of trust are identified, in both atomic (direct trust) and compound (social trust) forms.

Trust is the experience gained from an interaction between two individuals. So the actual experience is the source of trust. Considering the experience, or source of trust between two certain persons and individuals, this type of trust can be referred to as inter-individual trust or what is commonly referred to as *direct trust*, according to [25].

We can consider a setting of individuals across a web or network. If we consider this society of nodes and present the trust in this society and in this setting, then we are dealing with a new type of trust originating from the experiences gathered by a group of nodes or individuals. This new type of trust has its own source, from trust propagation in social settings or networks.

This type is called *relational trust, social networks driven trust* or in simple form, *social trust*, according to [25].

2) Trust computation in Web of Trust

Most of the models proposed for modeling trust on semantic web are more focused on probabilistic views of trust. They model trust using probabilities assigned as labels to the edges of the networks according to specified trust metric.

In order to derive and infer trust, edges are traversed and probabilistic trust values are gathered along the edges and using mechanism adopted, the trust value along the trust path will be computed and inferred. This setting is referred to as a Web of Trust. There are two reasons for making web of trust a candidate for adoption to trust in semantic web computation scenarios. First, both systems are open. Second, trust is considered as being transitive in both settings.

Web of Trust was a system that was introduced under the context of security and privacy systems, for instance PGP [55]. In this setting everyone can sign each other's key and act as certificate holder or certificate authority. Openness states the demand and need for metrics. Need for metrics, establishes and proves the relativity and computability of trust. The need for scalable trust metrics has been discussed and studied extensively [51] [52]. When metrics are applied all the links can carry them and trust can be inferred [27].

Under the assumption of trust transitivity and by enforcing metrics, pathways of trust can be formed and web of trust can be crawled and walked [53].

As stated, semantic web is a similar scenario in which each agent that forms a node on a network is connected to other nodes, agents, and these links and connections form a web of trust. In order to allow everyone, represented by an agent, to evaluate the statements of others in this open and heterogeneous environments, mechanisms and algorithms are developed or adopted to allow everyone to infer and evaluate trust in others using the trust metric-labeled links on the networks of trust.

3) Trust networks

The work in this field is mostly focused on the mathematical notion and presentation of networks but the amount of the practical work is limited.

Most of the works in this field do not consider design of larger infrastructures and ecosystems. Trust networks are described as weighted graph structures with directed edges. The edges in the generated graphs represent connections and relationships between individuals. Watts introduces the properties of a small world network [37]. He describes a model called ß-model [37] in order to model, construct and generate the structure of social systems. Many social systems have used this model within their infrastructure [34] [35] [36] [37] [38] [27].

Golbeck has done an extensive research effort on trust networks on semantic web, [27] [28] [29] [31]. She has constructed an ontology of trust, combining RDF and FOAF vocabulary to describe relationships comprising trust

networks. She has created applications on resulting networks of trust based on her ontology. These applications range from email filtering, TrustMail [27] [28], to web-based recommendation systems, FilmTrust [31].

Brondsema and Schamp [10] have created a system called Konfidi [33] that combines a trust network with the PGP Web-of-Trust (WOT). The system implements a metric and mechanism for inferring the trust on the networks formed. The generated network creates trust pathways in between email sender and receiver that can be crawled and using trust mechanism and metric, trust values are inferred [10].

III. Evaluating Trust Ontologies

This section gives an overview in some of the most important and influential works in modeling and designing trust ontologies. After giving a state-of-art overview in the observed ontologies, a framework for comparing and evaluating trust ontologies is introduced and the studied approaches are compared accordingly.

A. State-of-art in trust ontologies

As introduced earlier, Friend-Of-A-Friend (FOAF) [6] represents a vocabulary and introduces an ontology for describing a web of connected individuals.

This ontology can serve as a tool to model and eventually create a network of society of users by describing personal information about each person (realizing the node itself) and by describing personal information regarding a set of users whom the user knows about (realizing the neighbors on the network). Nodes on such a network are identified by their email address and email serves as their unique identification.

1) Golbeck's trust ontology

Jennifer Golbeck [27], introduces an ontology, that creates an important schema which extends FOAF by using *foaf:Person*, giving the users this possibility to state and represent their trust in individuals they know.

Metric used to express trust is a value on the scalar range of 0-9, in which each scale represents a trust level. These levels are set as properties under the domain of *foaf:Person*.

These levels correspond to: *Distrusts absolutely*, *Distrusts highly*, *Distrusts moderately*, *Distrusts slightly*, *Trusts neutrally*, *Trusts slightly*, *Trusts Moderately*, *Trusts highly*, *Trusts absolutely*, according to [27].

Context was introduced as a property of trust. Trust is context-sensitive, as a result meaning and semantics of trust can change depending on the context. This notion is represented in this ontology under *general trust* or *specific trust* or *topical trust*, according to [27].

For instance, Alice might trust Bob greatly on driving cars but might distrust Bob totally on repairing cars, adopted from [27]. In order to depict general trust within Golbeck's trust ontology, trust ratings (in the form of *trustsHighly* or *trustsModerately*) are described as properties in range of a person class under the range of another person.

To describe specific trust and topical trust, other sets of properties are introduced. These properties correspond to the nine values above, but are used to represent trust regarding a specific *topic* (for instance "*distrustsAbsolutelyRe*," "*trustsModeratelyRe*," etc), expressing the level of trust regarding a certain topic such as driving or dishwashing. The range of these properties is the "*trustsRegarding*", which has been defined to combine a person and a topic of trust. The "*trustsRegarding*" class has two properties: "*trustsPerson*" presenting the person being trusted (trustor), and "*trustsOnSubject*" presenting the subject that trust is stated towards, according to [27].

By having this ability we can query for trust about a person on a specific subject and it is possible also to infer trust on result trust network along the edges where given topic creates the connection and we can crawl along these paths to infer the trust value eventually.

2) Toivonen and Denker's Message and Context Ontology

Toivonen and Denker [41], study the trust in the context of communication and messaging. They state that there are many factors which can have immense impact on the honesty and trustworthiness of the messages we send and receive. The context-sensitivity of trust has been realized and taken into account in their work.

The work focuses on drastic changes that many issues, namely reputation, credibility, reliability, trustworthiness and honesty could have, and how they affect the progress of establishing and grounding trust, according to [41].

As a result of the work being done, a set of ontologies have been defined to capture context-sensitive messaging and trust. An ontology is developed to capture and denote the role of context-related properties and information. This ontology captures the domain of message communication and exchange and describes how the context information is actually attached to the messages. This ontology is constructed mainly to visualize how trust is related to message and communication.

It is important to note that this ontology extends the topical trust ontology of Golbeck [27], introduced earlier, and it relates the notion of trust to communication and messaging context. Basic idea behind this extension is that:" The topic of a message can have impact on its trust level" [27].

As a result, this trust ontology could be seen as an extension to topical trust ontology realizing the fact how trust can be fused within messages exchanged in the context of a communication environment. This concept is modeled and presented using *trustsRegarding* property. Links and connections between

persons are modeled by the *Trusts* property. Sub-properties of these two relationships conform to trust levels of Golbeck's ontology [27].

In order to model the relation of trust to the context, the *ctxTRUSTS* property is used. If we consider the environment of a simple communication setting, we see the sender, receiver and the communication network mediating them. The messages exchanged in between parties always have contexts, attached to them which in turn allow the computation of *ctxTRUSTS* properties through *Trusts* and *trustsRegarding* properties, according to [41].

3) Proof Markup Language's trust Ontology

Inference web [42] at Stanford University, has built a semantic web-enabled knowledge platform and infrastructure. This platform is designated to help users on the network to exploit the value of semantic web technologies in order to give and get trust ratings to and from resources on the web. This process is referred to as justification of resources. To this end, a language called PML is used.

PML [26] (Proof Markup Language) contains a term set for encoding the justifications and is designated to work in a question answering fashion [44]. PML is designated to help software agents to filter the resources on the web of semantics by proof checking them and justifying the credibility of these resources, on behalf of the users.

PML ontology contains three sub-ontologies including: provenance ontology, justification ontology and most importantly trust ontology which captures honesty and trustworthiness statements pertaining to resources.

The trust ontology [26] is one of the most important components in PML ontology and we briefly describe the structure of this ontology.

The approach presented here is modeling close notions of trust and belief and how it affects the credibility of resources on the web.

Notions of belief and trust, with respect to their close semantics, have been presented closely in this ontology. Ontology structure presents the trust and belief relations between a source and a sink (which are both realized and presented using agents) with respect to information from document source under investigation by respective agents.

The belief relation shows the belief of an agent about the source. The specific belief has a status (e.g. believes, disbelieves, ignorant). The trust relation shows an agent's overall beliefs about information from the specified source. The metric defined for trust and belief is probabilistic and for both elements a value between range of 0 and 1 has been designated.

4) Konfidi's trust ontology

With respect to metrics used for presenting the trust computational values and modeling the mathematical notion of trust, there exist two approaches: presenting a trust metric with discrete values and metrics with continuous values. Brondsema and Schamp [10] model and represent trust and distrust in a similar fashion using continuous values. Having continuous range of values allows easier propagation of trust values, along the edges on the networks, using inference mechanisms.

They represent the relationship as the class and main concept of the ontology. Each relation is directed from source (truster) to sink (trustee). Properties of relations are wrapped under the concept of trust item. The most important feature of this work is, like Jennifer Golbeck's ontology [27], they have incorporated the notion of "Topical trust" in their ontology. It is used as an attribute and property, which allows to state different features and properties of a relationship. Trust topics and trust values are stated as properties of the trust relationship.

