18th International Conference on Information Fusion
Washington, DC - July 6-9, 2015

ComTrustO: Composite Trust-based Ontology Framework for Information and Decision Fusion

Alessandro Oltramari
Carnegie Mellon University
Pittsburgh, PA
Email: aoltrama@andrew.cmu.edu

Jin-Hee Cho
US Army Research Laboratory
Adelphi, MD
Email: jinhee.cho@us.army.mil

***Abstract*—Interactions between humans and machines are often placed in a multi-layered network involving the multidimensional trust in communication, information, and socio-cognitive layers. In this complex environment, how to filter and fuse heterogeneous data is critical for effective decision making. In this work, we propose an ontology-based framework for information fusion, as a support system for human decision makers. In particular, we build upon the concept of composite trust, consisting of four trust types: communication trust, information trust, social trust, and cognitive trust. Based on the concept of multidimensional trust, we construct a composite trust ontology framework, called `ComTrustO`, that embraces four trust ontologies, one for each trust type. We present the details of the integrated ontology framework and discuss a concrete example scenario.**

***Index Terms*—ontology, composite trust, information fusion, quality-of-service, quality-of-information, social trust, cognition, situation awareness.**

I. Introduction

Information fusion techniques have been used to derive clear, correct, and relevant information with high certainty (i.e., confidence) where many different sources may provide uncertain information caused by imprecision, incompleteness, disagreement (e.g., conflicting evidence), and/or unavailability. Particularly, for systems associated with both machines and humans where a person is immersed in a multiple network environment when communicating with other people, deriving trust from the complex, multi-layered network is not trivial because of the complexity of multidimensional trust and unique characteristics of each network layer, resulting in increasing uncertainty of received information. Understanding the interplay between different trust dimensions of each layered network is critical to deriving trust as the basis for effective decision making.

Uncertainty can be caused by many different factors such as unreliable communication media, lack of source and information credibility, lack of trust relationships in social networks, and lack of competence in cognitive judgment. For example, when two parties are communicating through various media (e.g., email, phone, text, social media applications), reliability (or unreliability) of the communication media affects quality-of-service (QoS) received by the other party. Messages with high delay or out-of-order and lost messages may impact the user's satisfaction on the QoS received in the communication network. Accordingly, the poor QoS can affect the user's trust in credibility of the received information. The received information can be analyzed based on many different quality-of-information (QoI) criteria including correctness, completeness, credibility, relevance, or timeliness.

Moreover, as QoS and QoI affect a user's assessment in trust for the received information, the relationships between two entities in a social network also play a crucial role. For example, the social trust towards an information provider affects reliability of the information source, leading to high credibility in the received information. Many social trust metrics, including influence, betweenness centrality, proximity, social tie, and similarity, can be criteria for an entity to make decisions for how much certain information is weighted based on the social trust towards the information source. If an entity is a human acting in an environment according to her cognitive capabilities, individual differences in cognitive competence or tendency (e.g., risk-taking behavior, information processing styles) may affect decision making process, resulting in different outcomes.

The difficulty of deriving trust from a multi-layered network also depends on the many different attributes that can be defined and on which research communities often disagree. In this work, we are interested in deriving critical attributes of trust from a respective network layer and incorporate them into a data fusion framework that can provide effective decision making with a level of confidence (i.e., certainty). In this respect, we chose an ontology-based approach to effectively solve the problem based on its capability of semantic integration of information [11].

This work aims to present an information fusion framework as a decision support system for humans situated in a multi-layered network. From each layer of the network, corresponding trust can be inferred such as *communication trust*, *information trust*, and *social trust*. In addition to these three dimensions of trust, a human decision maker interprets environmental observations on the basis of her cognitive capability, which can be conceived as a form of *cognitive trust*. In this paper, we incorporate these four dimensions of trust into an ontology-based information fusion framework implemented in OWL (Ontology Web Language). We also show a concrete example that can be processed on the basis of our approach.

Our paper has the following contributions:

- We propose an ontology-based reasoning framework for

information and decision fusion based on multiple dimensions of trust deriving from unique characteristics of different layered networks: we name it ComTrustO (COMposite TRUST-based Ontology framework). To the best of our knowledge, this work is the first that integrates the four dimensions of trust in a complex, multi-layered cyber-physical space;
- ComTrustO takes a hybrid ontology approach combining a suite of multiple trust ontologies into one composite model. This integrated ontology framework is efficient in managing updates and queries when more attributes of trust are considered depending on context and application requirements;
- We use DOLCE (Descriptive Ontology for Linguistic and Cognitive Engineering) foundational ontology to represent trust as *the quality of a trustee* where trust is subjective in nature and its various attributes can be captured by different measurement units [31]. No prior work has taken this approach to develop a trust ontology with a large set of trust attributes based on layering structure.
- We intend ComTrustO to be the trust-oriented ontological extension of CRATELO, an integrated ontology for cyber security for the ARL's Cyber Security Collaborative Research Alliance (CRA) [34].
- We visualize a practical application example of ComTrustO in Protégé [1], and outline how the proposed approach can be used as a generic support tool in decision tasks.

