ORDAIN: An ontology for trust management in the Internet of Things

Short paper

Kalliopi Kravari✉ [0000-0002-2298-9038] and Nick Bassiliades [0000-0001-6035-1038]

Dept. of Informatics, Aristotle University of Thessaloniki, Thessaloniki GR-54124, Greece
✉kkravari@csd.auth.gr
nbassili@csd.auth.gr

Abstract. The Internet of Things is coming and it has the potential to change our daily life. Yet, such a large scaled environment needs a semantic background to achieve interoperability and knowledge diffusion. Furthermore, this open, distributed and heterogeneous environment raises important challenges, such as trustworthiness among the various types of devices and participants. Developing and sharing ontologies that support trust management models and applications would be an effective step in achieving semantic interoperability on a large scale. Currently, most of the ontologies and semantic description frameworks in the Internet of Things are either context-based or at an early stage. This paper reports on identifying and incorporating social and non-social parameters involved in the Internet of Things in a general-purpose ontology that will support trust management. This ontology will include among others data and semantics about trust principles, involved parties, characteristics of entities, rating parameters, rule-based mechanisms, confidence and dishonesty in the environment. Defining an ontology and using semantic descriptions for data related to trustworthiness issues will provide an important instrument in developing distributed trust (reputation) models.

Keywords: Ontologies, Semantics, Trust management.

1 Introduction

The Internet of Things (IoT) aims to create a world where everyone and everything, called Things, will be connected, changing the way people live, work and communicate. Numerous research areas and applications is expected to benefit from this large scaled environment. Smart environment, living and healthcare are just a few cases [6]. Yet, this revolution has to be supported by an effortless diffusion of knowledge. Hence, promoting and applying semantic technologies to the IoT is vital for the needed interoperability. However, IoT raises challenges, such as intelligence and trustwor-

thiness, due to its open and distributed nature which is combined with the enormous heterogeneity of things. The heterogeneity makes it difficult to standardize interaction and communication. The open and distributed environment allows malicious participants to pose a serious threat to the proper functioning of the network, harming its credibility. Hence, Things acting in such an environment will have to make decisions about the degree of trust that can be invested, a vital but challenging task. [11, 8, 7]

Although there is no single accepted definition for trust, there is a wide range of proposed trust and reputation models [12]. This diversity, the context-based approaches and definition discrepancies lead to a need for a general-purpose ontology for trust. Such an ontology will improve knowledge reusability and diffusion, enabling interoperability regardless of trust algorithms and/or mechanisms. Furthermore, it will support the design and development of novel approaches.

This paper reports on identifying and incorporating social and non-social parameters involved in the IoT in a general-purpose trust ontology, called ORDAIN. Non-social parameters are concepts related to establishment and maintenance of trust relationships. Usually, they can be found at most trust models and mechanisms. On the other hand, although, the IoT is not considered as a social network, studying the potential societal impacts and relationships objects and/or people is essential. In fact, research on the IoT is expected to shift from intelligent objects to objects with a real social consciousness. Hence, the social dimension of the IoT is currently an open research area [8, 10]. ORDAIN attempts to include data and semantics related to trust mainstream concepts and novel social approaches. The aim is to provide an instrument in developing distributed trust (reputation) models, which on their turn will allow Things to establish and maintain social relationships based on their experiences, preferences and requirements without complex underlying protocols.

2 Defining Trust and Reputation

A reference trust definition is provided by Dasgupta [2], according to him trust is a belief an agent has that the other party will do what it says it will (being honest and reliable) or reciprocate (being reciprocative for the common good of both), given an opportunity to defect to get higher payoffs. In other words, trust is generally defined as the expectation of competence and willingness to perform a given task. Yet, the involved parties are likely to be self-interested and might not always complete requested tasks. Moreover, given that the system is open, they can change their identity and re-enter, avoiding punishment for any past wrong doing. Since involved parties may be dishonest, reputation is a core element at trust establishment, in the sense that a better reputation can lead to greater trust. In general, reputation is the opinion of the public towards a party. Reputation allows parties to build trust, helping them to establish relationships that achieve mutual benefits [7].

Risk is a situation that involves exposure to danger or loss, since the probability of loss is usually non-zero. Hence, the amount of risk that a party may be willing to tolerate is directly proportional to the amount of trust that the party has in the other party. Finally, for purposes of better understanding consider a party A interacting with a

party X; party A can evaluate the other party's performance, affecting its reputation. The evaluating party (A) is called truster whereas the evaluated party (X) is called trustee. After each interaction, the truster has to evaluate the abilities of the trustee according to some parameters, such as response time, validity or cooperation.