In order to describe trust relationships, an ontology is presented using RDF, which in turn eases extending the FOAF vocabulary and profiles. Using the RDF properties, and taking into account that relationship can be described using FOAF vocabulary and ontology, then trust relationships can be described using trust ontology. Other technology that has been integrated is WOT [45] [46] (web-of-trust), that is used to describe web-of-trust resources such as key fingerprints, signature and signing capabilities and identity assurance [10] [46]. Ontology's RDF schema is made of 2 classes or concepts and 5 attributes or properties. As mentioned, the primary concept is Relationship between two people. Like most trust ontologies, there are two properties that are required for every Relationship, and they form the endpoints of every relationship; truster and trusted using FOAF vocabulary, both truster and trusted have *foaf:Person* objects as their targets.

Using WOT vocabulary, FOAF-defined Persons should also contain at least one *wot:fingerprint* property specifying the PGP, web-of-trust fingerprint of a public key held by the individual the Person refers to. Most importantly, this property serves for two reasons; first assures the identity of these people described on the both ends of relationship, and it also says if one of the people does not hold any keys then system can ignore instantiating a relationship between them.

B. Comparison and analysis

In this section we will compare some of the most important afore mentioned ontologies. We will try to point out common and shared points between mentioned ontologies, and we will also try to address strong and weak points among them. Table1 compares the ontologies reviewed so far based on the components of the ontologies.

TABLE I
COMPARISON AMONG TRUST ONTOLOGIES BASED ON ONTOLOGY COMPONENT STRUCTURE

Trust Ontologies	*Concept(s)*	*Relationship(s)*	*Instance(s)*	*Axiom(s)*
Jennifer Golbeck	Topical trust, Agent, Person	trustRegarding *(between agent and Topical trust)*	trust0...trust10 (range of trust metric), trustSubject, trustValue, trustedAgent, trustedPerson (subproperty of trustedAgent), trustRegarding	"A *Person or Agent* (e.g. Alice) *trustsHighlyRe* (*trust10*) *trustRegarding* a *trustedPerson or trustedAgent* (e.g. Bob) On *trustSubject* (e.g. Driving)"
Toivonen, Denker	Person, Topic, Receiver, Message	Trusts *(between Persons)*, ctxTRUSTS *(between receiver and message)*, trustsRegarding *(between Person and Topic)*	trustRegarding, reTopic, [trustsAboslutelyRe … distrustsAbsolutelyRe], ctxTRUSTS, [ctxtrustsAbosolutely … ctxdistrustsAboslutely], trustsRegarding, Trusts, rePerson, [trustsAboslutely … distrustsAboslutely]	Multiple axioms are inferable, for instance; 1) Stating topical trust; "A *Person* (Alice) *trustsAboslutelyRe trustsRegarding* (relationship) the *Topic* (Driving)", 2) Stating trust between two persons; "a *Person* (Alice) *trusts* another *Person* (Bob) *trustsAboslutely*"
PML	Belief Element, Trust Element, FloatMetric	Belief Relation (using *hasBelievedInformation* and *hasBelievingAgent* between *Agent, information* and *source*), Trust Relation (using *hasTrustee* and *hasTrustor* between *Agent, information* and *source*)	Agent, Source, Information, hasBelievedInformation, hasBelievingAgent, hasTrustee, hasTrustor, hasFloatValue,	Two kinds of Axioms regarding the trust and belief of agent in an information from a source can be inferred, for instance; 2) Stating trust; "*FloatTrust*, *hasTrustee* and *hasTrustor* *(agent: user's browser)* And *hasFloatValue* with *FloatMetric* (0.55). "
Konfidi	Relationship Item	About *(Between Item and Relationship)*	About, Truster, Trusted, Rating, Topic,	Trust Relationships can be stated like the following axiom; "A (trust) *Relationship* between *truster* (Alice) and *trusted* (Bob) exists, which is *about* trust *topic* (Cooking) with trust *rating* (.95)."

To further analyze the study we have done so far let's consider a set of analysis subjects that affect the discussion on the comparison between ontologies.

Depending on the context and the subject of the study certain approaches are used and implemented. If the subject of study is considering ontologies for knowledge management then, it is preferred to use an algorithm to compare ontologies, since such ontologies may be heavy and may contain a larg*e* number of concepts and properties. As a matter of fact we can use *weight* of ontology as the basis of comparison.

As all trust ontologies convey the same meaning and that is representation and modeling trust relationship, *Context* seems to be an important issue. So, we can compare trust ontologies depending on the context they have been modeled and considered in.

Since a model should also ease and facilitate the *inference* and computation of trust, then inference should be also an important topic to consider while analyzing trust ontologies.

Trust ontologies are used to generate trust networks and they serve as the gear to rotate the automation of trust network generation, inference and maintenance, therefore we can consider comparing ontologies based on the *ease of implementation* as well.

Ontologies should allow expressivity of trust statements. As axioms represent the trust expressions and statements on the social community of trust, then we can also consider the *semantic expressivity* of the axioms inferred based on the respective trust ontologies. Semantics of trust should be easy to understand and should allow inference and justifications.

The more trust ontologies incorporate and integrate technologies and *vocabularies* that create expressive and referenced, the more they will be easy to implement. Importing technologies and vocabularies make ontologies rich. As a matter of fact we can also consider basing our justification based on the number or technologies used in an ontology.

1) Weight

Considering the size of ontologies, Konfidi is the lightest ontology by having only two main concepts and 5 properties and only one single relationship.

PML has 5 main concepts, but there are 2 types of relationship existing with 8 instances, making PML trust ontology the second in the place.

While Golbeck's ontology has one single main concept (topical trust) and two other derived concepts (person and agent), 16 properties and one relationship, making it the third place holder. Trust ontology of Denker/Toivonen has 4 main concepts and 3 types of relationships, making it the heaviest ontological representation of all.

The reason for the excessive size of the number of properties of Golbeck and Denker ontologies, is the trust metric used; if the discrete scale between 0 to 10 was not chosen, and a probabilistic approach was used then the mentioned ontologies would be way lighter, bringing the total number of elements to 11 in Golbeck and to 14 in Denker/Toivonen, make them the top place holders at first and second place.

As a matter of fact we can conclude here that the choice of trust metric and the approach toward computational aspect of trust measurement could affect the size of ontology drastically.

2) Context / domain dependence

As described context is one of the most important subjects to consider while building a trust model for a domain of study. We also have to consider that there are main elements that affect the construction of trust ontologies that could alter their structure.

We want to consider construction of an ontology that could be based on the main axes of trust, semantic web and social network. Considering the main axes and elements that affect the structure of ontology, could create a drastically different ontology with a set of different components.

For instance if we consider the trust in service-oriented environments, we have to consider trust as a notion close to security, rather than belief and judgment. In that context trust is more close to reputation, while trust in the context of semantic web and semantic web driven social communities is more close to belief and justification.

As a result, context has a considerable impact of the constructing elements of trust ontologies.

Among the ontologies considered, Denker/Toivonen is the most context-dependant ontology, as the context of the trust study is communication and message-exchange. Taking a look into trust concepts incorporated into this ontology, we realize that the notion of trust relationship is tangled up in communicational concepts (Communication network, Message) make it completely dependent to communication context although the rest of the trust components are very well-engineered.

Since the trust ontology of PML is an axis of a triangle of provenance, justification and trust ontology, all of the mentioned ontologies are incorporated and imported into each other to take advantage of the technical facilities of ontologies description and consumption. This feature makes trust axis of PML ontology, dependent to other three ontologies and incorporating such ontology demands incorporation of the other two ontologies. At the same time this ontology is dedicated to evaluate and express the trust and belief of an agent into a piece of information taken from a source of information on the web. This feature makes it hard to express and conclude the trust between a set of persons, since the other pair should be described by agent as well, but it makes it easy to derive and justify the statements of a person and state the

belief and trust in the statement made by a person (for example on a social network). In general, the approach that PML follows is "Trust for Question Answering" [47]. As a result, PML trust ontology seems less context dependant in comparison to Denker/Toivonen and more customizable to the need for modeling trust, in general.

While Konfidi makes representation of trust in the context of social semantic networks fairly easy and straightforward, at the same time it is extensible and useful to different contexts and the future needs. Using the Konfidi's ontology, you can state a statement of topical trust between any set of resources or nodes (described by URI) on a semantic social network.

Golbeck's ontology seems the most essential and fundamental work on describing and stating trust using ontological modeling and representation for the consumption on semantic web. Both Konfidi and Golbeck's ontologies are among the most context and domain independent ontologies and that makes them easy to be customized and implemented in other domains of interests, demanding for modeling of trust.

We can state that the more ontology has components that directly expresses the trust relationships and has less components and properties related to other domains, the more context-independent it will be.

3) Inference capability

One of the most important issues while considering capturing of a domain inside the structure of ontology, is the reasoning based on that ontology.

Considering the subject of discussion, it should be possible to infer trust values easily using the corresponding trust ontology. As described, choice of trust metric plays a crucial role in the design and composition of ontology. Given a set of entities (for instance two persons located on a network), ontology should facilitate the inference of computational trust value for the given entities. There are certain factors that affect the efficient inference based on ontology such as the complexity and size of trust network generated. The lesser trust network generated is complex the lesser the inference mechanism implemented needs to be complex.