This paper is organized as follows. Section II gives background knowledge about ontology, and discuss existing work on ontologies for trust and data fusion. Section III describes the proposed ontology framework. We also discuss possible application scenarios of ComTrustO in Section III. Section IV concludes this work and outlines future research directions.

II. Background and Related Work

A. Background in Ontology

Borst [10] defines ontology as "a formal specification of a *shared* conceptualization," refining Gruber's definition of ontology [22]. Guarino [23] gives a finer characterization of the term 'conceptualization' as a language-independent view of the world, a set of conceptual relations defined on a domain space. Given a domain of entities, the domain space is a set of possible states of affairs of that domain (see Kripke's notion of *possible worlds* [29]). In this context, an ontology can be defined as a language-dependent cognitive artifact, committed to *a certain* conceptualization of the world by means of a given language [23]. An ontology indicates a set of representational primitives to model a domain of knowledge or discourse. The representational primitives include concepts, attributes of concepts, and relationships between concepts.

When ontologies are expressed within a logical framework, we talk about 'formal ontologies'; when formal ontologies are encoded in a machine-readable language, such as OWL, they become computational ontologies.

Ontological systems for meaning negotiation and information classification (from simple taxonomies to rich axiomatic systems) have been applied since the early 90's. This research area finds application in a variety of cases, from communication models to databases integration methods, consistency and security analysis of information systems to enterprise modeling and knowledge learning. The most important examples to date are the Semantic Web and semantic technologies explosion. In all these applications and domains, the ontological aspects of knowledge, which are intrinsically independent from the coding techniques, have acquired a high strategic value [4]. By means of an ontological characterization, information can be retrieved, described, organized, and integrated according to its most important value, the *content*. In the age of integrated enterprises and E-commerce, a rigorous organization of information contents is crucial and necessary to guarantee inter-communication among human and artificial agents. In this work, we focus our discussion on ontology applications in trust models and data fusion methods.

B. Trust Ontologies

A dictionary definition of trust is "assured reliance on the character, ability, strength, or truth of someone or something" and "confidence, hope, dependence, reliance, credit, trustworthiness, faith, non-competition, care, and commitment" [33]. Although a large volume of literature has discussed the multidimensional concept of trust, little work has addressed the common definition of trust across disciplines [15]. To embrace the multiple dimensions of trust and reduce the semantic ambiguity of the notion, ontology-based definitions and models of trust have been studied in various domains [39]. Jules et al. [27] propose an intelligent and dynamic Service Level Agreement (SLA) based on probabilistic ontology that detects and alerts potential violations of contract parameters for a cloud computing environment. Chang et al. [14] propose generic trust ontologies consisting of three class in service-oriented network environments: agent trust, service trust, and product trust. Dokoohaki and Matskin [17] propose a trust ontology with the design to improve the semantics of the structure of trust networks in the context of social institutions and ecosystems on Semantic Web.

Blasch [5] discusses many sources to derive trust in a system, namely the six general areas including user, hardware, software, network, machines, and the application. He maps trust associated with each area to specific attributes to define trust ontology. Golbeck and Parsia [21] present an ontology-based approach to integrate semantic web based trust networks with provenance information to evaluate and filter a set of assertions. Squicciarini et al. [36] design a reference ontology to develop privacy preserving trust negotiation systems that allow the secure exchange of protected resources and services by subjects in various security domains. Taherian et al. [38] enhance the extensibility of the ontology-based trust model encompassing features of pervasive computing contexts.

As the state of the art suggests, ontologies have been generally used to develop trust models limited to a particu-

Trust Type	Communication Trust	Information Trust	Social Trust	Cognitive Trust
Trustee	medium, machine source	information	relationships	human cognition
Attribute / Evaluating Factor	QoS	QoI	social capital	judgment competence
reliability	packet delivery	source credibility	expertise	logical thinking
availability	service availability	information availability	willingness	willingness
confidentiality	authentication	accessibility	privacy	morality
integrity	no network attack	correctness	honesty	truth-seeking
certainty	consistent data processing	consistency	stability	responsibility

TABLE I: Composite trust and example attributes corresponding to a trust type

lar network domain. But, unlike the contributions described above, our work adds novelty in that the proposed ontology is grounded on a multi-level domain consisting of communication, information, and social/cognitive layers of a network.

C. Data Fusion Ontologies

Data fusion is defined as "the process of fusing multiple records representing the same real-world object into a single, consistent, and clean representation" [9]. With the proliferation of many different information and sources, conflicting and uncertain data have been identified as the key challenge in data fusion [9]. Here we give an overview of various existing ontology models for data fusion.

Rogova and Bosse [35] define QoI for fusion-based human-system environments with three key attributes in terms of *source*, *content*, and *presentation*. They derive an ontology of each QoI with more granularity of sub-attributes. Blasch et al. [6] use two criteria to measure QoI fusion systems: *reliability* and *credibility*. Blasch et al. [6] view reliability as consistency of a source such as consistent data reporting by the source while credibility measures the believability of evidence embracing the attributes of veracity, objectivity, observational sensitivity, and self-confidence.

