Argumentation for Resolving Privacy Disputes in Online Social Networks

(Extended Abstract)

Nadin Kökciyan
Department of Computer Engineering
Bogazici University
34342 Bebek, Istanbul, Turkey
nadin.kokciyan@boun.edu.tr

Nefise Yaglikci
Department of Computer Engineering
Bogazici University
34342 Bebek, Istanbul, Turkey
ngyaglikci@gmail.com

Pınar Yolum
Department of Computer Engineering
Bogazici University
34342 Bebek, Istanbul, Turkey
pinar.yolum@boun.edu.tr

Categories and Subject Descriptors

I.2.1 [**Artificial Intelligence**]: Distributed Artificial Intelligence *Multiagent systems*

General Terms

Algorithms, Design

Keywords

Privacy; Online Social Networks; Argumentation

1. INTRODUCTION

Preserving privacy of users in online social networks is important. Usually, users specify their privacy constraints and the online social network is expected to enforce them. However, many times a piece of content is related to a number of users, whose privacy constraints might be incompatible. For example, when a user shares a party photo, her privacy constraints are enforced on the picture but the privacy constraints of the people in the picture are not. One way to deal with this problem is to enable collaborative policies to be written per content [5]. However, composing privacy policies from scratch is extremely time consuming. Further, it is difficult to overcome conflicts among users. Another way of dealing with this problem is to use agent-based approaches such that agents represent their users and employ agreement techniques to reach a conclusion on whether a content should be shared or not [3, 4]. Following this line of work, we advocate an agent-based approach where each user in the social network is represented by an agent that manages its user's privacy constraints. Each agent represents its domain knowledge using an ontology and its user's privacy constraints as semantic rules. When a user wants to post a content, her agent contacts the relevant agents (e.g., agents of tagged users in the content) to request permission. Upon receiving the request, these agents evaluate it using their own rules. If any of the agents has a concern; i.e., its privacy constraint is violated, then the agents engage in an argumentation session. The argumentation is done in a distributed manner where agents take turns to provide evidence as to why the content should be shared or vice verse. The evidence is generated from the agent's ontology and semantic rules on demand based on what the other agents have proposed. At the end of the argumentation, winning arguments are computed, leading to a decision on whether the content should be shared or not.

Appears in: *Proceedings of the 15th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2016), J. Thangarajah, K. Tuyls, C. Jonker, S. Marsella (eds.), May 9–13, 2016, Singapore.*

2. TECHNICAL DETAILS

We represent a social network user with an agent. The main goal of an agent is to manage its user's privacy constraints. For this, an agent is equipped with an ontology to represent the social network domain, the content being shared, the relationships of its user, and the privacy constraints of its user (e.g., not disclose location information). Each privacy constraint is represented as a semantic rule in the user's ontology.

2.1 Assumption-based Argumentation

We use Assumption-based Argumentation (ABA)[1] to generate arguments from information provided by the agents. In an ABA framework, there are four main constructs: (i) the language to describe information, (ii) a set of rules to derive arguments, (iii) a set of assumptions to represent nonfactual information, and (iv) a set of contraries to disprove validity of assumptions. In ABA, an argument is of the form $S \vdash^R \sigma$, where S (the support) is a set of assumptions, R is a set of rules and σ is the claim of the argument inferred by the use of R. Assumptions are the weak points of arguments and can be refuted by other arguments. An argument a_1 can attack another argument a_2 if the claim of a_1 is the contrary of one of the assumptions in a_2. In ABA, various semantics can be used to compute winning (acceptable) arguments. In this work, we use the credulous admissible semantics. Hence, an argument that is not attacked by any other argument or it is attacked but defended by other arguments in ABA is a winning argument. In a recent work, Fan *et al.* [2] propose an approach for multiple agent decision making as we do here. Our work is different in that: (i) Agents are equipped with ontologies to represent knowledge (the social network domain and the privacy constraints). (ii) Agents generate arguments by using their ontologies. (iii) Agents can consult other agents to enrich their knowledge base if they have missing information in their ontologies.

2.2 Distributed Argumentation

Prior to sharing a post, an agent starts an argumentation with other agents relevant to this post request. The initial assumption is that the post can be shared. During the argumentation, agents send *message*s to each other in a turn taking fashion to provide their arguments and to convince other agents. A message consists of rules, facts, assumptions and their contraries. After an agent sends a post request, relevant agents to this post request evaluate it by creating a post request instance in their ontologies. As a result of ontological reasoning, agents infer more information about this post request (e.g., the context). In another words, agents evaluate a given post request regarding the privacy constraints of their users; they make use of their ontologies to accept or reject a post request. If any of the agents rejects the post request, that agent provides new information (rules, facts, assumptions and contraries), and updates the ongoing message to attack other agents' assumptions. In order to formulate arguments, agents can use their own ontologies or consult other agents in their social network to collect information. This is similar to real life where people consult others if they do not have enough information about a topic. The argumentation session terminates when agents cannot provide new information and update the message. At the end of the argumentation, the initiator agent gives the final message to an ABA engine and queries its initial assumption. If the initial assumption is a winning argument, then the post is shared by the initiator agent. Otherwise, the post is not shared.