Golbeck's ontology was used for generating a network of semantic data, and was also used within a semantic web social network. Research has shown great inference capability for this ontology [27][28][29][31].Golbeck has studied the inference mechanisms and has created and implemented inference algorithm to study the trust inference based upon her trust ontology on two sets of trust networks, one a website for movie ratings and recommendations [30] and the other for spam filtering [28]. This makes Golbeck's trust ontology the only ontology widely used, implemented and inferred upon.

Konfidi is also tested against network of semantic data, and has shown good performance. Konfidi uses trust strategies to implement different sorts of inference mechanisms and algorithms, in order to test the inference capability of trust ontology, according to [10].

The inference capability of PML is implemented and has proven to be very effective as it is designated toward automatic resource evaluation.

It is important to consider that trust inference capability is an important factor that affects the implementation aspects of trust representation.

4) Semantic expressivity

Axioms that are inferred from trust ontologies express the semantics of trust. The more clear and expressive these axioms become the easier they will describe the semantics of trust within the implemented and stated context.

Golbeck's and Konfidi's respective ontologies state the semantic trust relationships very easy to understand and very expressive; for example using Konfidi; "*Relationship between truster (Alice) and trusted (Bob) exists, which is about trust topic (Cooking) with trust rating (.95).*" and using the Golbeck's ontology;" *"A Person (Alice) trustsHighlyRe trustRegarding a trustedPerson (Bob) on trustSubject (Driving)"*, adopted respectively from [27] [10].

As Denker/Toivonen use Golbeck's approach, but the axioms generated are less expressive as multiple contexts are taken under consideration and final driven axioms should have the notions of context, trust, communication. Considering all intermediary relationships for example, a trust relationship between person and topic could be described as; *"a Person (Alice) rePerson trustsAboslutelyRe (trust metric) trustsRegarding (relationship) reTopic Topic (Driving)"*, adopted from [27], which shows less expressivity than previous axioms.

As described in the table, PML has the less expressivity among all, but this is traded off with the inference capability of the ontology, as the inference should be consumed by software agents.

There seems to be a tradeoff between the expressivity of inference capabilities of ontologies; as the ontology becomes consumable by software agents, the less expressive the inference products become.

5) Size of trust networks

We discussed that the trust network should be automatically generated during runtime so we can analyze and evaluate and finally infer and compute the trust values based on the generated network.

As the size of the corresponding networks grows, the harder the crawling and walking the trust paths becomes. So, it is important to consider that the network generated could be analyzable and inferable. This has to do directly with the

structure based on which trust concepts and properties are presented and described.

For example Konfidi describes the topic and rating, as the extra edges on the network tree. The more topics we incorporate the larger the depth of the network generated becomes, so in order to increase the efficiency, authors of Konfidi's trust ontology state that the extra information attached to edges could be saved separately, according to [10].

As the semantic concept of trust relationship has been described very efficiently (using a small set of necessary elements, e.g. only one main concept), the networks generated are very well-formed. It is logical to state that the efficient design of ontology directly results on the efficient design of the networks generated and used.

As our ontology is introduced in next section, we use network size prospect to analyze the networks generated using our own ontology.

6) Vocabularies incorporated

As mentioned before, Golbeck's trust ontology was indeed a milestone in the field of the work being done for representing trust and belief in statements done on a semantic web-driven community and society.

She not only introduced a method of representing trust on semantic web and semantic web-powered societies, but she also introduced the notion of topical trust and subjective trust. By enabling the subjective trust we can state and represent how a sink and a source trust each other based on a specific subject and then measure this trust in subject and topic according to a specific trust metric.

Most of other works within trust representation on semantic web and semantic web-driven social networks either base their trust model completely or partially on Golbeck's trust ontology.

Denker and Toivonen incorporate the subjective and topical trust as well into their ontology. They also use the trust range of Golbeck for contextual trust and personal trust representation.

Konfidi also incorporates the topical trust. Although not standardized, topical or subjective trust is a requirement for any kind of model capturing the trust relationships. All of the studied ontologies take advantage of friend-of-a-friend (foaf) vocabulary. Golbeck and Konfidi use the foaf vocabulary to describe the two sides of trust relationship.

PML uses it to describe the agent that assesses and evaluates the information. Among studied ontologies, Konfidi incorporates and integrates the most number of vocabularies and technologies. In addition to foaf and topical trust vocabularies, Konfidi also incorporates relationship vocabulary [48] and it also uses WOT [45] (web of trust) vocabulary. Using the relationship vocabulary leaves space for adding other new features of trust relationships when needed; such as the date of initiation of trust relationship, terms of relationship, etc. Integrating different vocabularies, enriches the structure of the ontology, reduces the number of ontology components and eases the inference based upon the respective ontology.

Considering standardized vocabularies and ontologies, not only reduces the number of elements, but also eases future adoption of new properties of implemented vocabulary-driven features.

IV. Engineering and Construction of Trust Ontology

The same as all engineering sciences, in order to engineer an artifact, an iterative process should be considered where each step proliferates and extends the previous step in the loop to construct the artifact under focus.

Ontology engineering and learning is a semi-automatic process, consisting of six main interrelated phases, according to [50] [49].

These phases include: domain understanding, data understanding, task definition, ontology learning, ontology evaluation and refinement with human in the loop, respectively taken from [50] [49].

We use this approach in order to construct and build our trust ontology. We can state that our experience not only can serve as a methodology and mechanism for ontology construction but also, considering the domain of our problem, it can serve as a guide to engineering and construction of trust representations and protocols using ontologies.

1) Determining the domain and scope

Considering the domain of problem, we are engineering an ontology, which serves as the representational structure of the relationship visualizing trust and trustworthiness of a set of individuals based on a social network.

We can state that this ontology rotates on four main axes; Trust, Relation, Social network, Semantic Web. So, we can state that the domain of our ontology is representation of trust within a social network based on semantic web.

2) Understanding and learning the data

Domain and scope of ontology create boundary that captures the data relevant to the ontology under consideration.

Since our ontology serves as a representational model, then we understand that the focus will be put on the data that are represented, and that is trust relationships.

As relationships are compound data made of couple of atomic subcomponents, then atoms of relationships will form the data of our ontological domain. Relationships are described

between entities and these entities are individuals on the social network, connected with trust relationship together.

We consider persons on the social network, so data about people will serve as our data. Data about people on the social semantic network are described within FOAF files, which are described using RDF. At the same time Web-of-trust also provides data about the identity of people on our network as well as availability of links between these people on the network of relationships. As such relationships should describe trust as well, properties of trust are also among the pieces of information that are also useful to create data for ontology, such as the measurement and metric value used to describe the value of trustworthiness. In order to be able to describe the subject of the trustworthiness evaluation, we need also a subject list, so, available subjects and topics can be mentioned as available data on the domain.

The data needed within this ontology is information that composes trust relationships and properties that relationships have. The main data would be people's relationships and properties describing them and their relationships; here as mentioned metadata FOAF profiles of people can compose such relationships.

3) Defining tasks

Available data describe not only information about people that make the atoms of relationship molecules but also the properties of relationships. When domain is specified and the data available are recognized and learned, usages and functionalities of ontology being constructed is specified. Taking into consideration the domain and scope of ontology, which is representation of trust relationships and the data available that are information about people creating the relationships, we can state that the task of such ontology would be clearly, describing and representing trust relationships.

4) Ontology learning

Using the knowledge acquisition and learning capabilities with the help of our construction and development environment, we are able to learn the ontology.

As the main component of the ontology is relationship, that represents the connection between entities on the network then *relationship* itself serves as the main component and concept of this ontology.

We can think of relationship as a composite object made of subcomponents that reside within the relationship and describe the properties of relationship. Each relationship describes an edge on the network, this edge exists between a set of nodes. These nodes represent starts and ends of directed edges (of relationship). *hasTruster* and *hasTrustee* respectively represent the two important properties of relationship on a network. So far we have learned the elements of relationship on a social network.

Every relationship has a set of main properties, which describe the nature and purpose of relationship. These properties specify the details of trust relation. Each trust relationship has a *topic* or *subject* (topical or subjective trust). In order to make trust computable, on any existing edge on the network there should be a value. This value represents the trust metric used for the representation of trust relationship. So, we can consider Value also as a main property of relationship.

Now that we have learned the main elements of ontology, it appears most of the trust ontologies share the same components described so far. Relationship described using ontologies have a set of *auxiliary properties*, as well. Using this component we can put more details on the relationship and we can give it more weight and mass. It is important to realize that only properties that have less importance than main properties, are described using these properties. These properties are used to give more weight to Relationship. Using a separate element for auxiliary properties leaves space for future extensions that are needed to add to the network

Trust relationships are context-sensitive. *Context* describes whether this relationship is described inside a personal network or a business network. By using context, we can make networks of different types. Using this element we can create simple networks and hybrid networks.

For instance, simple networks are either a personal network (such as Orkut [56]) or a business network (such as LinkedIn [57]). We can have a relationship in the context of a personal network. We can also have a simple trust relationship in the context of a business network or perhaps a business environment. When the source is from a personal network and is connected to a sink from a business network we have connected two networks of simple type, creating a hybrid network. As a matter of fact context type can give more details about the type of network where this relationship is described in. This auxiliary element gives more details about the type of network the relationship is based upon.

Considering the reason that a relationship can be established based upon, we have also incorporated a *Goal* property describing the reason that a relationship was based upon. A relationship can have a goal that describes why respective relationship is formed. For instance on a social network, usually the goal for establishing a relationship is friendship, or on a business network, it is seeking business partnership.