Costa et al. [16] show the ontology reference model to reason and represent uncertainty, called the Uncertainty Representation and Reasoning Evaluation Framework (URREF). On top of the URREF, Blasch et al. [6] develop a mathematical relation of evidence based on two criteria: *credibility* for information content and *reliability* for information source to analyze uncertainty in information fusion systems. Blasch et al. [8] further explore the concept of *confidence* and *self-confidence* in URREF to enhance trust in information fusion systems. Boury-Brisset [11] presents a methodological approach for ontology management allowing development of extensible ontologies and the mapping from ontologies to information sources.

Eid et al. [18] present a two layer prototype ontology for sensor data fusion, consisting of the sensor data sub-ontology and the sensor hierarchy sub-ontology, that uses the IEEE Suggested Upper Merged Ontology (SUMO), and demonstrates the out-performance of the proposed ontology-based search in terms of precision and recall rates. Sun et al. [37] present an ontology fusion approach in order to establish a common framework for collaborative environments with three key steps: ontology mapping, ontology alignment, and ontology merging. Krenc and Kawalec [28] propose an ontology-based information fusion framework for pre-selected sensors for executing a specific task based on Dezert-Smarandache Theory (DSmT).

Although many approaches as above have proposed an ontology-based information fusion architecture, little work has investigated ontology-based data fusion methods that can integrate information derived from multi-layered networks: in this respect, our proposed work fills both a methodological and a practical need in the state of the art on trust models. Most importantly, by using a foundational ontology like DOLCE as core reference model and OWL as implementation language, the semantic interoperability of `ComTrustO` is guaranteed and formal mappings with existing ontologies of trust dimensions can be established.

Lu et al. [30] take a similar approach with our work. They propose a network composer ontology framework, as a generic inference engine, to derive information involving multiple types of networks including communication, information, and social networks. However, unlike our proposed framework, their work presents limitations in a range of trust attributes across network domains and does not consider an entity's cognitive ability that may significantly affect decision making.

III. `ComTrustO` Framework

In this section, we describe how the proposed `ComTrustO` is structured and give details of each trust ontology across domains, including ontologies for communication trust, information trust, social trust, and cognitive trust. Besides, we visualize the representation of the `ComTrustO` in Protégé [1].

A. Trust Attributes in Multi-Layered Networks

In Table I, we show how composite trust consists of multiple types of trust and of common trust attributes that can be evaluated across domains: we categorize four types of trust, including communication, information, social, and cognitive trust. Depending on each trust type, we define an entity or object to be evaluated as a *trustee* and what aspect of trust in the trustee should be evaluated. We view QoS, QoI, social capital, and judgment competence as the key evaluating factors in assessing communication, information, social, and cognitive trust, respectively. Although QoS and QoI are popularly accepted aspects of trust to be evaluated in communication and information networks, *social capital* and *judgment competence* are newly introduced in this work as the key evaluating factors for social and cognitive trust. In social networks, *social capital* refers to the benefits that individuals or groups have because of their location (or status) in social structure [13]. Thus, we chose social capital as a key measure of social trust

because of its direct productivity of social trust relationships. According to Johnson and Grayson [26], *cognitive trust* refers to confidence or willingness of a trustor to rely on a trustee's competence and reliability [26]. Cognitive trust is often related to the use of accumulated knowledge to make predictions, but with uncertainty for possible risk. Therefore, how to deal with uncertain situations can be affected by individuals' cognitive tendency, which is closely related to judgment competence.

For this reason, we select five common attributes across trust domains, which include reliability, availability, confidentiality, integrity, and certainty, as a paradigmatic categorization of representative trust attributes. Our primary concern is to derive composite trust in a cyber-physical environment concerning cyber security. We denote the five common trust attributes as FCTA for notation convenience.

The sub-attributes under each attribute of the FCTA can vary on the basis of the contextual features of a system. We show example sub-attributes that can be mapped to each attribute of the FCTA in Table I. More detailed trust ontologies for each trust type are shown in Figs. 2-5.

B. Structure of Composite Trust Ontology

In this section, we illustrate the structure of an ontology for trust-based data fusion based on the concept of composite trust. We name each trust ontology as `commTO`, `infoTO`, `socialTO`, and `cogTO`, corresponding to communication, information, social, and cognitive trust ontologies, respectively. In Fig. 1, the brown arrows in the bottom-left part represent all the possible directions of the reasoning flow in `ComTrustO`. Accordingly, any systematic assessment of a trust dimension necessarily involves multiple levels: for instance, the upper-right part of Fig. 1 illustrates a dependency structure (brown-dotted lines) grounding *judgment competence* on *social capital*, *QoI* and *QoS*.