3 ORDAIN Ontology

3.1 Ontology Contents

The first step towards an ontology for trust management is to study and classify all concepts that affect reputation, the establishment and maintenance of trust between parties. Information sources, criteria, metrics and entities' roles are just a few of these. This subsection provides part of the reference taxonomy. This work is the result of a thorough literature review and previous work on reputation models [4, 5, 7, 8, 12, 1]. In order to elicit the requirements for such an ontology we compared available reputation models, extracting common concepts and relationships. Next, we studied IoT issues, such as the fact that devices are often not connected to the owners, and we tried to discard concepts that are or seem non applicable to IoT while we kept those that can be adopted even with some modifications.

Type of Trust.
Trust can be distinguished in *communication*, *information*, *social* and *cognitive trus*t. Communication trust studies uncertainties that cause low communication quality. Cognitive trust refers to truster's confidence or willingness to rely on trustee's competence. Social trust refers to entities' social relationships and how they affect trustworthiness, including metrics about influence, proximity, social ties and similarity.

Type of Control.
There are two system types, *centralized* and *distributed*. A centralized approach identifies a central authority that observes, manages and controls the system. A distributed approach has no central authority. Centralized approaches, usually, lead to global reputation values whereas distributed approaches lead to personalized estimations.

Roles of Involved Parties.
Parties may act as *Trusters*, *Trustees*, *Recommenders* or *Witnesses*. A witness provides reports based on personal previous experience whereas a Recommender usually propagates reports based on others' experience or observation.

Characteristics of Involved Parties.
Each entity has its own unique characteristics. It is not possible to provide here an exhaustive list of the characteristics that might have an entity. Yet, the most common of them are trade relationships, occupation or type of service, club membership, etc.

Information Context.
Contextual information is the means for a meaningful description of all available data, providing sufficient details about how parties interact. In the literature most cases refer to a *single* context domain whereas other more complex cases refer to *multiple*. Multiple context could be the result of multi-sourcing rating collection.

Information Sources.
Collecting ratings in an open, distributed environment is not always easy. Possible sources are *direct experience* which is the result of an individual's personal interactions or *direct observation* where a party observes the interaction between two other parties and records its opinion. Additionally there are cases of *indirect experience*, provided by witnesses and recommenders, called relational or social networks based trust. There is also another case, called *derived* information, which is obtained from sources that were not explicitly designed to be used as reference sources but act as such under specific circumstances. Finally, there is *prejudice*, which is a source that allows bootstrapping of trust and reputation when no other information is available.

Information Aggregation.
Aggregation is the mechanism behind the estimation process. The *counting* category includes *summation*, *averaging*, *weighting* and *normalization*, considering reputation as single value. Other approaches consider reputation as a multiple *discrete* value, using qualitative values for the rating procedure, such as "Untrustworthy". Another aggregation category involves *probabilistic* approach that computes the likelihood of a hypothesis being correct. An improvement of this category, is the aggregation that uses logic. This is the case of rule-based mechanisms. There are approaches that use *fuzzy logic* or *defeasible logic*. Finally, there are the social approaches. They adopt principles mainly from *social graphs* and *peer-to-peer networks*.

Types of Evaluation.
There are two evaluation approaches, the *holistic* and the *atomistic*. In the atomistic approach all past interactions are detailed described and taken into account. Some management systems in order to take into account more recent ratings, use weights and a time window. In the holistic cases, systems use summarized information rather than detailed reports in order to provide a single, overall trustworthiness estimation.

Evaluation criteria.
It is not possible to provide an exhaustive list of criteria. Besides, they are domain-specific. Yet, there are some of them that are frequently used in most models, e.g. *response time*, *validity*, *cooperation*, *competence*, *correctness* and *outcome feeling*.

Data aging.
Data aging is a technique that can reduce the available set of reports that have to be processed. Decaying information is the most common approach. It reduces the confi-

dence and granularity of older rating reports as time passes. Another approach is to *discard* information after a specific time period or used-defined criteria.

Reward or Punishment.
Self-interested entities are unwilling to sacrifice time and resources in order to contribute in a trust management system. Hence, there is a need for a motivation mechanism. To this end, there are two possible approaches, namely explicit *rules* and *incentives*. Rules force an entity to act only within a predefined manner. Incentives (or disincentives) motive or even guide entities by using rewards and/or punishments.

3.2 Ontology Implementation

The proposed ORDAIN ontology is an attempt to provide a reusable trust taxonomy and a tool that will support the development of novel trust management systems. It provides the necessary information that will clarify trust issues while new approaches in trust management, such as graph-based trust propagation, will promote research in the field. This section provides some information regarding the core implementation of the proposed ontology in OWL, using RDF/XML Syntax.

