Replicated Computations Results (RCR) Report for “Design and Verification of Trusted Collective Adaptive Systems”

MAURICE H. TER BEEK, Consiglio Nazionale delle Ricerche (CNR), Istituto di Scienza e Tecnologie dell’Informazione (ISTI)

The article “Design and Verification of Trusted Collective Adaptive Systems” by Aldini proposes a process-algebraic framework for modeling and verifying trusted collective adaptive systems. To favor reuse, the system and trust models can be specified separately, only to be integrated at the semantic level. Through a combination of behavioral equivalence checking and model checking against branching-time temporal logic with trust predicates, the framework allows comparative analyses of different trust models as well as analyses of the effects of attacks to the trust models. The applicability of the formal framework is illustrated by means of two representative use cases: the security analysis of a trust-incentive service management system and a comparison of two different reputation systems.

This replicated computations results report focuses on the reproducibility of the experiments performed in the aforementioned article, i.e. on the automatic verification of properties against models of these use cases encoded in the well-known NuSMV model checker. It was straightforward to reproduce all results from the article in reasonable time using a standard laptop machine.

CCS Concepts: • **Security and privacy → Trust frameworks**; **Logic and verification**; • **Theory of computation → Process calculi**; **Verification by model checking**; • **Computing methodologies → Model verification and validation**;

Additional Key Words and Phrases: RCR report, collective adaptive systems, trust and reputation models, model checking

ACM Reference format:

Maurice H. ter Beek. 2018. Replicated Computations Results (RCR) Report for “Design and Verification of Trusted Collective Adaptive Systems”. *ACM Trans. Model. Comput. Simul.* 28, 2, Article 10 (February 2018), 3 pages.

https://doi.org/10.1145/3170502

1 INTRODUCTION

The article “Design and Verification of Trusted Collective Adaptive Systems” by Aldini [1] proposes a process-algebraic framework for modeling and verifying an important, yet understudied, aspect of Collective Adaptive Systems (CAS). That aspect is the individuals’ attitude to cooperation—measured in terms of trust—as a means to prevent selfish and malicious behavior. The system and trust models can be specified separately to favor their reuse, after which they are seamlessly integrated at the semantic level. Through a combination of behavioral equivalence checking and model checking against branching-time temporal logic with trust predicates, the framework allows

Authors’ address: M. H. ter Beek, Consiglio Nazionale delle Ricerche (CNR), Istituto di Scienza e Tecnologie dell’Informazione (ISTI), Via G. Moruzzi 1, Pisa, 56125, Italy; email: maurice.terbeek@isti.cnr.it.

https://doi.org/10.1145/3170502

comparative analyses of different trust models and analyses of the effects of a number of possible attacks to the trust models. These attacks range from *bad mouthing/ballot stuffing*, i.e., negative/positive feedback reported by one individual about the behavior of another (trusted/malicious) individual, to *collusion*, i.e., a conspiracy of individuals against an honest individual, to *whitewashing*, i.e., a misbehaving individual who leaves the system as soon as the individual's reputation is compromised only to rejoin under a different identity [6]. The applicability of the formal framework is illustrated by means of two representative use cases: the security analysis of a trust-incentive service management system and a comparison of two different reputation systems.

This is a replicated computations result report for the aforementioned article. The replication of the results of the latter article proceeded as follows. First, the NuSMV tool [4] used in the article was downloaded from http://nusmv.fbk.eu/ and installed. While NuSMV is a well-known symbolic model checker, with which I already had some experience, I downloaded and installed its latest version (NuSMV v2.6) for this purpose. Subsequently, all (model-checking) experiments described in the article were replicated. This work was supported by documentation provided by the author.