`ComTrustO` is encoded in OWL-DL (Web Ontology Language-Descriptive Logic) using Protégé frame-based platform [1]. The expressiveness of the ontology is SIQ(D), a decidable extension of the descriptive logic SHIN [25]. We map the FCTA to a trust 'quality space,' a set of suitable dimensions that can be used to assess the trustworthiness of a network. We use DOLCE (Descriptive Ontology for Linguistic and Cognitive Engineering) foundational ontology to represent *trust* as the *quality of a trustee* where trust has its various attributes to be considered in a different measurement unit [31]. DOLCE is part of a library of foundational ontologies developed under the WonderWeb project consortium [3].

DOLCE represents a cognitive bias that captures the conceptual primitives underlying natural language, commonsense reasoning, and human behavior. Qualities are conceived in DOLCE as *inherent* in other entities and *associatedWith* specific values. For example, 'shape,' 'size,' 'color,' 'weight,' 'sound,' 'smell' are quality types while 'triangular,' 'small,' 'red,' '50 pounds,' '70 Hz,' 'bitter' are value types. The relation of inheritance in DOLCE explains that the color exhibited by a particular object (a specific quality) is treated as different from its color value (a specific value). An example

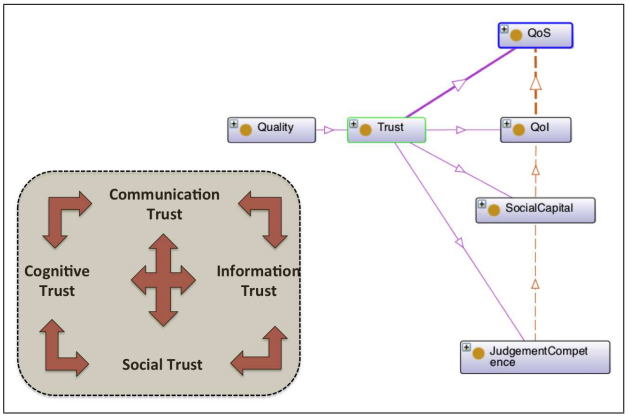

Fig. 1: Structure of `ComTrustO` and representation of the dependencies across trust domains. As the bottom-left section of the figure shows, `ComTrustO` doesn't commit to any fixed order in the dependence between trust layers. On the contrary, the multidirectional arrows represent the intermingled connections across trust layers.

can be found in physical and spatial magnitudes, such as the diameter of the Moon and the measure of 3476 Km or the frequency range of the human voice and the interval 500-2000 Hz. In DOLCE, quality values denote the position of an individual quality in a conceptual space [20]. By leveraging on DOLCE, we model trust as a *quality* of the class 'Trustee', where trust can be represented by means of a wide spectrum of conceptual spaces, which corresponds to the network layer for each trust type.

Fig. 1 shows the core structures of `ComTrustO` (right hand side). This graphical representation of the OWL model illustrates the four different trust aspects that originate the corresponding four trust ontologies. As already mentioned, the notion of trust is modeled as a quality on the basis of DOLCE conceptualization.

Expanding sub-attributes of the FCTA in Table I, we show the trust ontologies for each layered trust domain in Figs. 2-5 including `commTO`, `infoTO`, `socialTO`, and `cogTO`. In the following section, we provide a more concrete representation in Protégé.

C. Representation of `ComTrustO` in Protégé

As displayed on the left side of Fig. 6, `ComTrustO`'s taxonomy of trustees currently includes 'Human Cognition', 'Information', 'Medium' (of communication) and 'Relationship' (in a social context). In ontological terms, 'Trustee' is a role that can be played by objects, events, or information entities [32].

Depending on the trust space considered, `ComTrustO` distinguishes each trust type such that there exist distinctions between trust as QoS, QoI, judgment competence and social capital. We call these four different trust aspects *trust-quality types*. Trust-quality in each trust type is structured according to

