Model Checking of Trust-Based User-Centric Cooperative Networks

Alessandro Aldini and Alessandro Bogliolo
University of Urbino "Carlo Bo"
Urbino, Italy
{*alessandro.aldini,alessandro.bogliolo*}*@uniurb.it*

***Abstract*—The success of user-centric networks depends on the willingness of the participants to cooperate by sharing resources and services. Reputation-based incentives and remuneration (based either on fiat money or on virtual currency) have emerged as two complementary incentive mechanisms to increase users' motivation and to discourage selfish behaviors. In this paper, we conduct a formal study of the benefits of the joint application of these two mechanisms in the context of a cooperation model recently proposed for user-centric wireless networks. To this purpose, several performance properties of cooperation incentives mechanisms are defined and analyzed through model checking of probabilistic systems with an underlying Markov process semantics.**

***Keywords*-trust, virtual currency, model checking, user-centric networks.**

I. INTRODUCTION

As more and more people get involved in any kind of online communities, ranging from social networks to sharing communities and online games, user centric networking is becoming more and more relevant for the future of the Internet. User centricity, however, entails cooperation among members of broad communities who usually do not know each other in person. Hence, cooperation incentives and trust mechanisms are essential requisites of any community, the success of which strongly depends on the willingness of its members to cooperate and can be impaired by mistrust and selfishness. This is particularly true in user-centric wireless networks (UCNs), where even the underlying communication infrastructure is dynamically built by users who share their Wi-Fi connections, and the inherent limitations of mobile devices (in terms of battery, CPU, and bandwidth) can keep users from adopting prosocial behaviors.

When *inherent* motivations (including fairness, synergy, and sense of community) provide no sufficient cooperation incentives [1], they need to be complemented by *extrinsic* motivations, such as reputation, reciprocity, and monetization. It has been recently shown that a suitable support for the implementation of extrinsic cooperation incentive mechanisms in UCNs can be provided by the joint application of *trust management* [2] and *virtual currency* [3] systems [4]. Trust and virtual currency infrastructures provide the means for implementing the so-called *soft security*, which is characterized by relaxation of the security policies and enforcement of common ethical norms for the community [5]. Such means do not rely on pervasive controls concerning, e.g., assurance of payment or service delivery, thus exposing the system to dishonest behaviors that, however, are contrasted by the adoption of cooperation incentives. Hence, it is important to verify to what extent the incentives can deal successfully with mistrust, selfishness, and cheats.

A game-theoretic analytical study [6] has recently revealed that reputation-based and price-based strategies must be integrated in order to optimize the effects of cooperation incentives. Game theory has been widely used to conduct a mathematical analysis of the complex interactions among nodes of wireless ad-hoc networks [7], [6]. The results of the analytical study are consolidated by simulation results showing the fast convergence towards cooperative behaviors in the case of mixed incentive strategies.

This work provides an orthogonal view of the benefits of mixed cooperation incentives by employing formal analysis techniques for the evaluation of quantitative properties of systems. In particular, as a real-world case study, we analyze several performance metrics of the cooperation process envisioned by Bogliolo et al. [4] for UCNs.

Formal methods provide mathematically rigorous techniques and tools for the design and verification of systems. More precisely, formal specifications are mathematical models (e.g., automata), formal verifications are based on well-formed statements (e.g., in a temporal logic), and automatic checks rely on analysis algorithms (e.g., model checking). In this paper, we evalute the cooperation model under study through the probabilistic model checker PRISM (see, e.g., [8], [9] for a survey of the approach). The modeling language of PRISM is a state-based mathematical formalism based on the Reactive Modules introduced by Alur and Henzinger [10], from which different types of probabilistic models can be derived, including discrete-time Markov chains (DTMCs) and Markov decision processes (MDPs) [11], [12]. Performance properties are expressed in a temporal logic – subsuming both probabilistic computation tree logic (PCTL) and linear time logic (LTL) – which is expressive enough to specify state-based and path-based properties, and including both probabilistic and reward operators [13].

In the remainder of the paper, we briefly introduce the cooperation model of [4] and the related modeling assumptions (Section II), we report and discuss the results of the model checking analysis (Section III), and we draw conclusions (Section IV).

II. Cooperation Model

This section briefly outlines the cooperation model under study [4] and the modeling assumptions adopted for analysis purposes. Cooperation involves users providing services, hereafter called *requestees*, and recipients of such services, hereafter called *requesters*. According to [4], the cooperation process entails four phases, which rely on trust management and virtual currency.