The most important subsidiary and optional property that we have considered in our ontology is having a *recommender* as the initiator of the trust relationship establishment. *hasRecommender* is an auxiliary property describing a person on the network that has recommended trustee, or the sink of relationship, to the truster. In other words, we have described notion of "trust in recommendation" in order to shape and form a relationship, initiated from truster, ended up in trustee, based on guarantee of trust recommender. Using such property we can create networks of different strengths; we can have networks of weak links and strong links.

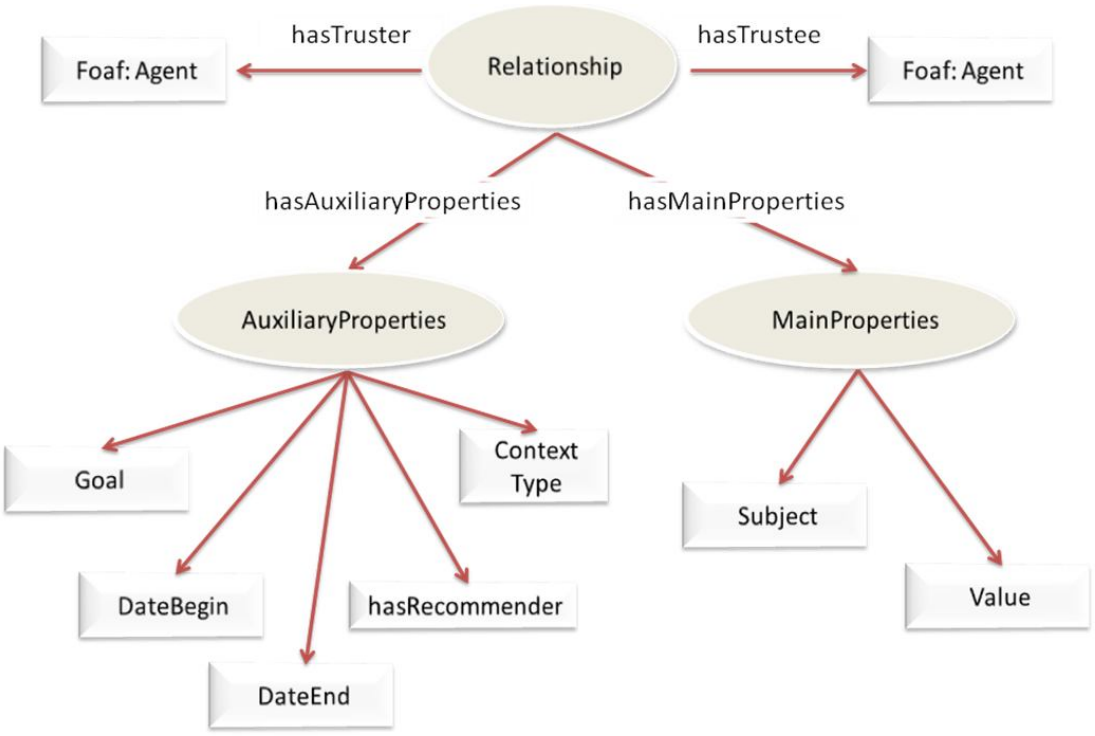


Fig. 1. Structure of our trust ontology, 3 main concepts of trust ontology as well as two edges connecting them together. [2]

A *strong link* is a relationship based upon the recommendation of an entity. The more recommenders a relationship has, the stronger this relationship become. A *weak link* is a relationship that has no recommenders.

When speaking in terms of trust, in context of information systems, a way of achieving trust is using a recommender. Considering the transitivity property of trust, the trust in recommender is used in certificate authorities to achieve trust in a third-party. We can take advantage of this property in semantic-web driven social networks to create strong paths in order to use them as the path for aggregating and computing trust values along the network.

By specifying auxiliary properties we follow two important goals; Adding more details about relations to ontology and giving more meaning and details to specification of relationships, as well as leaving space for adding more elements describing the other aspects of relationships that may be needed in future.

5) Ontology evaluation

As ontology development is a semi-automatic approach and demands involvement of both human and machines, in this phase as well as previous phase we take advantage of using an automated tool in order to build and evaluate our ontology. In this phase we build and evaluate the ontology learned in previous phase. By evaluating the ontology, we estimate the quality of the modeled solution to the addressed tasks defined in previous sections.

It is worth mentioning that in most of the phases of ontology engineering the role of human wouldn't be completely fade and human will participate in almost all of the phases of ontology development. In order to model and describe the elements and components of the ontology we use Protégé[3] ontology editor and knowledge acquisition system.

Figure 1 visualizes the structure of our trust ontology.

As shown our ontology has 3 main concepts or classes that capture the structure of the trust relationships on the networks.

Relationship is the main element and concept of our ontology. *MainProperties* and *AuxiliaryProperties* are the other main components of our ontology. We have two associations that connect both *MainProperties* and *AuxiliaryProperties* to *Relationship*. These associations are *hasMainProperties* and *hasAuxiliaryProperties*.

Relationship always has a sink and a source, which we have described here as *truster* and *trustee*. Both *hasTruster* and *hasTrustee* are defined on the range of *foaf:Agent* which enables us to describe relationships in the context of semantic social ecosystems. This agent can be a person, an organization or just a software agent. Each Relationship has to have a truster and a trustee and at least one main property. Without these mentioned elements, a relationship is partial and partial relations are undefined using our ontology. In order to ensure having at least these mentioned elements, we have put restrictions on ontology subcomponents. Restriction defines a blank node with restrictions. It refers to the property that is constrained and defines the restriction itself. Cardinality

[3] *Protégé*, http://protege.stanford.edu/

constraints define how many times the property can be used on an instance of a class. We have minimum, maximum, exact cardinalities.

We have used two exact cardinalities on *hasTrustee* and *hasTruster*, in order to state having exactly one truster and one trustee for a relationship. We have also used minimum cardinality for *hasMainProperties* to make sure having at least a topic and a value for each relationship, and since we can have more than one topic to base the relation upon, we have used minimum cardinality (at least).

MainProperties element has two main properties; *Subject* and *Value*. We have described these two properties using data type properties, in OWL (Web Ontology Language). Subject takes string value. It is recommended that subject taxonomies or topic ontologies be defined, so we can use a common namespace for describing topics and subjects. Each relationship can have multiple main properties, which means it can be about different topics and subjects, but each main property has to have one and only one topic and only one value.

For instance in the relationship between Alice and Bob, Alice can completely trust Bob on Driving (Subject="Driving", Value="0.95"), and also can distrust Bob on Cooking completely (Subject="Cooking", Value="0.10"). This constitutes two distinct main properties in relationship between Alice and Bob. But we cannot have multiple subjects and values in the *MainProperties* of Alice and Bob on Cooking, for example. In order to enforce this property we have put restriction on both properties of value and subject. By using exact cardinality restriction we have enforced having exactly one subject and exactly one value for each item of trust within a relationship.

Finally, *AuxiliaryProperties* concept of domain has 5 properties and also leaves space for more properties whenever needed. *AuxiliaryProperties* has an object property and 4 data type properties. It has *hasRecommender*, which is the element describing the strength of relationship and is defined on the range of *foaf:agent* that lets us to state which node on the network is the recommender for the establishment of this relationship. *ContextType* is defined as a string data type property that states the context of the trust network, the relationship is based on. *Goal* of the relationship is also defined using a string data type property. *DateBegin* and *DateEnd* are described using Date data-type property. Clearly we don't need to have restrictions on any single property of *AuxiliaryProperties* concept.

6) Discussion

As modeling trust is the main target of our work, a brief discussion on the notion of trust and how we have modeled the trust in our approach seems necessary.

As discussed, trust is a context-sensitive issue. While considering the context of the trust ontology and trust analysis, we realize that this context is a multi-dimensional entity composed of two substantial and main dimensions; semantic web and social networks. Trust in the domain of social semantic networks, has three relatively close notions such as belief, provenance and justification.

Some of these notions have very close and sometimes overlapping meaning to trust. Among mentioned notions, belief seems to be a very close notion to trust. It seems that belief and trust go hand in hand.

Discussion on modeling belief has a long background. The work on belief goes back to Willard Van Orman Quine's "web of belief" [22]. A reminiscent of web of trust is created by [23] and is weaved into semantic web. They define web of belief as following "by cognitively viewing knowledge as individuals' rational beliefs about the world, individuals share knowledge and form a distributed knowledge network, which is called the *web of belief*, where rational belief links individuals with world facts and trust interlinks individuals as external information sources." [23].

In our work, we have only considered modeling trust and distrust. Considering modeling other notions described takes a great effort and deal of modeling, as each one of these mentioned notions demand their own properties and eventually their own ontologies.

As a matter of fact, as we have generalized the notion of trust relationship in our approach to Relationship, then we have provided enough space for future extension. We can build belief ontology that can be imported within our trust ontology and certain elements of these ontologies can be shared and consumed whenever needed. Aside from such possibility then there is a need for future research for defining the nature, usage and representation of belief and judgment in semantic social networks.

Using our ontology, we can describe trust in other people on the network regarding a certain topic. Taking into account the discussions we had in previous section, what we are describing here is trust in performance.

When we state that "Alice trusts Bob regarding Driving", this means that, "Alice trusts in *eventuality of performance* of Bob to some extent, when the act of driving is performed". Trust in performance describes that truster states the trust in the performance of act of trustee, when this act is performed. This trust uses a probabilistic approach to describe trust relationships, so we can say how much someone trusts the other on a range between 0 and 1.

For example, as shown previously we can state, Alice trusts Bob completely regarding a topic. This amount of trust is mapped to a floating point value between 0 and 1, so we can state range of 0.9 to 0.99, is a range showing that you completely trust the person you are expressing trustworthiness about. Considering the discrete range of Golbeck's ontology, which is between trust0 to trust10, then we realize that we are having an implicit mapping from a range of discrete values to

a range of concrete values. Choice of trust topic is also considerable for improvement in future works.

