Verification of Socio-Technical Models of Multi-Agent Systems and E-Voting Protocols

Wojciech Jamroga and Wojciech Penczek
Institute of Computer Science, PAS, Warsaw
{penczek,Jamroga}@ipipan.waw.pl

1. Project Description

Multi-agent systems describe interactions of multiple entities called agents, often assumed to be intelligent and autonomous. Alternating-time temporal logic **ATL∗** and its fragment **ATL** [1] allow for reasoning about strategic interactions in such systems, by extending the framework of temporal logic with the game-theoretic notion of strategic ability. Hence, **ATL** enables to express statements about what agents (or groups of agents) can achieve. Such properties can be useful for specification, verification, and reasoning about interaction in complex agent systems. They have become especially relevant due to active development of algorithms and tools for verification where the "correctness" property is given in terms of strategic ability [4]. In particular, models and formulas of **ATL** can be used to specify and verify essential properties of protocols for secure voting, such as *coercion resistance*, *voter verifiability*, and *end-to-end verifiability* [6,7].

However, there are several obstacles First, most of the existing tools and algorithmic solutions focus on agents with perfect information, i.e., agents who at any point of the game know exactly the global state of the game, which is unrealistic in all but the simplest multi-agent scenarios. Moreover, model checking **ATL** with imperfect information is hard, both theoretically and in practice. Secondly, the semantics of strategic logics are almost exclusively based on synchronous concurrent game models. That is, one implicitly assumes the existence of a global clock that triggers subsequent global events in the system. However, many real-life systems are inherently asynchronous. Thirdly, modern IT systems include technical as well as social components. Voting procedures are a good example here, and provide suitable material for case studies. However, the existing approaches to modelling and verification focus on the technical side of a system or a protocol, and it is not generally known how to formally specify the relevant human aspects.

The project aims at the development of novel methods of verification for multi-agent systems with imperfect information, in which technological components and machine-generated processes operate together with humans and their groups. The formal methodology is expected to build on suitable extensions of strategic logic interpreted in asynchronous models [2]. Regarding practical applications, the focus will be on modelling, specification, and verification of e-voting protocols.

More specifically, the verification methods developed by the candidates may include:

- Equilibrium-based specifications of vote privacy and coercion resistance, and ATL-based characterizations of rational coercion resistance, voter-verifiability, and accountability.

- Logical analysis of socio-technical interaction: development of semantics and algorithms for information-theoretic extensions of ATL, as well as entropy-based optimization of strategies.

- Separation and integration of concerns through assume-guarantee verification.
- Verification of information-theoretic properties in socio-technical games, including optimization of strategies based on incentives, effectivity, and degree of control, as well as reductions for socio-technical models of voting.
- Implementation of algorithms for model checking, strategy synthesis, and strategy optimization.
- Case studies in e-voting protocols.

The above topics are supposed to provide the contents of at least two potential PhD theses.

2. Profile of the Candidates

The candidates are required to have a strong background in mathematical logics, including modal logics, as well as programming skills (C++, Java, Python). Some knowledge of formal methods and verification techniques is expected. The candidates should also have good communication skills and good skills in oral and written English.

Bibliography

1. R. Alur, T. A. Henzinger, and O. Kupferman. Alternating-time Temporal Logic. Journal of the ACM, 49:672–713, 2002.
2. C. Dima, B. Maubert, and S. Pinchinat. Relating paths in transition systems: The fall of the modal mu-calculus. In Proceedings of MFCS, volume 9234 of Lecture Notes in Computer Science, pages 179–191. Springer, 2015.
3. W. Jamroga, M. Knapik, and D. Kurpiewski (2018), Model Checking the SELENE E-Voting Protocol in Multi-Agent Logics. Proceedings of the International Joint Conference on Electronic Voting E-VOTE-ID 2018, Lecture Notes in Computer Science vol. 11143, pp. 100-116. Springer.
4. W. Jamroga, W. Penczek, P. Dembinski, and A. Mazurkiewicz (2018), Towards Partial Order Reductions for Strategic Ability. Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems AAMAS 2018, pp. 156-165. IFAAMAS.
5. W. Jamroga and M. Tabatabaei (2017), Preventing Coercion in E-Voting: Be Open and Commit. Proceedings of the International Joint Conference on Electronic Voting E-VOTE-ID 2016. Lecture Notes in Computer Science, vol. 10141, pp. 1-17.
6. D. Kurpiewski, W. Jamroga, and M. Knapik (2019), STV: Model Checking for Strategies under Imperfect Information. Demo Track, AAMAS 2019.
7. A. Lomuscio, H. Qu, and F. Raimondi. MCMAS: An open-source model checker for the verification of multi-agent systems. International Journal on Software Tools for Technology Transfer, 2015.