2.3 Running Example

Consider a scenario where Bob wants to share a photo of Alice. Bob would like to consult Alice before sharing it since this content could violate Alice's privacy constraints. For this, Bob starts an argumentation session with Alice. It creates an initial message where he puts information about the post request. Moreover, Bob's agent `:bob` has an initial assumption that the post can be shared (A_{B_1}). Alice rejects any post request, which includes a photo taken abroad since she does not want other users to know when she is abroad. This privacy concern is represented as a privacy rule in Alice's ontology (R_{A_1}). Upon receiving the message, her agent `:alice` assumes that the photo is taken abroad (A_{A_1}). If an agent can prove that the photo is taken in Alice's home country, that would oppose A_{A_1}. Bob has two rules in his ontology. The first rule states that a country is the home country of a person if this person was born in a city of that country (R_{B_1}). The second rule states that if the photo is taken in a country, which is the home country of an agent, then the photo is taken in the home country of this agent (R_{B_2}). Bob also has an assumption about which country the photo was taken in (A_{B_2}).

Initially, `:bob` prepares a message where it puts factual information about the post request (e.g., tagged agents) and its initial assumption A_{B_1}, and it sends the message to `:alice`. In its turn, `:alice` evaluates the post request in its ontology. The post request violates the privacy rule R_{A_1} since `:alice` has the assumption A_{A_1}, `:alice` rejects the post request. `:alice` updates the message by adding R_{A_1} to the rule set and A_{A_1} to the assumption set of the message. Next, `:bob` receives the message and evaluates the message in its ontology. `:bob` knows the city where Alice was born hence it uses R_{B_1} to infer the home country of Alice. Moreover, it has the assumption A_{B_2} and the rule R_{B_2}. It turns out that the photo is taken in the home country of Alice hence `:bob` proves the contrary of A_{A_1}. `:bob` updates the message and sends it to `:alice`. When `:alice` receives the message again, it checks whether it can attack A_{B_2}. Since it has no supporting knowledge in its ontology, it consults `:carol` (a friend of `:alice`) to gather extra information for attacking A_{B_2}. `:carol` cannot provide any information either. The argumentation session terminates since `:alice` and `:bob` cannot update the message with new information. `:bob` uses the final message to compute winning arguments in an ABA engine. For this, it queries its initial assumption A_{B_1}, which results in a winning argument. Thus, `:bob` shares the photo in the online social network. In this scenario, `:bob` has convinced `:alice` to share the photo by providing information that `:alice` was not aware of. If there would not be such environment for agents to challenge each others' arguments, the post would not be shared; i.e., `:bob` would not share the photo to protect `:alice`'s privacy.

3. DIRECTIONS

Our current approach assumes all the agents are trustworthy since they are connected to each other in the social network. However, it would be interesting to study situations where the rules and assumptions are added to the argumentation based on the trustworthiness of the agents. It would also be interesting to study the formal properties of the decisions that are reached through argumentation as well as analyze the performance of our approach when multiple agents engage in argumentation.

Acknowledgments

This work has been supported by TUBITAK under grant 113E543.

REFERENCES

[1] P. M. Dung, R. A. Kowalski, and F. Toni. Assumption-based argumentation. In *Argumentation in Artificial Intelligence*, pages 199–218. Springer, 2009.

[2] X. Fan, F. Toni, A. Mocanu, and M. Williams. Dialogical two-agent decision making with assumption-based argumentation. In *International Conference on Autonomous Agents and Multi-agent Systems (AAMAS)*, pages 533–540, Richland, SC, 2014.

[3] R. Fogues, P. Murukanniah, J. Such, A. Espinosa, A. Garcia-Fornes, and M. Singh. Argumentation for multi-party privacy management. In *The Second International Workshop on Agents and CyberSecurity (ACySe)*, pages 3–6, 2015.

[4] Y. Mester, N. Kökciyan, and P. Yolum. Negotiating privacy constraints in online social networks. In F. Koch, C. Guttmann, and D. Busquets, editors, *Advances in Social Computing and Multiagent Systems*, volume 541 of *Communications in Computer and Information Science*, pages 112–129. Springer, 2015.

[5] R. Wishart, D. Corapi, S. Marinovic, and M. Sloman. Collaborative privacy policy authoring in a social networking context. In *Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY)*, pages 1–8, 2010.