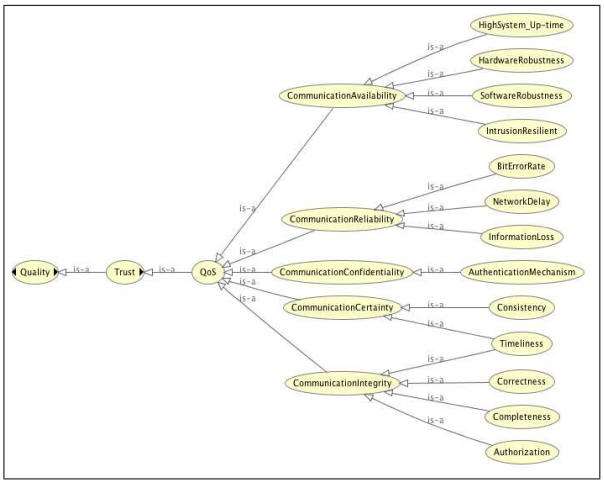

Fig. 2: commTO: QoS as trust in communication medium

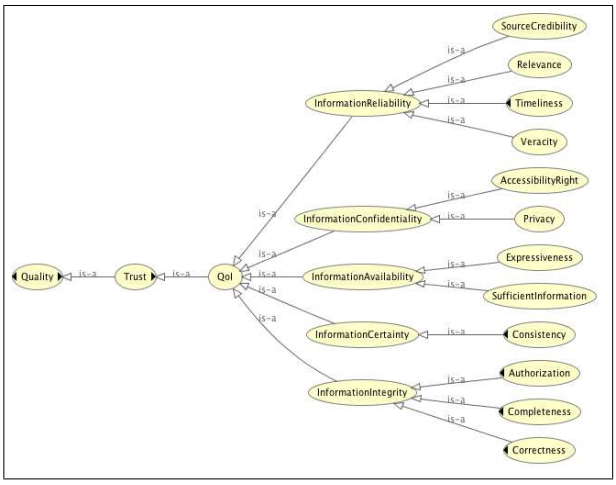

Fig. 3: infoTO: QoI as trust in information

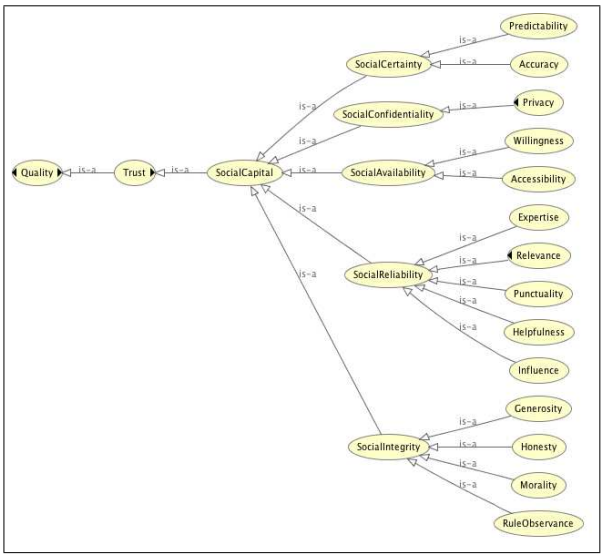

Fig. 4: socialTO: Social capital as trust in relationships

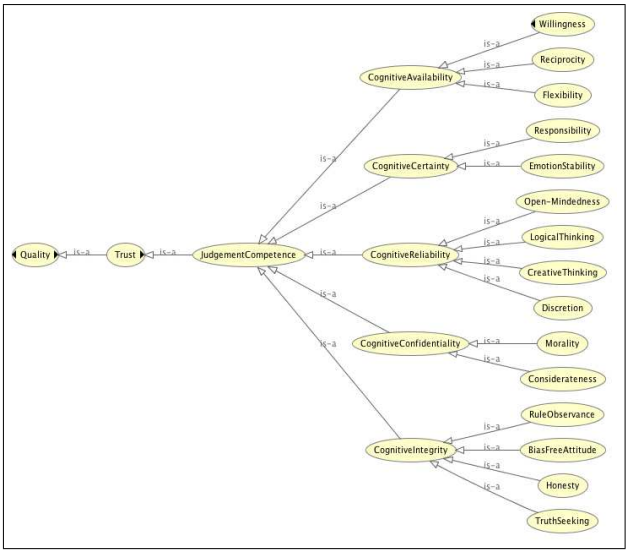

Fig. 5: cogTO: Judgment competence as trust in cognition

the five common trust attributes (FCTA) where the contextual properties of each attribute map to different spaces via the ontological relation *has_dimension*, indicated by the yellow dotted *arc* in the central part in Fig. 6.

As an example case on how each trust can be derived from this framework, let's focus on communication trust ontology, commOT, in ComTrustO. commTO currently defines reliability as a quality associated to two dimensions in the 'CommunicationTrustSpace,' namely, 'BitErrorValue' and 'NetworkDelayValue.' If we assume that an acceptable delay in a communication network has a value included within 0.1 and 0.215 ms, this implies that any out-of-range value makes data communication unreliable, therefore untrustworthy. This scenario is partially visualized in the bottom part of Fig. 6. We create an instance of 'Communication Network,' called 'MyNetwork' and a corresponding attribute 'ReliabilityMyNetwork' with value 0.3 ms, which is greater than the maximum delay as previously defined. By triggering the automatic reasoner Hermit [2] in Protégé, the ontology consistently classifies 'NetworkDelayMyNetwork' as untrustworthy, showing that the specific delay is *associatedWith* the 'ReliabilityMyNetwork' quality. This inference, highlighted in Fig. 6 with a pale yellow mark, is derived by the dichotomic structure of the 'NetworkDelayValue.' From a technical standpoint, this result is obtained using the closure axiom on 'NetworkDealyValue,' which covers the kinds of children the class can have, namely either 'TrustworthyNetworkDelayValue' or 'UntrustworthyNetworkDelayValue.'