In the first phase, called *discovery and request*, the requester searches for a requestee offering the required service. Reputation of the requestee is a parameter guiding the choice. If the requester is trustworthy enough to access the required service, then the issued request can be accepted. However, it may be also refused because of, e.g., lack of willingness to cooperate. In the second phase, called *negotiation*, requester and requestee establish service parameters and reward, possibly taking into account the trust of the requestee on the requester. In the third phase, called *transaction*, service is delivered and then the related payment is provided. In the fourth phase, called *evaluation and feedback*, the transaction results are used to adjust, if necessary, reputation of the involved parties.

A. Reputation System

As usual in several trust-based systems [5], we model trust (reputation) as a discrete metric. Basically, the cooperative attitude of the requestee depends on two parameters: the dispositional trust dt, representing the initial willingness to trust incoming requests, and the service trust level st, representing a threshold below which the service is not accessible. Then, given a requestee i and a requester j, the computation of the trust level of i towards j is obtained by mixing direct experience and indirect recommendations:

$$T_{ij} = \alpha \cdot trust_{ij} + (1 - \alpha) \cdot recs_{ij}$$

where $\alpha \in [0, 1]$, $trust_{ij}$ is the trust metric deriving from previous direct interactions of i with j (the initial value of $trust_{ij}$ is set to the dispositional trust of i, dt_i), and $recs_{ij}$ is the average of the trust metrics towards j of other users (different from i) that in the past negotiated directly with j. Notice that, if $T_{ij} < st_i$ then the service request of j cannot be accepted by i.

B. Virtual Currency System

Reputation-based and reward-based incentives are combined by including the trust level T of the requestee towards the requester as a parameter affecting the cost of the negotiated service. The other parameters are C_{min}, which is the minimum reward (cost) asked by the requestee regardless of his/her trust on the requester, C_{max}, which is the maximum reward asked to serve untrusted users, and T', which is the trust threshold above which the minimum cost is applied to the requester. Then, the cost function C proposed in [4] is defined as follows:

$$C(T) = \begin{cases} C_{min} + \frac{C_{max} - C_{min}}{T'} \cdot (T' - T) & T < T' \\ C_{min} & T \geq T' \end{cases} \quad (1)$$

C. Modeling Assumptions

For the sake of simplicity, here we assume that users do not play the roles of both requester and requestee. Moreover, we consider a unique type of service that is offered by each requestee in the network. Trust values range in the interval $[0, 10]$, such that $null = 0$, $low = 2$, $med = 5$, $high = 8$, and $top = 10$. Based on the system described above, the modeling assumptions concerning the four-phase cooperation process are as follows.

1) *Discovery and request.* The choice of the requestee can be nondeterministic, prioritized (precedence is given on the basis of (i) requestee's reputation and then (ii) requestee availability to negotiate; choice among requestees with the same reputation is random), or probabilistic (probabilities are weighted by requestee's reputation). By default, the chosen requestee i refuses the request of requester j if and only if $T_{ij} < st_i$. The default initial reputation is *low* for every requestee.
2) *Negotiation.* The agreement between i and j is successful. The cost C determined by i through the application of Equation (1) is accepted by j without any further negotiation. The default values are $C_{min} = 0$, $C_{max} = 10$, and $T' = high$.
3) *Transaction.* By default, the service is delivered with success. Then, j decides whether to pay or not, either nondeterministically or probabilistically with parameter $p \in [0, 1]$, namely j pays the obtained service with probability p.
4) *Evaluation and feedback.* Since the service is satisfactory, the reputation of i as perceived by j is increased by 1. On the other hand, the trust of i towards j increases (decreases) by 1 (by a factor k) in the case j pays (or not) the service. Feedback is provided by i to the other requestees.

The reader interested in the PRISM formal specifications of the cooperation model and of the logic-based properties analyzed in the following section can refer to: `http://www.sti.uniurb.it/aldini/prism_uloop/`.

III. Model Checking of the Cooperation Model

The analysis of the cooperation process through model checking is divided into two steps. First, we study the vulnerabilities of the trust-based mechanism with respect to a possibly cheating requester that may decide not to pay the obtained services. Based on the results of such an analysis, we then verify the efficiency of the mixed cooperation incentives in discouraging selfish behaviors of the requestees and motivating honest behaviors of the requester.