Involved Parties and Ratings.
Involved parties, as discussed, can have any of the four potential roles: Truster, Trustee, Recommender and Witness. Yet, at a specific time point they comply only with one of them. As a result, the role classes, subclasses of class Entity, are disjoined in ORDAIN. Each of these classes is associated with a number of properties, such as those presented below for the Truster case. A Truster `isInterestedIn` a specific Trustee whereas it may `requestsInformationFrom` some Wintesses (Fig. 1). A Trustee could `hadPreviouslyInteracted` with a witness. If this witness `isRequestedInformationBy` (inverse property with `requestsInformationFrom`) the aforementioned Truster will `provideRating` (range: Rating).

```
<owl:Class rdf:about="&ordain;Truster">
 <rdfs:subClassOf rdf:resource="&ordain;Entity"/>
 <rdfs:subClassOf><owl:Restriction>
   <owl:onProperty
                 rdf:resource="&ordain;isInterestedIn"/>
   <owl:someValuesFrom rdf:resource="&ordain;Trustee"/>
 </owl:Restriction></rdfs:subClassOf>
 <rdfs:subClassOf><owl:Restriction>
   <owl:onProperty
         rdf:resource="&ordain;requestsInformationFrom"/>
   <owl:someValuesFrom rdf:resource="&ordain;Witness"/>
 </owl:Restriction></rdfs:subClassOf>…</owl:Class>
```

Fig. 1. Part of Truster class' source code.

Ratings are core elements in reputation management. From a practical point of view, they include the evaluation data. A typical rating (Fig. 2) is in the form:

Rating [Truster, Trustee, TimeStamp, Evaluationcriterion$_1$Value,…, Evaluationcriterion$_n$Value, Confidence, Importance, TransactionValue] (1)

```
<owl:Class rdf:about="&ordain;Rating">
 <rdfs:subClassOf><owl:Restriction>
   <owl:onProperty rdf:resource="&ordain;byTruster"/>
   <owl:someValuesFrom rdf:resource="&ordain;Truster"/>
 </owl:Restriction></rdfs:subClassOf>
 <rdfs:subClassOf><owl:Restriction>
   <owl:onProperty rdf:resource="&ordain;forTrustee"/>
   <owl:someValuesFrom rdf:resource="&ordain;Trustee"/>
 </owl:Restriction></rdfs:subClassOf>
 <rdfs:subClassOf><owl:Restriction>
   <owl:onProperty
         rdf:resource="&ordain;hasEvaluationCriteria"/>
   <owl:someValuesFrom rdf:resource="&ordain;Criteria"/>
 </owl:Restriction></rdfs:subClassOf>
 <rdfs:subClassOf><owl:Restriction>
   <owl:onProperty rdf:resource="&ordain;hasConfidence"/>
   <owl:someValuesFrom><rdfs:Datatype>
     <owl:onDatatype rdf:resource="&xsd;float"/>…
   </rdfs:Datatype></owl:someValuesFrom>
 </owl:Restriction></rdfs:subClassOf>…</owl:Class>
```

Fig. 2. Part of Rating class' source code.

Aggregating mechanism.
Aggregation rating reports and trustworthiness values is perhaps the most difficult and challenging aspect of a trust management system. There are plenty of approaches while new are frequently proposed. ORDAIN includes each category as class with a number of subclasses and plenty of properties. For instance, a typical graph aggregation mechanism includes the following:

GraphAggregation [NumOfNodes, NumOfTies, connectedNodes, NodeID, TieID, hasTieValue, isNodeEntity, hasNodeCharacteristics, NodeTrustworthiness] (2)

Actually, each of these elements/values, just like above, are associated with the class GraphAggregation, subclass of AggregationMechanism, with appropriate properties, such as hasNumOfNodes that refer to an integer number (rdf:resource="&xsd;integer").

Combining Information Sources.
Combining different types of experience and, thus, available trustworthiness values is a really challenging task and, actually, an open research area. However, ORDAIN includes the `TrustCombining` class, with a number of subclasses (e.g. `WeightedTrustCombining`), that can be considered as a guideline.

`TrustCombining [Trustee, Timestamp, SourceType`$_1$`Value, …, SourceType`$_n$`Value, AggregationType] (3)`

Beardly speaking, ORDAIN includes a variety of classes and properties that can enable a different degree of trust management simulation and implementation based on the domain specific needs.

4 Related Work

In the IoT a common agreement on ontological definitions is still an open research issue. Ontologies and semantic frameworks are either at an early stage providing just a few basic properties or they are defined in the context of different projects.