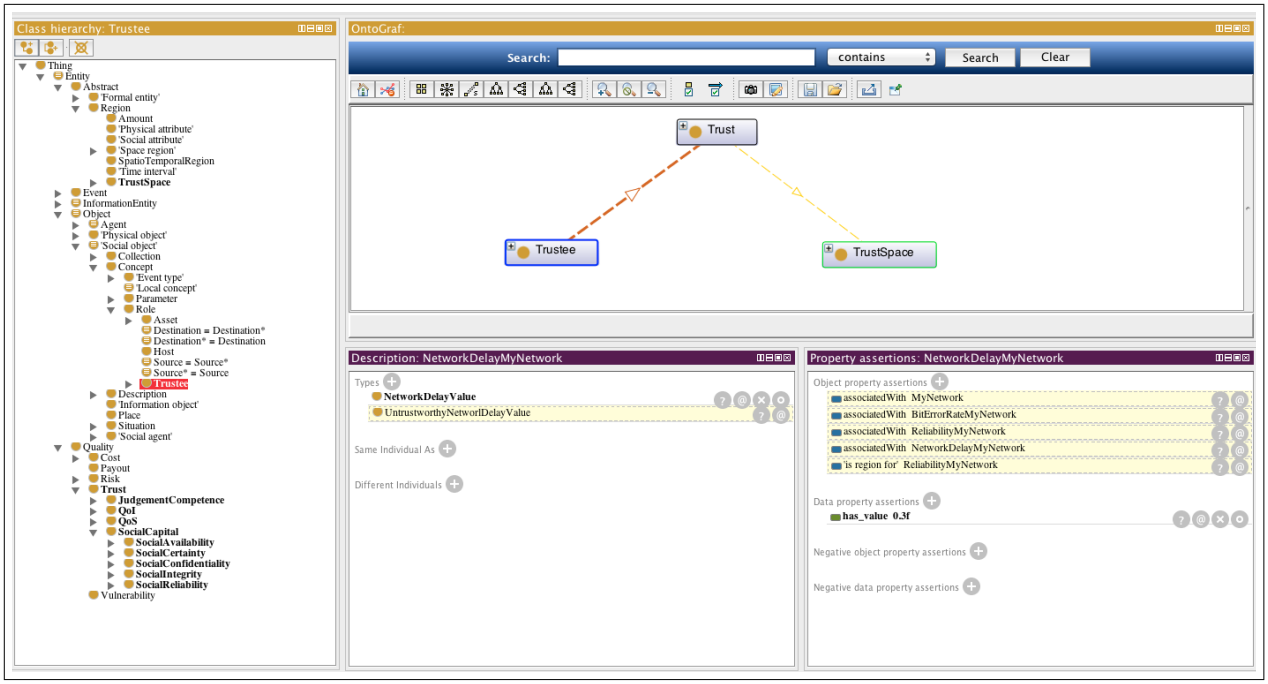

Fig. 6: A Protégé visualization of the ComTrustO model. From the left to the bottom (clockwise): 1. The backbone taxonomy of ComTrustO (in bold) included in DOLCE; 2. The core relational schema formed by *has_dimension* relation (yellow dotted arc) and *associatedWith* (grey line); and 3. The logical inference underlying the 'MyNetwork' example.

Similar arguments and examples apply to the other four attributes of trust (i.e., availability, confidentiality, integrity, and certainty) across domains (i.e., trust types). For instance,'Privacy' is a component of the quality 'Confidentiality' in a social network and the 'Privacy' can be represented by different dimensions in the trust space, from values of password strength to biometric parameters. Figs. 2-5 represent the upper levels of the four core ramifications of trust ontologies in ComTrustO.

As seen in Section III-B, DOLCE constitutes the reference model for our modular-hybrid approach. In particular, it supplies the necessary conceptual infrastructure to the four trust ontologies represented as boxes on left side in Fig. 1. Most importantly, we claim that a composite trust assessment is only possible through the nesting of trust components across network levels. To this end, we exploit DOLCE relationship *has_constituent* in ComTrustO.

D. Key Features of ComTrustO

In this section, we discuss the two key novel features introduced in the proposed ComTrustO.

First, ComTrustO *is constructed based on a hybrid approach of integrating multiple ontologies deriving from different trust domains*. Despite this idea being not new to the area of decision-support systems for situational awareness [7], no prior work has proposed an integrated trust ontology based on multiple sub-ontologies. In a given cyber, physical or cyber-physical spaces, situation awareness (SA) is defined as perception of the current situation, comprehension of the current situation, and prediction of the situation's outcomes [19]. In this regard, information fusion is considered a fundamental support tool for decision makers since it can help frame a holistic perspective on heterogeneous data and better understand the environment. In particular, ontology-driven information fusion aims at modeling different information aspects by means of a coherent logically-consistent conceptual framework. Boury-Brisset [12] discusses three main approaches to develop ontology-based frameworks: 'single ontology approach' (a.k.a. 'monolithic approach') which uses a global ontology to federate diverse data sources; 'multiple ontologies approach' based on different ontologies to model different data sources; or 'hybrid approach,' which combines the previous two approaches. A special case of the third type deals with 'modular ontologies' [24]. Modularity guarantees wide coverage and maintainability of the integrated information. In our work, we adopt a suite of trust ontologies related to multiple trust domains using a modular approach, which gives higher efficiency in managing updates and queries than maintaining a single, centralized ontology. The integrated ontologies can reliably combine the different dimensions of trust at different levels of categorization, representation of trustees and trust dimensions, and the corresponding qualitative and quantitative

measures. In the decision-making cycle, an ontology-driven model for trust-based information fusion can help humans to perform more reliable risk assessement and orient subsequent actions accordingly.