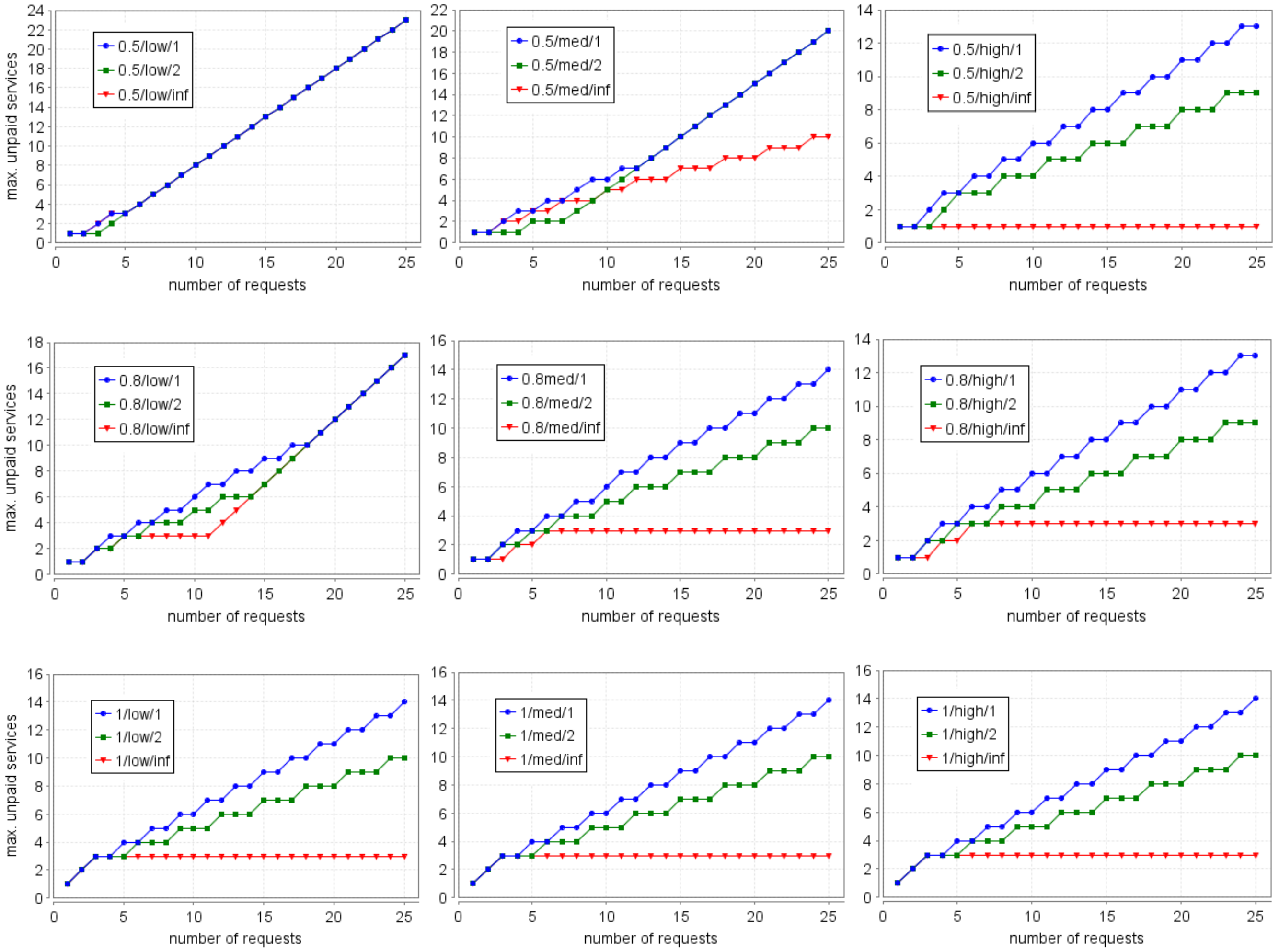


Figure 1: MDP analysis: verification of Property 1 for 27 combinations of parameters $\alpha/st/k$.

A. MDP Analysis

The effectiveness of the trust-based mechanism with respect to cheating requesters is expressed through the following property:

Property 1. What is the maximum number of services (out of nr requests) that can be obtained by a requester without honouring the payment?