As we stated, we have modeled *Specific Trust* and we have clearly eliminated the notion of general trust. It is important to point out that a relationship should have at least a topic. One of the important notions that we can consider discussing here, is *distrust*.

For instance, *"Alice distrusts Bob regarding babysitting to some extent (0.65)"*, using our ontology it can be also stated like *"Alice trusts Bob regarding babysitting to some (complementary) extent (0.35)*", adopted from [27] [10]. As it is clear we have modeled distrust, implicitly. We have assumed that there is a tradeoff between trust and distrust on the same topic.

We can also model feelings using our trust model. If we take all of the evaluation values for a relation, and average it, we can derive the amount of feelings between the trustee and truster. We can derive negative or positive feelings. If there are certain number of trust items (or *MainProperties*; subjects and values) for a relationship, for instance at least 3, we can consider taking average of the values and deriving a general feeling of truster for trustee.

For instance, if Alice has low trust values for Bob in all of the subjects in their relationships, then we can state that she has negative feelings for him, or vice versa. Although, there are many certain properties that should be considered that affect feelings of people for each other and trust is only one of them. Therefore, we can state here that more elements are needed to give us this ability to create feelings statements in our ontology.

We want to be able to choose two nodes, a source or truster and a sink or a trustee (trusted), and gather trust values on a path between them on the network and eventually compute a value representing the trust of truster in trustee. In order to address this problem; we have made sure that each relationships on the network has a value, and we have introduced recommenders.

Our ontology ensures that if there is a relationship (a link on the network) between two nodes, then this link has a value, although this value doesn't reflect the general trust value of trust between truster and trustee. In addition to using recommenders, we can use our ontology to create a network of recommendation on the network of trust.

We can use recommended links for our trust inference. As we described, recommendation can state the strength of an existing link, so we can use such "recommended link" for our inference along the paths. Theoretically, such paths are stronger and can give better values than other paths that do not have recommenders.

One of the main challenges in this context is dealing with distrust values, when encountered on the network. Values of distrust drop the aggregated values along the paths on the network, and there is no certain procedure or methodology to address dealing with this problem.

V. Trust Network Analysis

We begin by analyzing a network of small size. This gives us the ability to easily, visualize and realize the structure of modeled relationships. Then we move to networks of larger size where we introduce two types of trust network structures; hybrid and meshed networks.

A. A small size network

Let us begin with the smallest network size, possible; a network of two people, with a single relationship, containing a main property and an auxiliary property. Let us consider modeling following relational semantics for this atomic network:

"Alice trusts bob in driving a lot."

Using our OWL trust schema and ontology, this network will be presented in RDF format as following;

```
<foaf:Person rdf: ID="Alice"/>
<foaf:Person rdf:ID="Bob"/>
<Relationship rdf:ID="Relationship_Alice_Bob">
      <hasTrustee rdf:resource="#Bob"/>
      <hasTruster rdf:resource="#Alice"/>
   <hasMainProperties>
      <MainProperties rdf:ID="MainProperties_Alice_Bob">
         <Subject rdf:datatype="&xsd;string">Driving</Subject>
         <Value rdf:datatype="&xsd;float">0.95</Value>
      </MainProperties>
   </hasMainProperties>
</Relationship>
```

B. Hybrid trust networks

Here, we will consider 2 groups of people, representing two networks of different contexts. Each group of four people is interrelated and interlinked, forming a *simple network*. At the same time a set of these people are connected outside of their own local networks, to other foreign network.

These relations work as glue connecting networks of different context, creating *Hybrid networks.*

In hybrid network depicted in Figure 3, people located on one network, are shaping a personal context and their goals are more or less establishing friendship relations, while people on the other network are members of a business network, and their goals are establishing business partnerships and relationships and they could be colleagues in an office environment. It is also considerable to think of the business network as a business-value adding network, or a service oriented environment. In that case, then four latter members

can be software agents, which can also be described using our ontology.

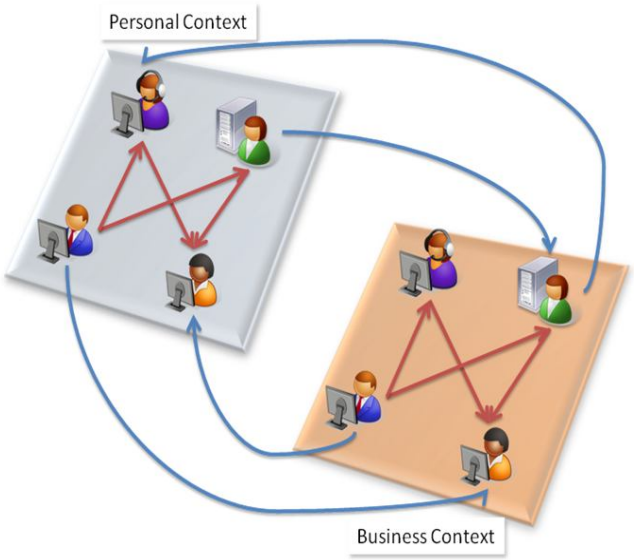


Fig.3. A hybrid network. Two connected networks of different contexts; a personal and a business network. Hybrid networks, contains 8 people and 12 relations. 8 links are interconnections (local), and 4 links are acting as glue connecting two networks (foreign).

In order to consider the structure and size of the network generated, a circular representation of network is given in Figure 4.

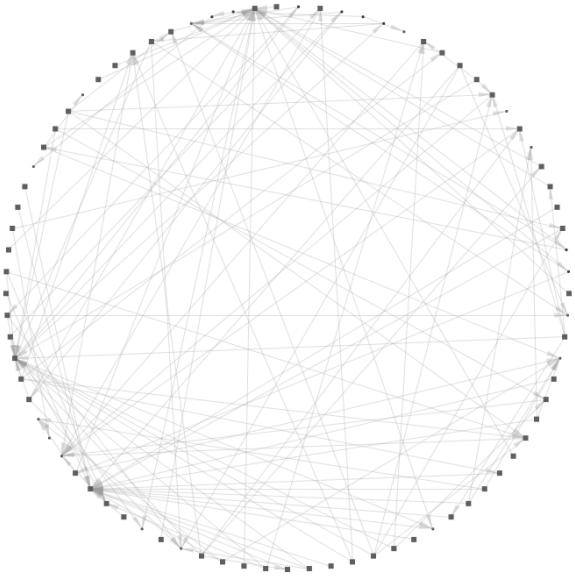


Fig.4. a circular representation of hybrid network subject to study. (Network contains 48 nodes and 92 edges)

Figure 4 visualizes the RDF trust network depicted in Figure 3. Figure 4 is visualized using Welkin[4].

C. *Meshed trust networks*

The motivation for studying larger networks of trust, was considering real-world scenarios of network formations. Such networks are complex, combined networks of different sizes and different contexts. We call these networks, *Meshed networks*.

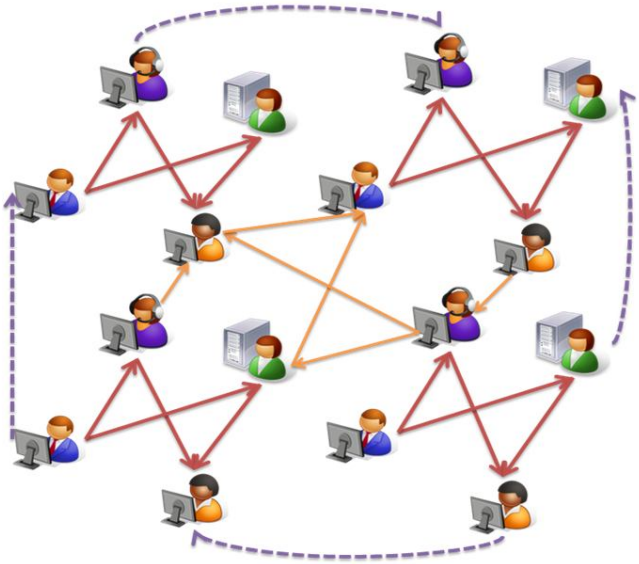


Fig. 5. A partial meshed network made-up of two connected hybrid networks. This network contains 16 people and 26 relations.

Meshed networks are considered networks, where every node is connected to all other nodes on the network.

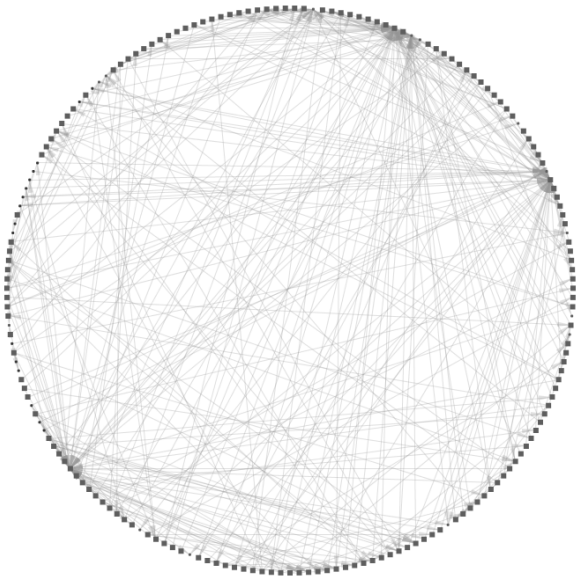


Fig. 6. A circular representation of meshed partial network. (Network contains 98 nodes and 198 edges)

As such, assumption is unrealistic, and there is only a subset of nodes available that are fully connected to all other nodes, we consider *partial* and *fully connected meshed networks*. Taking idea from networking topologies, partial meshed networks are trust networks where each node is at least connected to a subset of nodes it has data exchange with. On the other hand, a fully connected meshed network is a trust network where each node is connected to everyone.