Second, *Constitutive discontinuity from an ontological layering technique is used to define characteristic of trust across network levels*. Intuitively, a constituent is a part belonging to a lower layer. Since layering is actually a partition of the world described by the ontology, constituents are not properly classified as parts, although this kinship can be intuitive for common sense. An advantage of this distinction is to allow us to describe physical constituents of non-physical objects (e.g., systems) while this cannot be done only by relying on parts. For example, a social system consists of people with the molecules constituting a person, the atoms constituting a river, etc. In this example, we notice a typical discontinuity between the constituted and the constituent object such that, for example, a social system is conceptualized at a different layer from the persons that constitute it, a person is conceptualized at a different layer from the molecules that constitute them, and a river is conceptualized at a different layer from the atoms that constitute it. Similarly, constitutive discontinuity can be conceived as a defining characteristic of trust across network levels and trust domains. An exemplifying scenario is as follows. An operator A receives a data transmission by a sender B from an unknown destination node in a network, and the transmission is fragmented and has a high bit error rate. A is likely to conclude that the communication network is untrustworthy. By means of the cascading effect driven by ontology-reasoning, all the other network layers will also be untrustworthy. In this sense, A can decide that the information exchanged with B is not reliable, as well as the source of transmission, B. By using her logical thinking, A may generalize and predict that any future data flow coming from B would need to be initially flagged and require further investigation.

IV. Conclusions

In this work, we proposed an ontology-driven data fusion framework based on the concept of composite trust, whose attributes are derived from the unique characteristics of different layered networks and domains. We considered four trust ontologies as the constituents of an integrated composite semantic model, called `ComTrustO`: concrete application examples were modeled in OWL and visualized using Protégé platform.

`ComTrustO` aims to support decision-making for trust-based information fusion. To this end, we plan (1) testing the proposed framework on relevant case studies; (2) conducting comparative performance analysis of `ComTrustO` and the existing counterparts; and (3) investigating the applicability of real datasets that include trust as a dimension of risk assessment.

V. Acknowledgements

This research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-13-2-0045 (Cyber Security CRA). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

References

[1] Webprotégé. URL `http://protege.stanford.edu/`.

[2] Hermit owl reasoner: The new kid on the owl block, 2004. URL `http://hermit-reasoner.com/`.

[3] Wonderweb: Ontology infrastructure for the semantic web, 2004. URL `http://wonderweb.man.ac.uk/`.

[4] T. Berners-Lee. *Weaving the Web*. Harper, San Francisco, 1997.

[5] E. Blasch. Trust metrics in information fusion. In *Proc. SPIE 9119*, 28 May 2014. Machine Intelligence and Bio-inspired Computation: Theory and Applications VIII, 91190L.

[6] E. Blasch, K. B. Laskey, A.-L. Jousselme, V. Dragos, P. C. G. Costa, and J. Dezert. URREF reliability versus credibility in information fusion (STANAG 2511). In *16th International Conference on Information Fusion (FUSION'2013)*, Istanbul, Turkey, July 9-12 2013.

[7] E. Blasch, Y.B. Al-Nashif, and S. Hariri. Static versus dynamic data information fusion analysis using DDDAS for cyber security trust. In *Proceedings of the International Conference on Computational Science,ICCS 2014, Cairns, Queensland, Australia, 10-12 June, 2014*, pages 1299–1313, 2014.

[8] E. Blasch, A. Jøsang, J. Dezert, P.C.G. Costa, and A.-L. Jousselme. URREF self-confidence in information fusion trust. In *17th International Conference on Information Fusion (FUSION'2014)*, pages 1–8, Salamanca, Spain, 2014.

[9] J. Bleiholder and F. Naumann. Data fusion. *ACM Computing Surveys*, 41(1), Dec. 2008. Article 1.

[10] W.N. Borst. *Construction of Engineering Ontologies*. Centre for Telematica and Information Technology, University of Tweente, Eschede, 1997.

[11] A.-C. Boury-Brisset. Ontology-based approach for information fusion. In *Proceedings of the Sixth International Conference of Information Fusion (FUSION'2003)*, volume 1, pages 522–529, Cairns, Queensland, Australia, 8-11 July 2003.

[12] A. C. Boury-Brisset. Ontology-based approach for information fusion. volume 1, pages 522–529, 2003.

[13] R. S. Burt. *Research in Organizational Behavior*, volume 2, chapter The network structure of social capital. 2000.

[14] E. Chang, T. S. Dillon, and F. Hussain. Trust ontologies for e-service environments. *International Journal of Intelligent Systems*, 22:519–545, 2007.