This property is investigated in a scenario with a single requester and three alternative requestees. With respect to the assumptions of Section II-C, we consider requester's choices to be nondeterministic. Hence, the requester can be viewed as an adversary controlling the way in which the nondeterminism is solved adaptively. The aim of such an adversary is to find out the strategy maximizing the number of unpaid services, thus revealing the worst case from the viewpoint of the requestees.

Formally, the semantics of the model turns out to be an MDP on which Property 1 is evaluated by solving the nondeterminism in all possible ways. Then, the model checker returns the result for the *best adversary* strategy. Notice that such a strategy corresponds to the most powerful adversary, which can observe the behavior and the configuration parameters of all the requestees.

We assume three equal requestees characterized by the configuration of parameters $\alpha/st/k$, where: $\alpha \in \{0.5, 0.8, 1\}$ is the contribution of direct experience to trust, $st \in \{low, med, high\}$ is the service trust threshold, and $k \in \{1, 2, \infty\}$ denotes the rapidity with which the trust towards a cheating requester is decreased each time a payment is not honoured (∞ stands for the immediate assignment of the value *null* to the trust level). The dispositional trust is chosen to be equal to the service trust threshold in order to make it possible for a new requester to start negotiating services with the requestees.

All the 27 combinations of the parameters introduced above are analyzed, as illustrated in Fig. 1. The horizontal axis denotes the total number of requests nr, ranging from 1 to 25, while the vertical axis reports the maximum number of unpaid services. From the analysis, we observe that for each value of α and st the success of the cheating strategy is inversely proportional to the factor k. In practice, the higher the value of k is, the faster the reaction to dishonest behaviors and, therefore, the negative effect upon trust. For the same reason, the higher the service trust level st is, the lower the number of unpaid services. When $\alpha = 1$, however, the service trust level does not affect the results because any decision depends only on previous direct experience. The analysis could be extended to values of $\alpha < 0.5$, obtaining results similar to those related to $0.5/low/\_$, regardless of the value of st. These results reveal a typical attack of a dishonest requester cheating only one requestee, which gives too much weight to the positive recommendations provided by the other requestees.

The results of Figure 1 suggest to categorize the behavior of the requestee according to two limiting profiles:

- *risky* profile, for which the unpaid services increase linearly and most of the served requests are unpaid (see, e.g., configurations $0.5/low/\_$, $0.8/low/\_$ and $\_/\_/1$).
- *cautious* profile, for which the number of unpaid services is essentially constant (see, e.g., configurations $\_/high/\infty$, $0.8/med/\infty$, and $1/\_/\infty$).

B. DTMC Analysis

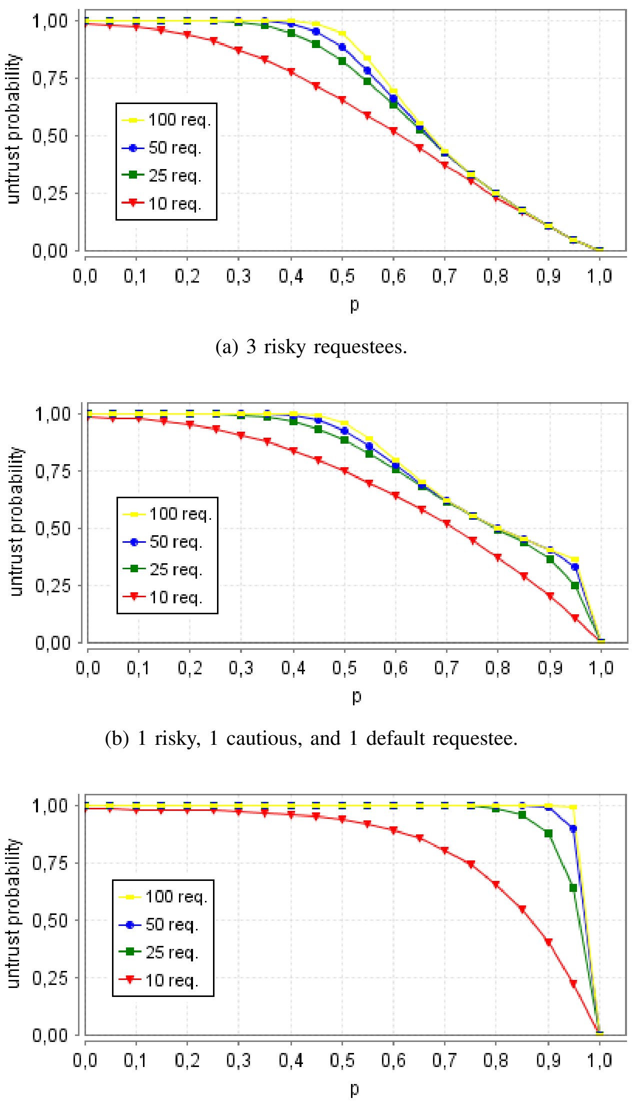
The two profiles defined above give a clear and precise perception of requestee's attitude to take prosocial decisions in an environment where requesters are possibly cheating. This subsection reports the results of further investigations conducted by considering risky requestees represented by configuration $0.5/low/1$ and cautious requestees represented by configuration $0.8/med/\infty$. Whenever the profile is not specified, configuration $0.8/low/1$ is taken as default.