[4] Welkin, http://simile.mit.edu/welkin/

In the former, inferring trust values between a pair of nodes on the network seems difficult but, finding a path between a set of nodes on the network is guaranteed. Using our ontology, recommendations can find efficient paths on the network.

Figure 5 depicts a partial meshed network of people from different contexts and with different goals perhaps, and can be thought of two hybrid networks integrated and merged together. Figure 6 is a visualization of the RDF network for trust network depicted in Figure 5.

VI. STRUCTURAL COMPARISON

In order to emphasize the importance structural determination of trust networks, in this section we consider comparing the structure of the trust networks generated based on three different ontologies; our ontology, Golbeck's and Konfidi's. In the last subsection we discuss in details the results of comparison.

For the sake of comparison, we have divided the experiment datasets into two sizes; small sized networks and large sized networks.

A. Trust networks of small size

Based on our structural point of view, Table 2 lists the number of nodes and edges on the compared networks.

TABLE II
COMPARISON BETWEEN THE SIZES OF SMALL NETWORKS

Trust Networks	Golbeck	Ours	Konfidi
Nodes	15	20	22
Edges	28	34	37

c) Networks of 4 people and 4 relationships. (Increase in size)

Trust Networks	Golbeck	Ours	Konfidi
Nodes	19	28	29
Edges	46	54	58

d) Networks of 4 people and 6 relationships. (Increase in depth)

As it is clear, in general the nodes and edges on the networks generated using Golbeck's ontology is quite smaller than networks generated using our ontology and Konfidi's.

At the same time in both cases our network has a smaller number of nodes and edges than Konfidi's networks, although the difference is not that much.

B. Trust networks of large size

We described and defined hybrid and meshed networks. At the same time, we modeled these networks using datasets that to some extent reflect the structure of such networks. The same datasets were also injected into the structure of two other tested ontologies to consider the structure of the resulting trust networks.

Based on our structural point of view, Table 3 lists the number of nodes and edges on the networks.

TABLE III
COMPARISON BETWEEN THE SIZES OF LARGE NETWORKS

Trust Networks	Golbeck	Ours	Konfidi
Nodes	27	48	50
Edges	73	92	105

a) Hybrid Network (network of 8 people and 12 relationships).

Trust Networks	Golbeck	Ours	Konfidi
Nodes	49	98	86
Edges	132	198	211

b) Meshed network (Networks of 16 people and 26 relationships).

Table 3a shows the number of nodes and edges on the networks representing the hybrid network.

Network generated using Golbeck's ontology has less nodes and edges than both of ours and Konfidi's. Although, network generated using our ontology has less number of edges and nodes in comparison to Konfidi's.

Table 3b shows the number of nodes and edges on the networks representing meshed networks.

Again, Golbeck's network has less number of nodes and edges than our network and Konfidi's network. Our network has greater number of nodes than both, Golbeck's and Konfidi's networks, but lesser number of edges than Konfidi's.

C. Trust networks of larger size

We continued our study by modeling and presenting the trust networks of larger sizes.

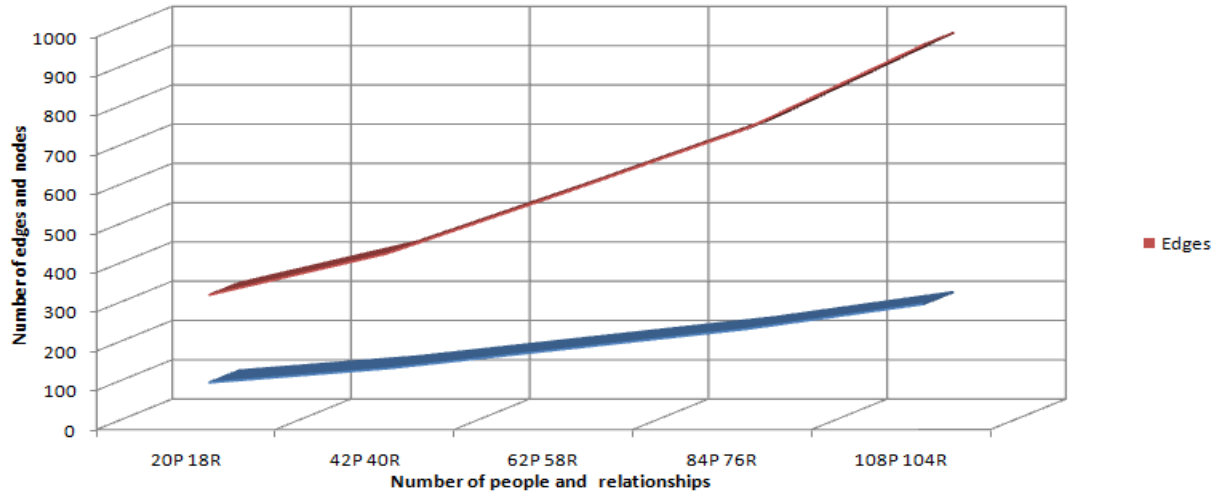
We also expanded our sample partial meshed network and increased the number of people in the networks and their corresponding relationships randomly.

The structure of the resulting networks was studied from the perspective of number of edges and nodes, the same structural perspective used for comparison between networks of small and large size.

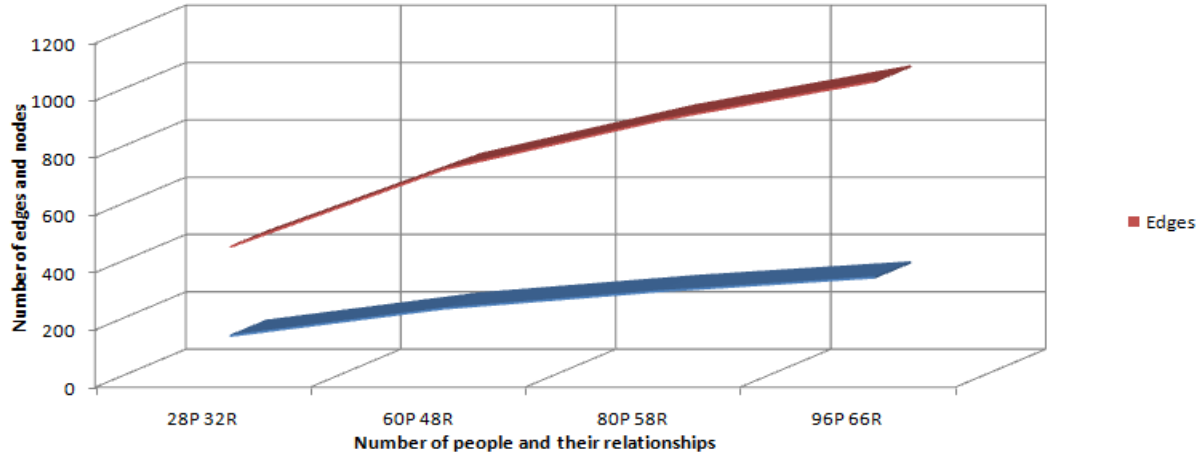
In our experiment we expanded the sample partial meshed network of 16 people and 26 relationships. The number of people and their corresponding relationships were sampled and plotted at each sample increase to reflect the progress of expansion across the network structure.

These data were generated using all three ontologies being evaluated.

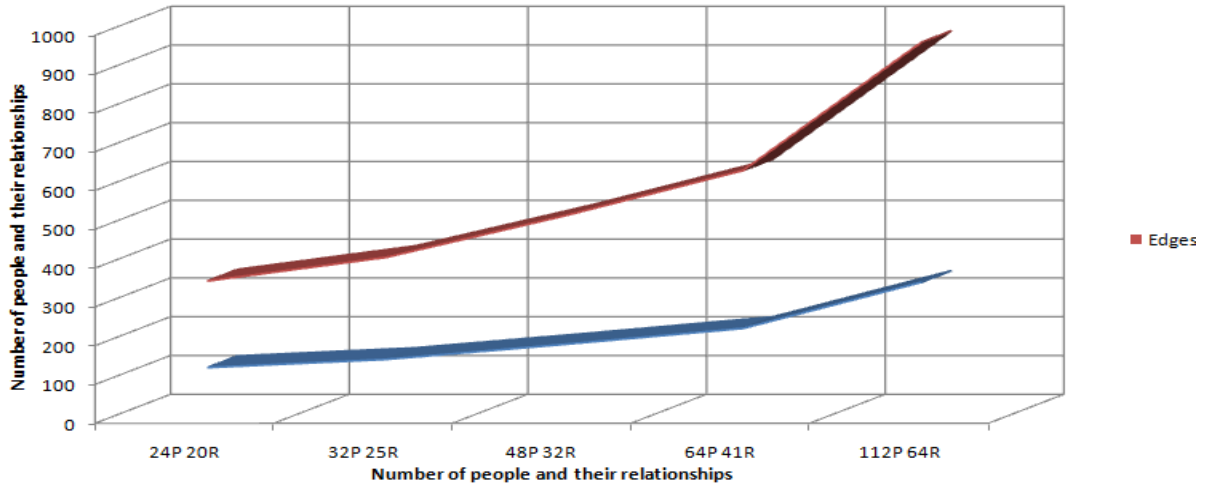
Figure 7, depicts the effect of seamless increase in the size of trust networks of larger size from structural point of view.



a) Increasing the size of Golbeck's trust networks. The diagram depicts the increase in range of nodes and edges, starting from network of 20 people and 18 relations, ending at a network of 108 people and 104 relations.



b) Increasing the size of Konfidi's trust networks. The diagram depicts the increase in range of nodes and edges, starting from network of 28 people and 32 relations, ending at a network of 96 people and 66 relations.



c) Increasing the size of our trust networks. The diagram depicts the increase in range of nodes and edges, starting from network of 24 people and 20 relations, ending at a network of 112 people and 64 relations.