[15] J.H. Cho, A. Swami, and I.R. Chen. A survey of trust management in mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, 13(4):562–583, 2011.

[16] P. C. G. Costa, K. B. Laskey, E. Blasch, and A-L. Jousselme. Towards unbiased evaluation of uncertainty reasoning: The unref ontology. In *15th International Conference on Information Fusion (FUSION'2012)*, pages 2301–2308, Singapore, 9-12 July 2012.

[17] N. Dokoohaki and M. Matskin. Structural determination of ontology-driven trust networks in semantic social institutions and ecosystems. In *International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM'2007)*, pages 263–268, Papeete, France, 4-9 Nov. 2007.

[18] M. Eid, R. Liscano, and A. E. Saddik. A universal ontology for sensor networks data. In *IEEE International Conference on Computational Intelligence for Measurement Systems and Applications*, pages 59–62, Ostuni, Italy, 27-29 June 2007.

[19] M.R. Endsley. Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37:32–64(33), March 1995.

[20] P. Gärdenfors. *Conceptual Spaces: the Geometry of Thought*. MIT Press, Cambridge, Massachussetts, 2000.

[21] J. Golbeck and B. Parsia. Trust network-based filtering of aggregated claims. *International Journal of Metadata, Semantics and Ontologies*, 1(1):58–65, 2006.

[22] T. R. Gruber. A translation approach to portable ontology specifications. *Knowledge Acquisition*, 5:199–220, 1993.

[23] N. Guarino. Formal ontology in information systems. In Nicola Guarino, editor, *Formal Ontology in Information Systems. Proceedings of FOIS98, Trento, Italy, 6-8 June 1998*, pages 3–15. IOS Press, Amsterdam, 1998.

[24] S. Spaccapietra H. Stuckenschmidt, C. Parent. *Modular Ontologies - Concepts, Theories and Techniques for Knowledge Modularization*. Springer, 2009.

[25] U. Sattler I. Horrocks, O. Kutz. The irresistible sriq. In *OWLED 2005 - "OWL: Experiences and Directions")*, volume 188, Galway, Ireland, 2005.

[26] D. Johnson and K. Grayson. Cognitive and affective trust in service relationships. *Journal of Business Research*, 58:500–507, 2005.

[27] O. Jules, A. Hafid, and M.A. Serhani. Bayesian network, and probabilistic ontology driven trust model for sla management of cloud services. In *IEEE 3rd International Conference on Cloud Networking (CloudNet'2014)*, Luxembourg, 8-10 Oct. 2014.

[28] K. Krenc and A. Kawalec. An application of DSmT in ontology-based fusion systems. In *12th International Conference on Information Fusion (FUSION'2009)*, pages 1218–1225, Seattle, WA, 2009.

[29] S. Kripke. *Naming and Necessity*. Basil Blackwell, Oxford, 1980.

[30] S. Lu, A. Tazin, and M.M. Kokar. Network composition for situation assessment: A "trusted meeting" case study. In *15th International Conference on Information Fusion (FUSION'2012)*, pages 346–353, 9-12 July 2012.

[31] C. Masolo, N. Guarino A. Gangemi, A. Oltramari, and L. Schneider. WonderWeb Deliverable D17: The WonderWeb Library of Foundational Ontologies. Technical report, 2002.

[32] C. Masolo, G. Guizzardi, L. Vieu, E. Bottazzi, and R. Ferrario. Relational roles and qua individuals. In *AAAI Fall Symposium on Roles, an Interdisciplinary Perspective*, VA, USA, 2005.

[33] Merriam and Webster Dictionary. Definition of trust, 2015.

[34] A. Oltramari, L. Cranor, R. Walls, and P. McDaniel. Building and ontology of cyber security. In *9th Conference on Semantic Technologies for Defense, Intelligence and Security*, Fairfax, VA, USA, 2014.

[35] G. L. Rogova and E. Bosse. Information quality in information fusion. In *13th Conference on Information Fusion (FUSION'2010)*, pages 1–8, Edinburgh, Scotland, 26-29 July 2010.

[36] A.C. Squicciarini, E. Bertino, E. Ferrari, and I. Ray. Achieving privacy in trust negotiations with an ontology-based approach. *IEEE Transactions on Dependable and Secure Computing*, 3(1):13–30, Jan.-March 2006.

[37] H. Sun, W. Fan, W. Shen, , and T. Xiao. Ontology fusion in high-level-architecture-based collaborative engineering environments. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 43(1):2–13, Jan. 2013.

[38] M. Taherian, R. Jalili, and M. Amini. Pto: A trust ontology for pervasive environments. In *22nd International Conference on Advanced Information Networking and Applications - Workshops (AINAW'2008)*, pages 301–306, Okinawa, Japan, 25-28 March 2008.

[39] L. Viljanen. *Trust, Privacy, and Security in Digital Business*, volume 3592, chapter Towards an Ontology of Trust, pages 175–184. Springer-Verlag Berlin Heidelberg, 2005. Lecture Notes in Computer Science.