In order to analyze more specific properties, we assume prioritized choice of the requestee and payment honoured probabilistically with parameter p (see Section II-C). Hence, now the semantics of the model is a DTMC, on which both *steady-state* and *transient-state* analyses can be conducted.

On one hand, the steady-state analysis reveals the success of the cooperation mechanism on the long run. Indeed, it turns out that at steady state for each $p < 1$ the requester becomes untrusted with probability 1 by any requestee. On the other hand, the transient analysis is important to study the convergence speed towards such a result.

Property 2. What is the probability for a cheating requester of being untrusted by each requestee after nr requests?

We evaluate this property by varying parameter p and by assuming $nr \in \{10, 25, 50, 100\}$. Moreover, we consider: (i) three risky requestees (see Fig. 2a), (ii) three requestees among which one is risky and one is cautious, while the default configuration is adopted for the third one (see Fig. 2b), and (iii) three cautious requestees (see Fig. 2c). All the curves tend rapidly to 1 for $p < 0.5$ and converge to zero as p tends to 1. In particular, notice that in the case of 3 cautious requestees, for $nr \geq 25$ the curves approximate a step function, meaning that a cheating requester is almost immediately untrusted by each requestee.



(a) 3 risky requestees.

(b) 1 risky, 1 cautious, and 1 default requestee.

(c) 3 cautious requestees.

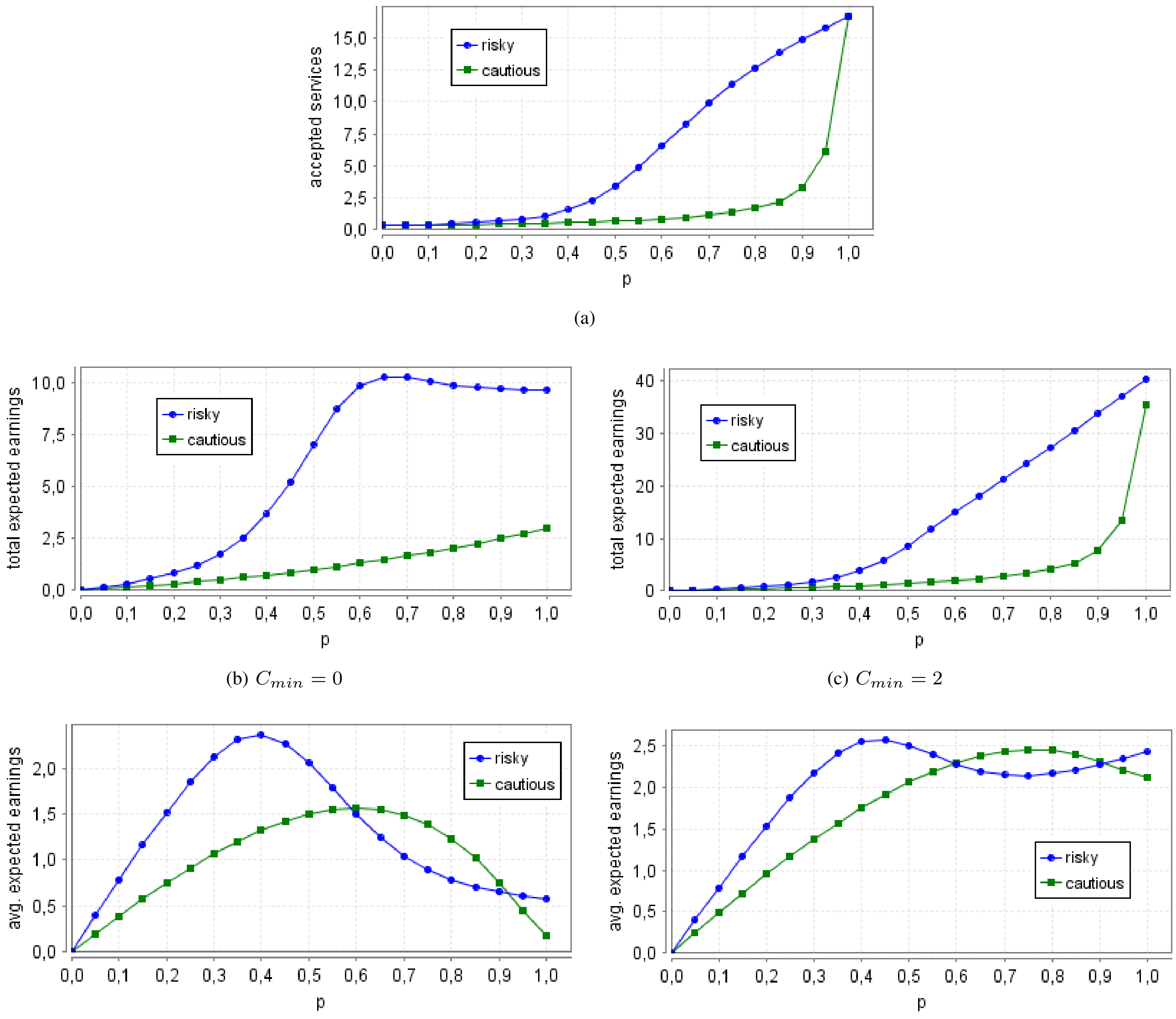
Figure 2: DTMC analysis: verification of Property 2.

