Weryfikacja socjotechnicznych modeli systemów wieloagentowych i protokołów elektronicznego głosowania

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

1. Opis Projektu

Systemy wieloagentowe opisują interakcje wielu podmiotów zwanych agentami, często uważanymi za inteligentne i autonomiczne. Logika temporalna czasu alternującego **ATL*** i jej fragment **ATL** [1] pozwalają na wnioskowanie o strategicznych interakcjach w takich systemach, rozszerzając formalizm logiki temporalnej przez pojęcie *strategicznych umiejętności* z teorii gier. W związku z tym **ATL** umożliwia wyrażanie własności na temat tego, co agenci (lub grupy agentów) mogą osiągnąć. Takie własności mogą być przydatne do specyfikacji, weryfikacji i wnioskowania o interakcjach agentów w złożonych systemach. Stały się one szczególnie istotne ze względu na aktywny rozwój algorytmów i narzędzi do weryfikacji, gdzie własność "poprawności" jest zadawana przy użyciu strategicznych umiejętności [4]. W szczególności, modele i formuły ATL mogą posłużyć do specyfikacji i weryfikacji istotnych własności protokołów bezpiecznego głosowania, takich jak *odporność na przymuszanie, sprawdzalność oddanego głosu* oraz *sprawdzalność wyniku wyborów* [6,7].

Istnieje jednak kilka przeszkód. Po pierwsze, większość istniejących narzędzi i rozwiązań algorytmicznych koncentruje się na agentach dysponujących pełną informacją, tzn. agentów, którzy w dowolnym momencie gry dokładnie znają globalny stan gry, co jest nierealistyczne za wyjątkiem najprostszych scenariuszy. Z kolei weryfikacja modelowa **ATL** z niepełną informacją jest trudna zarówno teoretycznie, jak i z praktycznego punktu widzenia. Po drugie, semantyka logik strategicznych jest niemal wyłącznie oparta na synchronicznych modelach gier współbieżnych. Oznacza to, że zakłada się wprost istnienie globalnego zegara, który taktuje kolejne globalne zdarzenia w systemie. Jednak wiele rzeczywistych systemów jest z natury asynchronicznych. Po trzecie, współczesne systemy łączą w sobie elementy techniczne i społeczne, co znakomicie widać na przykładzie procedur wyborczych. Jednakże istniejące podejścia do modelowania i weryfikacji koncentrują się na technicznej stronie systemu bądź protokołu; nie bardzo wiadomo zaś, jak uwzględnić w formalnej specyfikacji aspekty związane z działaniem ludzi.

Celem projektu jest opracowanie nowych metod weryfikacji systemów wieloagentowych z niepełną informacją, w których elementy technologiczne i procesy maszynowe przeplatają się z działaniem ludzi i ich grup. Przewidujemy, że podejście formalne będzie oparte o odpowiednie rozszerzenia logiki strategicznej interpretowanej w modelach asynchronicznych [2]. Jeśli chodzi o praktyczne zastosowania, główny nacisk zostanie położony na modelowanie, specyfikację i weryfikację procedur i protokołów e-głosowania.

W szczególności, rozwijane przez kandydatów metody weryfikacji mogą wykorzystywać następujące podejścia:

- Specyfikacja konfidencjonalności głosów i odporności na przymuszanie, oparta o pojęcia równowagi w grach; charakteryzacje racjonalnej odporności na przymuszanie, sprawdzalności głosu i odpowiedzialności za nieprawidłowości.
- Logiczna analiza of interakcji socjo-technicznej: semantyka i algorytmy dla rozszerzeń **ATL**, opartych o pojęcia z teorii informacji; optymalizacja strategii oparta o entropię.

- Separacja i integracja podproblemów poprzez weryfikację typu *assume-guarantee*.
- Weryfikacja teorio-informacyjnych własności gier socjotechnicznych, w tym optymalizacja strategii w oparciu o bodźce ekonomiczne, efektywność i stopień kontroli, a także redukcje dla socjotechnicznych modeli głosowania.
- Implementacja algorytmów weryfikacji modelowej, syntezy strategii i optymalizacji strategii.
- Analiza formalna przykładowych protokołów e-głosowania.

Powyższe zagadnienia składają się na tematykę co najmniej dwóch potencjalnych rozpraw doktorskich.

2. Profil Kandydatów

Kandydaci muszą mieć dobre przygotowanie w zakresie logiki matematycznej, w tym logiki modalnej, a także umiejętności programowania (C++, Java, Python). Oczekuje się znajomości podstaw metod formalnych i technik weryfikacji. Kandydaci powinni posiadać również dobre umiejętności komunikowania się oraz dobrą znajomość języka angielskiego w mowie i piśmie

Bibliografia

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.