2 REPLICATION OF COMPUTATION RESULTS

The author supplied all NuSMV models designed for the two use cases described in the article, together with detailed information on how to replicate the experiments. This included translations of the CTL formulae reported in the article into the textual format accepted by NuSMV, involving mathematical symbols (e.g., & instead of $\wedge$ and ! instead of $\neg$) as well as notations used in the NuSMV models (e.g., cdsr1.trust for the trust metric from $Club_1$ to P_2, denoted by $t_{Club_1 P_2}$ in the article). Such detailed information was very useful for a smooth replication.

I performed the experiments on my MacBook Pro equipped with a 2.9GHz Intel Core i5 and 16GB of RAM.

It was straightforward to reproduce the results concerning the evaluation of an NuSMV model of the Trust-Incentive Service Management system [7] (TIM) that led to Figures 1 to 3 in Section 4. The same holds for the results that led to Figure 4 in Section 5, concerning the comparison between NuSMV models of the Reputation-based Framework for Sensor Networks [5] (RFSN) and of the Robust Reputation System integrated in the CONFIDANT protocol [2, 3] (RSS). In Section 5, this comparative analysis of two trust models was extended to the case in which at least one individual exhibits selfish or malicious behavior. It was forthright to verify that Formula 4 is indeed satisfied by the NuSMV model of the RSS, in which a malicious version of agent Req_2 is specified, but not by the model containing the original specification of agent Req_2. (Instead, the NuSMV model of the RFSN is robust against false recommendations provided by Req_2.) Finally, at the end of Section 5, the author discusses the case of a dishonest forwarder agent *For* denying the forwarding service and that of a forwarder *For* colluding with Req_2 to send positive recommendations to agent Req_1. In both cases, and for both trust models, the model-checking results confirming the differences between the original specifications and the ones with malicious behavior could be reproduced effortlessly.

ACKNOWLEDGMENTS

The author would like to thank Alessandro Aldini for providing detailed instructions and all necessary NuSMV models and CTL formulae to replicate the experiments described in the article to which this report refers.

REFERENCES

[1] Alessandro Aldini. 2018. Design and verification of trusted collective adaptive systems. *Transactions on Modeling and Computer Simulation* 28, 2, Article XX, XX pages.

[2] Sonja Buchegger and Jean-Yves Le Boudec. 2002. Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02)*. ACM, 226–236. DOI: http://dx.doi.org/10.1145/513800.513828

[3] Sonja Buchegger and Jean-Yves Le Boudec. 2004. A robust reputation system for P2P and mobile ad-hoc networks. In *Proceedings of the 2nd Workshop on Economics of Peer-to-Peer Systems (P2PEcon'04)*. Harvard University, Cambridge, MA, USA.

[4] Alessandro Cimatti, Edmund M. Clarke, Enrico Giunchiglia, Fausto Giunchiglia, Marco Pistore, Marco Roveri, Roberto Sebastiani, and Armando Tacchella. 2002. NuSMV 2: An opensource tool for symbolic model checking. In *Proceedings of the 14th International Conference on Computer Aided Verification (CAV'02)*, Lecture Notes in Computer Science, Ed Brinksma and Kim Guldstrand Larsen (eds.), Vol. 2404. Springer, Berlin, 359–364. DOI: http://dx.doi.org/10.1007/3-540-45657-0_29

[5] Saurabh Ganeriwal, Laura K. Balzano, and Mani B. Srivastava. 2008. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks* 4, 3, Article 15, 37 pages. DOI: http://dx.doi.org/10.1145/1362542.1362546

[6] Félix Gómez Mármol and Gregorio Martínez Pérez. 2009. Security threats scenarios in trust and reputation models for distributed systems. *Computers and Security* 28, 7, 545–556. DOI: http://dx.doi.org/10.1016/j.cose.2009.05.005

[7] Yu Zhang, Li Lin, and Jinpeng Huai. 2007. Balancing trust and incentive in peer-to-peer collaborative system. *International Journal of Network Security* 5, 1, 73–81. http://ijns.jalaxy.com.tw/contents/ijns-v5-n1/ijns-2007-v5-n1-p73-81.pdf.

Received November 2017; accepted November 2017