Epistemic Analysis of Communicating Agents

Fatemeh Ghassemi

University of Tehran

Abstract: Agents communicate via a predefined protocol, specified in an operational manner by specifying the communication patterns among the agents involved. Many security properties are of epistemic nature, e.g., what each agent believes after having seen a run of the protocol. We propose a generic framework for epistemic reasoning about communicating agents. Our reasoning framework is based on a logic of beliefs, and we allow for the operational specification of untruthful communications. We reason what credulous rational agents can infer about a particular run if they know the protocol beforehand. (A credulous agent is an agent that is ready to believe what is told unless it is logically inconsistent.) We express the epistemic properties of such specifications in a rich extension of modal μ-calculus with past and the belief modality. We define the semantics of our operational models in the semantic domain of our logic. To make the verification of epistemic properties on our operational models feasible, we propose a set of operational rules governing the efficient generation of models with regard to given properties. These operational rules automatically reduce the semantics with respect to a class of epistemic properties and can potentially reduce an infinite state space into a finite one. We formulate and prove criteria that guarantee belief consistency for credulous agents.

Keywords: Process theory, State Space Reduction, Epistemic Protocols, Epistemic logic

1 Introduction

Agents communicate via a predefined protocol, specified in an operational manner by specifying the communication patterns among the agents involved, order by causal or temporal order. We call such specifications of protocol “operational” since they involve the operational details of the communication patterns. Examples of common operational frameworks for protocol specification include sequence diagrams, state diagrams, or domain-specific languages based on message passing. Epistemic reasoning about such protocols provides a natural means for reasoning about their properties such as anonymity and privacy [1,2,3,4,5]. Hence, providing a vehicle to verify epistemic properties on operational specifications of protocols brings about the advantage of using two expressive paradigms for specification and verification: the operational paradigm for protocol specification and the epistemic paradigm for property specification and verification. In the recent past, several such paradigms have been proposed [1,3,5].

In this paper, we propose such a framework (based on an earlier proposal by Dechesne, Mousavi, and Orzan [1]) and show how reasoning about protocols can be made efficiently

through an on-the-fly reduction of the state space based on the class of epistemic properties of interest.

Two features of our framework are that it caters for: 1) the possibility of untruthful communications (telling lies), and 2) using belief constructs in protocol specifications.

2 Research Goals

A contribution of this research is to provide an operational framework (i.e., based on actions and their relative ordering) that enables reasoning about belief-related properties. An essential difference between knowledge and belief is that knowledge has to be true, while belief does not have to; an untrue belief can, for example, be held when lies are told or facts are concealed. A lie is an intentional announcement of (believed-to-be) incorrect information in order to deceive the audience [6,7]. A lie is an action, while (untrue) belief is a possible consequence of that action in agents' states. The belief aspect, i.e., epistemic, of lies is often captured by modeling the effect of lies as belief revisions or updates. Modeling lies and their epistemics have attracted substantial attention in the recent literature concerning Dynamic Epistemic Logic (DEL, cf. [6,7,8] for some recent examples; also see [0] for applications of DEL in security). Our framework extends an earlier operational framework [1] based on process algebra [10] to allow for telling lies, i.e., communicating messages in such a way that a certain audience may believe that something else (or nothing at all) has been communicated.

To reason about epistemic properties of specifications, we maintain the history of actions in the configurations of the operational model and define a relation among the configurations to relate those configurations that a credulous agent cannot distinguish. (Credulous agents are those agents that are willing to accept what is being told to them as long as it does not lead to any logical inconsistency with the rest of their belief.) We focus on two types of logical properties: first, what an agent consistently believes, and second, whether an agent can detect a particular lie in the course of a protocol execution. We express properties in a rich extension of modal μ-calculus with Dynamic Epistemic Logic constructs and define the semantics of our operational models in the semantic domain of our logic. In addition to providing the basic specification framework and its formal semantics, we also address the issue of efficient verification.

Reference

[1] F. Dechesne, M. R. Mousavi, S. Orzan, Operational and Epistemic Approaches to Protocol Analysis: Bridging the Gap, *Proc. 14th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning*, Springer, 226–241, 2007.