For instance, in [3] authors propose a service oriented ontology. They assume that trust can be directed towards either an agent, product or service. They propose an ontological representation of agent, service and product trust in the sense that an agent develop trust in an agent, product or service. In their approach there are three distinct domains, namely Agent Trust Ontology, Service Trust Ontology and Product Trust Ontology. Opposed to that limited approach, we provide a single general-purpose ontology that can be adopted in a variety of domains. However, we do acknowledge that services, being an important component, are involved in the IoT.

In [9] authors propose an ontology-based framework for information fusion, as a support system for human decision makers. They build their approach upon the concept of composite trust, consisting of four trust types, communication, information, social and cognitive trust. Based on the concept of multidimensional trust, they constructed a composite trust ontology framework, called ComTrustO, that embraces four trust ontologies, one for each trust type. Their approach, similarly to ours, acknowledges the need for comprehensive ontologies and identifies four trust types. However, they provide four domain specific ontologies rather than a general-purpose approach. Furthermore, our approach includes many other concepts, such as trust aggregation.

5 Conclusions

Internet of Things faces interoperability issues and challenges, due to its open, distributed, heterogeneous nature. This paper proposed an ontology for trust management in the IoT. This ontology was the result of a detailed study on trust management systems presented in the literature. The proposed approach is a general-purpose ontology that takes into account social and non-social features. Trust, reputation and risk were discussed while a taxonomy of concepts related to trust (reputation) manage-

ment was reported. The key feature of the proposed ontology is that it captures the whole life-cycle of trust from the involved parties to decision mechanisms.

As for future directions, first of all, we plan to study further the proposed ontology in order to adopt any new concept or approach published in the literature. More technologies could be adopted for these purpose; machine learning techniques and user identity recognition and management being some of them. Another direction towards improving the proposed ontology is also to combine it with Semantic Web metadata for trust. Furthermore, we plan to evaluate it in order to report its added value as well as its weakness that will be subject of further improvement.

Acknowledgments

The Postdoctoral Research was implemented through an IKY scholarship funded by the "Strengthening Post-Academic Researchers / Researchers" Act from the resources of the OP "Human Resources Development, Education and Lifelong Learning" priority axis 6,8,9 and co-funded by The European Social Fund - the ESF and the Greek government.

References

1. Cho, J.-H., Chan, K., Adalı, S.: A survey on trust modeling. ACM Computing Surveys 48(2), 40, Article 28 (2015).
2. Dasgupta, P.: Trust as a commodity. Gambetta D. (Ed.). Trust: Making and Breaking Cooperative Relations, Blackwell, pp. 49-72 (2000).
3. Hussain, F. K., Chang, E., Dillon, T. S., Trust Ontology for Service-Oriented Environment. IEEE Int. Conference on Computer Systems and Applications, pp. 320-325 (2006).
4. Kravari, K., Bassiliades, N.: DISARM: A Social Distributed Agent Reputation Model based on Defeasible Logic. Journal of Systems and Software, 117, 130-152 (2016).
5. Kravari, K., Bassiliades, N.: HARM: A Hybrid Rule-based Agent Reputation Model based on Temporal De-feasible Logic. 6th International Symposium on Rules: Research Based and Industry Focused. Springer Berlin/Heidelberg, LNCS, 7438, pp. 193-207 (2012).
6. Li, S., Da Xu, L., Zhao, S.: The internet of things: a survey. Information Systems Frontiers, 17(2), pp. 243-259 (2015).
7. Medić, A.: Survey of computer trust and reputation models – the literature overview. Int. journal of information and communication technology research, 2(3), 254-275 (2012).
8. Nitti, M., Girau, R., Atzori, L.: Trustworthiness management in the social internet of things. IEEE Transactions on knowledge and data engineering, 26(5), 1253-1266 (2014).
9. Oltramari, A., Cho, J. H.: ComTrustO: Composite trust-based ontology framework for information and decision fusion. 18th Int. Conf. on Information Fusion, pp. 542-549 (2015).
10. Ortiz, A. M, Hussein, D., Park, S., Han, S. N., Crespi, N.: The cluster between internet of things and social networks: Review and research challenges. IEEE Internet of Things Journal, 1(3), 206-215 (2014).
11. Whitmore, A., Agarwal, A., Da Xu, L.: The Internet of Things—A survey of topics and trends. Information Systems Frontiers, 17(2), 261-274 (2015).
12. Yan, Z., Zhang, P., Vasilakos, A. V.: A survey on trust management for Internet of Things. Journal of network and computer applications, 42, 120-134 (2014).