Three more properties are tested in order to investigate the economic aspects of the cooperation mechanism:

Property 3. What is the number of requests accepted by each requestee?

Property 4. What is the total expected earning for each requestee?

Property 5. What is the average earning per accepted request?



(a)

(b) $C_{min} = 0$

(c) $C_{min} = 2$

(d) $C_{min} = 0$

(e) $C_{min} = 2$

Figure 3: DTMC analysis: verification of Properties 3, 4, and 5.

We use these properties to compare the two profiles in a scenario with 50 requests and three requestees like those of Fig. 2b. Fig. 3 reports the performance of the risky and cautious requestees as a function of parameter p. The curves show the following results.

The number of services accepted by the risky requestee is higher than that related to the cautious requestee, see Fig. 3a. The difference is due to the relaxed conditions applied by the risky requestee, in particular the assumption $k = 1$ (resp. $k = \infty$ for the cautious requestee). In fact, by setting $k = \infty$ also for the risky requestee, its curve would collapse with that of the cautious requestee. Notice that in case of honest requester (i.e., $p = 1$), the profile of the requestees does not play any role, so that the requests are equally distributed among them, because they are assigned with the same initial reputation.

As p increases, the total expected earnings of the risky requestee become much higher than those of the cautious one, see Fig. 3b. The difference can be interpreted as a reward for taking more risk.

Similarly, Fig. 3d shows that the average expected reward/cost per service grows with the value of p up to a maximum point beyond which the expected reward/cost decreases because of the effect of the trust-based discount applied to trustworthy requesters. Such a maximum point is reached earlier by the risky requestee, thus motivating the better performance of the cautious requestee for $p \in [0.6; 0.9]$. We also observe that in such an interval the trust level of the requester becomes stably high from the viewpoint of the risky requestee, as emphasized by the total earnings curve of Fig. 3b. For $p \geq 0.95$, the result is better for the risky requestee, because the requester becomes trustworthy also from the viewpoint of the cautious requestee, with a positive impact upon the number of services such a requestee accepts, see Fig. 3a.

In general, the combined effect of cost function and trust management works as an incentive to adopt a ”risky” prosocial behavior. On the other hand, it is clear that the requester obtains more services at a lower average cost whenever adopting a honest behavior.