Fig. 7. Networks of larger sizes: Effect of increasing the number of people on the networks described using different ontological structures.

D. Detailed analysis of structural comparisons

In this section we further analyze and study the results of our experiment and comparisons.

As shown in Tables 1 and 2, trust networks modeled, described and presented using our ontology and others are compared based on the number of nodes and edges (structural perspective). Comparison shows that in networks of small size, our ontology shows average performance in comparison to other ontologies, meaning that trust networks generated have average sizes, in comparison. But as the size of the networks increases, certain aspect of trust network size increases more than other compared network, showing less efficient performance. This decrease in efficient performance is also well-depicted in networks of larger size in Figure 7.

There are a set of reasons, which can be stated here.
Clearly, the main reason, for size increase in networks, is the number of elements incorporated within the structure of ontology. Golbeck's ontology uses only one main element, Konfidi uses two main elements, while our ontology uses three main concepts.

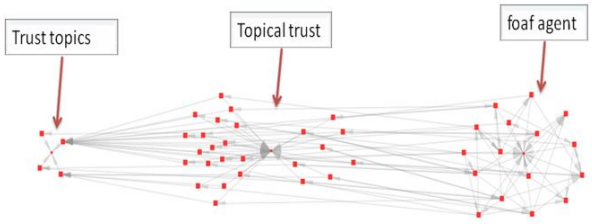


Fig. 7. A clustered visualization of the structure of a meshed trust network based on Jennifer Golbeck's ontology. This network contains 49 nodes and 132 edges.

The second reason would be efficient design of the ontology. Golbeck's ontology is indeed, a mile stone in the work on trust in semantic web, from different perspectives.

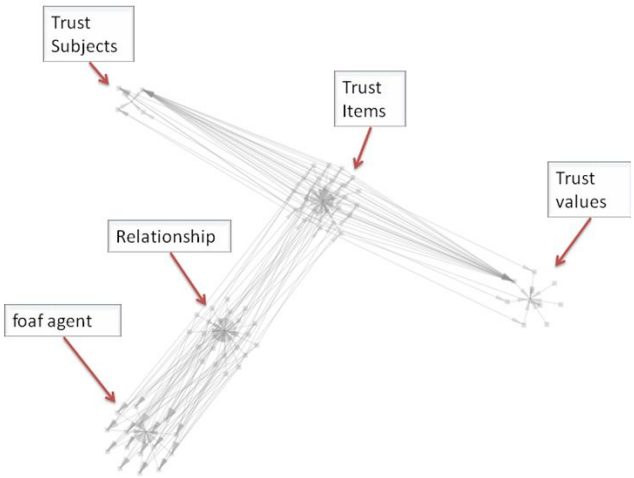


Fig. 8. A clustered visualization of the structure of a meshed trust network based on Konfidi's trust ontology. This network contains 86 nodes and 211 edges.

Her trust schema has a very efficient design. Such design has certain aspects that reduce the size of the networks described using that ontology; first, defining levels of trust (trust0...trust10) and trustRegarding on the range of *foaf:agent* lets you describe the trust directly as the properties of agents and on the trust network. Such efficiency in design lets you describe relations very easily with lesser elements, as seen in results. Konfidi's trust ontology has more or less the same structure like our ontology. Our ontology has one more element than Konfidi's, however we have seen networks of smaller size generated by using our ontology have less complex structures than the ones generated by using Konfidi's ontology.

Figures 9 visualizes the structure of the networks generated using our ontology. The emphasis on the visualizing was put on the gravity of the instances on the network toward their originated main elements. An efficient structure will depict the overall organization of the ecosystem and its sub-ecosystems. Our network shows better clustering of elements among the two other samples.

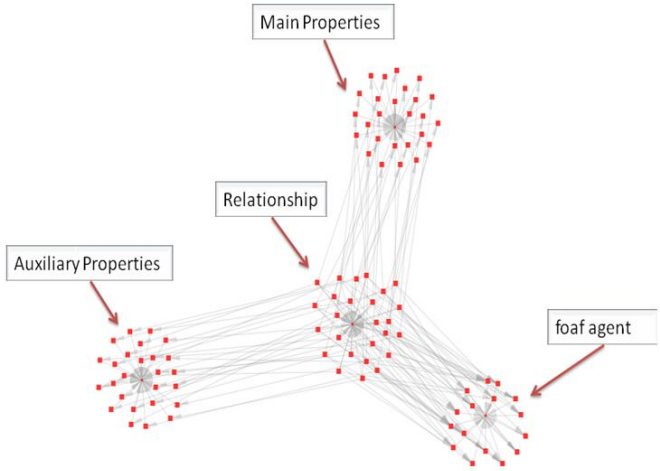


Fig. 9. A clustered visualization of the structure of a meshed trust network based on our trust ontology. This network contains 98 nodes and 198 edges.

The third reason is the *AuxiliaryProperties* element of our ontology. As we incorporated an extensibility element for describing secondary and optional properties, we will incorporate extra nodes and more importantly extra edges into the network. In most of the test data for the comparison section, we have auxiliary property elements with at least one sub-element filled. For instance, when describing hybrid networks, all relationships have *AuxiliaryProperties* with *ContextType* property of either simple social network, or simple business network, or hybrid network. It should be mentioned here that none of the other compared ontologies, have any element for describing extra properties; extending Golbeck's trust ontology seems to be very hard and needs drastic changes because of its architecture, and Konfidi doesn't have any elements for describing extra properties. Taking into account this information, if we eliminate the *AuxiliaryProperties* element, then the size of our network becomes even more efficient than both other ontologies, in certain situations.

VII. Conclusion

We analyzed the modeling and representation of trust relationships across the networks within semantic web-driven ecosystems. In order to capture, model and represent the semantics of trust relationships within semantic web, main components of relationships are represented and described using ontologies. To analyze the methodologies and mechanisms used to described trust relations, we studied and analyzed a set of trust ontologies, specially Jennifer Golbeck's and Konfidi's trust ontologies, which share the same context with our research context. At the end, we engineered and analyzed a trust ontology based on the context of our research, social networks and semantic web.

We constructed a trust ontology in which relationship is the focus of ontology, as ontology captures the semantic of trust relationships, and two other elements state the properties of trust relationships. In comparison to previous works, there are certain new features that our work introduces to trust ontologies in this context; using our *AuxiliaryProperties*, we give relationships more weight and meaning. We have introduced the *hasRecommender* property that can determine the strength of the links on social network and can be used for finding the suitable inference path on the network.

We claimed that determining the structure of trust networks could be possible by efficiently designing and engineering trust ontologies that such networks are based upon. We also demonstrated this fact by using the same datasets on both our ontology and two other ontologies. Results of our experiment fairly prove our claim. Having more elements than other ontologies, networks generated based on our ontology show average size and structure. Also our trust networks shows far more manageable structure and architecture as the size increases, in comparison with two other compared ontologies.

As a conclusion, we can state that ontologies are very promising technologies. Utilizing ontologies in modeling and representing trust in semantic web-enabled social systems seems to be a highly efficient methodology and mechanism.

VIII. Future work

Studying the social phenomena within computer science and especially semantic web, demands more attention. I believe by having a liaison between social sciences and computer sciences, more fruitful results can be achieved, that can help bringing social ecosystems into life on the web.

Number of vocabularies, used to describe the elements of ontologies should increase. There is a vocabulary to express relationships [48], but there is no standard vocabulary to express for instance, common subjects and topics of a relationship, while we can describe vocabularies using we can easily describe a vocabulary for this matter.

The application domain is very limited and one of the most important future works on this field is spotting certain fields that demands further attention. Current applications are just limited to Spam filtering and user rating systems across web sites on internet.

One of the most important future works is spotting further applications for social trust, where trust relationships can be modeled and expressed using ontologies.

References

[1] H. Mariotti, "Autopoiesis, Culture, and Society", (Accessed June 26, 2005). Available at: http://www.oikos.org/mariotti.htm

[2] N. Dokoohaki, M. Matskin, "Structural Determination of Ontology-Driven Trust Networks in Semantic Social Institutions and Ecosystems", Proceedings of the International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM'07) and the International Conference on Advances in Semantic Processing (SEMAPRO 2007), November 4-9, 2007 - Papeete, French Polynesia. 2007, ISBN 0-7695-2993-3, IEEE Computer Society, Los Alamitos, CA, USA, pp. 263-268.

[3] S. Milgram, "The Small World Problem", Journal of Psychology Today, Vol. 1 (1), pp. 60-67, (1967).

[4] S. Downes, "The Semantic Social Network", published February 14, 2004, (2004). Retrieved from: http://www.downes.ca/post/46

[5] S. Downes, "Semantic Networks and Social Networks". The Learning Organization Journal, Emerald Group Publishing Limited, ISSN 0969-6474, Vol. 12, No. 5, pp. 411-417, (2005).