[2] R. v. Meyden, Two Applications of Epistemic Logic in Computer Security, *Proof, Computation and Agency - Logic at the Crossroads*, vol. 352 of Synthese library, Springer, 133–144, 2011.

[3] S. Knight, C. Palamidessi, P. Panangaden, F. D. Valencia, Spatial and Epistemic Modalities in Constraint-Based Process Calculi, *Proc. 23rd International Conference on Concurrency Theory*, Springer, 317–332, 2012.

[4] J. V. Eijck, M. Gattinger, Elements of Epistemic Crypto Logic, *Proc. International Conference on Autonomous Agents and Multiagent Systems*, ACM, 1795–1796, 2015.

[5] A. Lomuscio, H. Qu, F. Raimondi, MCMAS: an open-source model checker for the verification of multi-agent systems, *Int. J. Softw. Tools Technol. Transf*. 19 (1) (2017) 9–30.

[6] H. van Ditmarsch, J. van Eijck, F. Sietsma, Y. Wang, On the Logic of Lying, *Games, Actions and Social Software: Multidisciplinary Aspects*, vol. 7010 of LNCS, Springer, 41–72, 2012. 51

[7] T. Ågotnes, H. van Ditmarsch, Y. Wang, True lies, S*ynthese.* 195 (10) (2018) 4581–4615.

[8] H. Van Ditmarsch, Dynamics of lying, S*ynthese* 191 (5) (2014) 745–777.

[9] R. Pucella, Knowledge and Security, CoRR abs/1305.0876, URL http://arxiv.org/abs/1305.0876.

[10] J. C. M. Baeten, T. Basten, M. A. Reniers, Process Algebra: Equational Theories of Communicating Processes, *Cambridge Tracts in Theoretical Computer Science*, Cambridge University Press, 2009.

تحلیل معرفتی عامل‌های ارتباطی

چکیده: عامل ها از طریق یک پروتکل از پیش تعریف شده با یکدیگر تعامل دارند که این تعامل به صورت عملیاتی با مشخص کردن الگوهای ارتباطی بین عوامل درگیر توصیف می‌گردد. بسیاری از ویژگی های امنیتی ماهیت معرفتی دارند، به عنوان مثال، آنچه هر عامل پس از مشاهده اجرای پروتکل به آن اعتقاد دارد. ما یک چارچوب کلی برای استدلال معرفتی در مورد عامل‌های ارتباطی پیشنهاد می کنیم. چارچوب استدلال ما بر اساس منطقی از باورها است، که در آن امکان توصیف عملیاتی ارتباطات که ممکن است عاملی دروغ بگوید وجود دارد. هدف ما در این پژوهش این است که به دست بیاوریم که یک عامل زودباور اگر از قبل پروتکل را بدانند، به چه باروهایی در مورد یک اجرای خاص پروتکل خواهد رسید. (یک عامل زودباور عاملی است که هر آنچه به او گفته می شود ، در صورتیکه از لحاظ منطقی ناسازگار نباشد را باور می کند). ما ویژگی‌های معرفتی توصیف پروتکل ها را در بسط غنی حسابان μ با استفاده از عملگرهای زمانی گذشته و باور بیان می‌کنیم. سپس معناشناسی مدل های عملیاتی خود را در حوزه معنایی منطق خود تعریف می کنیم. برای عملی ساختن درستی‌سنجی ویژگی‌های معرفتی در مدل‌های عملیاتی خود، مجموعه‌ای از قوانین عملیاتی را پیشنهاد می‌کنیم که تولید کارآمد مدل‌ها با توجه به ویژگی‌های داده شده را نتیجه می دهند. این قوانین عملیاتی به طور خودکار فضای حالت را برای یک کلاس از ویژگی‌های معرفتی کاهش می‌دهند و می‌توانند یک فضای حالت نامتناهی را به یک فضای محدود کاهش دهند. ما معیارهایی را ارائه و اثبات می کنیم که ثبات باور را برای عوامل زودباور تضمین می کند.

کلمات کلیدی: جبر پردازه، کاهش فضای حالت، پروتکل معرفتی ، منطق معرفتی