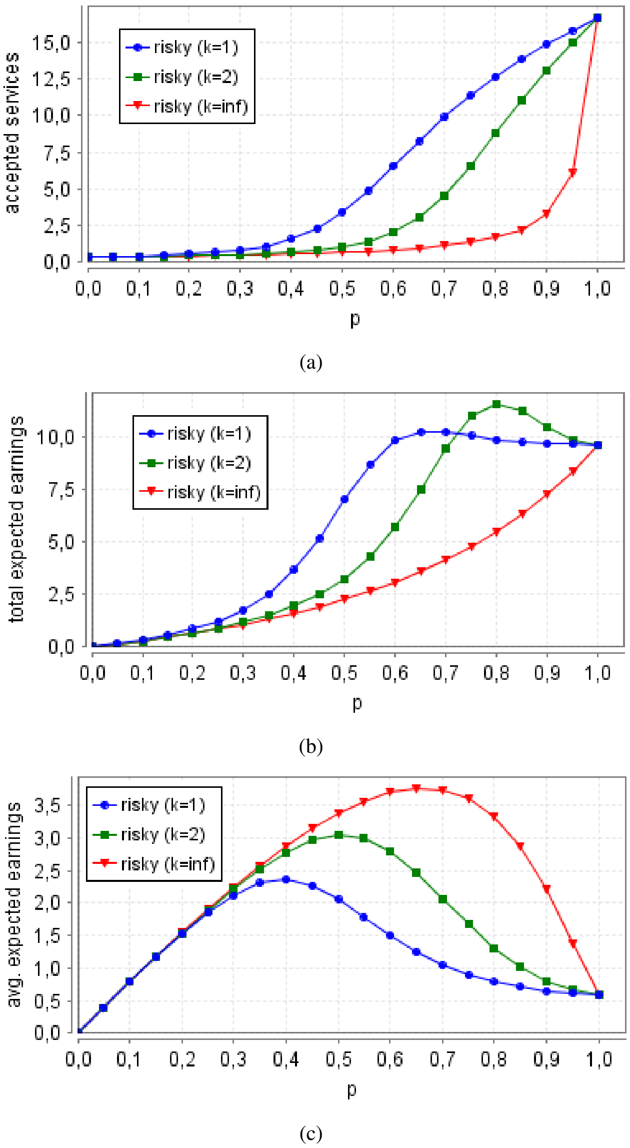
In order to show that the shape of the reward/cost curves is not purely a side effect of the assumption $C_{min} = 0$, in Figs. 3c and 3e we show the total and average expected reward/cost obtained in the case $C_{min} = 2$. The major earnings with respect to the corresponding curves of Figs. 3b and 3d reflect the difference between the minimum costs applied in the two experiments.

In order to emphasize the effect of parameter k on trust, in Fig. 4 we show the performance of the risky requestee for $k \in \{1, 2, \infty\}$ and by assuming the same scenario of Fig. 3. Observe that the curves related to number of accepted services and total earnings improve their performance as k decreases. Indeed, as we have previously seen, k and tolerance to cheating behaviors are inversely proportional. Instead, we observe the opposite result for the average earnings, because a high value of k corresponds to a fast trust decrease and, therefore, higher costs per service. Also notice that whenever the requester is honest and, as a consequence, k is never used, the three curves converge to the same values.

Similarly, we now study the impact of the dispositional trust. By varying parameter $dt \in \{low, med, high\}$, in Fig. 5 we show the performance for the risky requestee in the same scenario of Fig. 3. Increasing the dispositional trust has a twofold impact. On one hand, it works as an incentive to accept more services and augment the total earnings whenever the requester is not always honest. On the other hand, as p tends to 1, the service cost rapidly converges towards the minimum cost thus impairing the total earnings. The same considerations apply to the analysis of the relation between average reward/cost and dispositional trust.

C. *Requestee’s Reputation*

Requestee’s reputation is an orthogonal aspect the effects of which are analyzed in Fig. 6. The objective is to measure the impact of requestee’s reputation with respect to Property 3. In Fig. 6a we consider prioritized choice of the requestee, one risky requestee with reputation *high*, one cautious requestee with reputation *low*, while the reputation of the third requestee (with default profile) is *med*. Regardless of the profile, all the requests are served by the requestee with highest reputation, as imposed by the choice strategy followed by the requester. In fact, an analogous result would be obtained by swapping the reputations of the risky and cautious requestees. Giving less importance to reputation during the discovery phase has the effect of mitigating such a drastic behavior, as confirmed by the following experiment, in which the prioritized model of choice is replaced by the probabilistic one (see Section II-C). The results, shown in Fig. 6b, emphasize that also the cautious requestee can obtain some service. However, regardless of the value of p, it is always outperformed by the risky requestee.