[6] D. Brickley, L. Miller, "FOAF Vocabulary Specification, Namespace Document", September 2, 2004, Available at: http://xmlns.com/foaf/0.1/

[7] A. L. Cervini, "Network Connections: An Analysis of Social Software That Turns Online Introductions into Offline Interactions", Master's thesis, Interactive Telecommunications Program, New York University. (2003).

[8] Ch. Li, "Profiles: The Real Value of Social Networks", Forrester. July 15, (2004). Available at: http://www.forrester.com/Research/Document/Excerpt/0,7211,34432,00.html

[9] M. Gladwell, "The Tipping Point: How Little Things Can Make a Big Difference", Little, Brown & Company, Boston, MA. ISBN 0-349-11346-7. (2000).

[10] D. Brondsema, A. Schamp, "Konfidi: Trust Networks Using PGP and RDF". Proceedings of the WWW'06 Workshop on Models of Trust for the Web (MTW'06), Edinburgh, Scotland, UK, May 22, 2006 (2006).

[11] J. G. Breslin, A. Harth, U. Bojars, S. Decker, "Towards Semantically-Interlinked Online Communities", Proceedings of the 2nd European Semantic Web Conference (ESWC'05), Springer, (2005).

[12] SIOC (Semantically-Interlinked Online Communities). Available at: http://rdfs.org/sioc/

[13] D. Brickley, S. Stefan, A. Miles, L. Miller, D. O. Caoimh, C. M. Neville, "SIOC Ontology Specification", (2007). Available at: http://rdfs.org/sioc/spec

[14] U. Bojars, J. G. Breslin, A. Passant, "SIOC Ontology: Applications and Implementation Status". W3C Member Submission, (2007). Available at: http://www.w3.org/Submission/sioc-applications/

[15] S. Wasserman, K. Faust, D. Iacobucci, M. Granovetter, "Social Network Analysis: Methods and Applications". Cambridge University Press, ISBN 0-521-38707-8 (1994).

[16] J. P. Scott, "Social Network Analysis: A Handbook". Sage Publications, London. ISBN 0-7619-6338-3 (2000).

[17] I. Cantador, P. Castells, "Multilayered Semantic Social Network Modeling by Ontology-Based User Profiles Clustering: Application to Collaborative Filtering", No. 4248, pp. 334-349, Lecture Notes in Computer Science – Springer, ISSN 0302-9743 (2006).

[18] B. Aleman-Meza, M. Nagarajan, C. Ramakrishnan, L. Ding, P. Kolari, A. P. Sheth, I. Budak Arpinar, A. Joshi, T. Finin, "Semantic Analytics on Social Networks: Experiences in Addressing the Problem of Conflict of Interest Detection". Proceedings of the 15th international conference on World Wide Web, (2006).

[19] P. Mika, “Flink: Semantic Web Technology for the Extraction and Analysis of Social Networks”, Journal of Web Semantics: Science, Services and Agents on the World Wide Web, Vol. 3, No. 2-3, pp. 211-223, (October 2005).
[20] T.W.A. Grandison, “Trust Management for Internet Applications”. PhD thesis, Imperial College of Science, Technology and Medicine, University of London, Department of Computing, (2001).
[21] T.W.A. Grandison, M. Sloman, “A Survey of Trust in Internet Applications”, IEEE Communications Surveys and Tutorials, 1553-877X, Vol.3, No. 4, Page 2, (2000).
[22] W.V.O. Quine, J. S. Ullian, ”The Web of Belief”, Random House, New York, ISBN 0-394-32179-0, (1978).
[23] L. Ding, T. Finin, “Weaving the Web of Belief into the Semantic Web”, Proceedings of the 13th International World Wide Web Conference, (2004).
[24] A. Abdul-Rahman, S. Hailes, “A Distributed Trust Model”. Proceedings of Workshop on New Security Paradigms. (1998).
[25] J. Huang, M.S. Fox, “An Ontology of Trust – Formal Semantics and Transitivity”, Proceedings of the 8th ACM International Conference on Electronic Commerce. Fredericton, New Brunswick, Canada, pp.: 259 – 270, ISBN 1-59593-392-1, (2006).
[26] PML 2 Trust Ontology. Available at: http://iw.stanford.edu/2006/06/pml-trust.owl
[27] J. Golbeck, B. Parsia, J. Hendler, ”Trust Networks on the Semantic Web”, ISSU 2782, pp. 238-249, Lecture Notes in Computer Science – Springer, (2003).
[28] J. Golbeck, J. Hendler, “Accuracy of Metrics for Inferring Trust and Reputation in Semantic Web-based Social Network”, ISSU 3257, pp. 116-131, Lecture Notes in Computer Science – Springer (2004).
[29] J. Golbeck, “Computing and Applying Trust in Web-based Social Networks”, University of Maryland, (2005). Available at: https://drum.umd.edu/dspace/bitstream/1903/2384/1/umi-umd-2244.pdf
[30] J. Golbeck, “Inferring Trust Relationships in Web-based Social Networks”, ACM Transactions on Internet Technology, Vol. 7, No. 1, (2006).
[31] J. Golbeck, “FilmTrust: Movie Recommendations from Semantic Web-based Social Networks”, IEEE Consumer Communications and Networking Conference, (2006).
[32] D.L. McGuiness, P.P. Da Silva, L. Ding, “Proof Markup Language (PML) Primer”, (2005). Available at: http://iw.stanford.edu/2005/wd-pml-primer/
[33] Konfidi, Available at: http://konfidi.org/
[34] G. F. Davis, M. Yoo, W.E. Baker, "The Small World of the American Corporate Elite", Journal of Strategic Organization, Vol. 1, No. 3, pp.301-326, Springer, August 2003, (2003).
[35] C. C. Foster, A. Rapoport, C. J. Orwant, “A Study of a Large Cociogram: Elimination of Free Parameters”. Behavioral Science, Number 8, pp.56-65. (1963).
[36] M. E. J. Newman, "The Structure of Scientific Collaboration Networks," Proceedings of the National Academy of Sciences; 98: 404 - 409. (2001).
[37] D. Watts, “Small Worlds: The Dynamics of Networks between Order and Randomness”. Princeton, NJ: Princeton University Press, ISBN 0-691-00541-9, (1999).
[38] D. Watts, S. H. Strogatz, "Collective Dynamics of Small-World Networks", Journal of Nature, MacMillan Magazines, London, ISSUE 6684, pp. 440-442, (1998).
[39] M. S. Fox, J. Huang, “Knowledge Provenance: An Approach to Modeling and Maintaining the Evolution and Validity of Knowledge”. 22 May 2003, (2003). Retrieved from: http://www.eil.toronto.edu/km/papers/fox-kp1.pdf
[40] J. Huang, M. S. Fox, "Trust Judgment in Knowledge Provenance," DEXA, pp.524-528, 16th International Workshop on Database and Expert Systems Applications (DEXA'05), (2005).
[41] S. Toivonen, G. Denker, ”The Impact of Context on the Trustworthiness of Communication: An Ontological Approach.”, Workshop on Trust, Security, and Reputation on the Semantic Web, (2004).
[42] J. Hradesky, B. Acrement, ”Elements for Building Trust”. Proceedings of iTrust; A Conference on Trust Management. (1994).
[43] Inference Web, Knowledge Systems AI laboratory, Stanford University. Available at: http://iw.stanford.edu/
[44] D.L. McGuiness, P. P. Da Silva, L. Ding, “Proof Markup Language (PML) Primer”, (2007). Available at: http://inference-web.org/2007/primer/
[45] Web of Trust Vocabulary, Version 0.1. Available at: http://xmlns.com/wot/0.1/
[46] D. Brickley, “WOT RDF Vocabulary”. (2002)
[47] I. Zaihrayeu, P. P. Da Silva, D. L. McGuinness, “IWTrust: Improving User Trust in Answers from the Web”. Proceedings of the 3rd International Conference on Trust Management (iTrust). Lecture Notes in Computer Science - Springer. (2005).
[48] I. Davis, Jr. E. Vitiello, “Relationship: A Vocabulary for Describing Relationships Between People”, RDF Vocabulary Specification. (2005). Retrieved from: http://vocab.org/relationship/rel-vocab-20040308.html
[49] J. Davies, R. Studer, P. Warren, “Semantic Web Technologies: Trends and Research in Ontology-based Systems”. John Wiley & Sons, ISBN 0-470-02596-4. (2006).
[50] J. Brank, M. Grobelnik, D. Mladenic, ”A Survey of Ontology Evaluation Techniques”. Proceedings of the Conference on Data Mining and Data Warehouses (SiKDD 2005), Ljubljana, Slovenia. (2005).
[51] A. Jøsang, S. J. Knapskog, “A Metric for Trusted Systems.” Proceedings of the 21st National Security Conference, NSA, October (1998).
[52] J. Avnet, J. Saia, “Towards Robust and Scalable Trust Metrics”. IEEE International Conference, (2003).
[53] G. Caronni, “Walking the Web of Trust”. Proceedings of IEEE 9th International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises, (WET ICE), ENABL-00, page 153, ISBN 0-7695-0798-0. (2000)
[54] T. Beth, M. Borcherding, B. Klein, “Valuation of Trust in Open Networks”. In Proceedings of the Third European Symposium on Research in Computer Security, ISSU 875, pp. 3–18. Lecture Notes in Computer Science – Springer, (1994)
[55] PR. Zimmermann, “The Official PGP User's Guide”. MIT Press, ISBN 0-262-74017-6, Cambridge, MA, USA. (1995)
[56] Orkut, http://www.orkut.com/.
[57] LinkedIn, http://www.linkedin.com/.