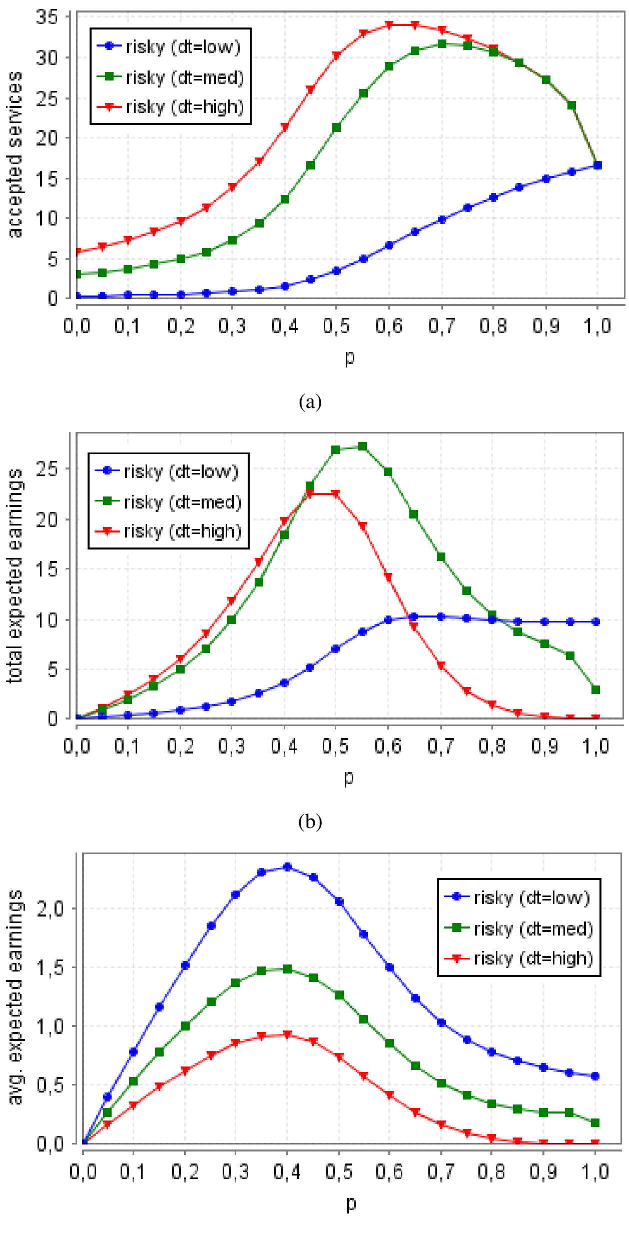
(a)

(b)

(c)

Figure 4: DTMC analysis: verification of Properties 3 to 5 for the risky requestee by varying parameter k.

The effect of requestee’s reputation is investigated also by testing the performance of a paranoid requestee ($\alpha = 0.5$, $dt = low$, $st = med$, $k = \infty$) replacing the cautious requestee in the experiment of Fig. 3. In Fig. 7a we evaluate

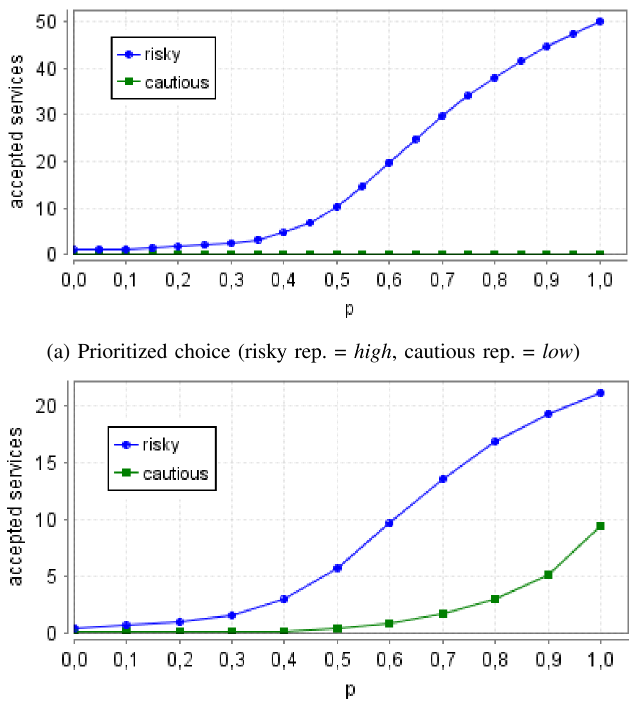


(a)

(b)

(c)

Figure 5: DTMC analysis: verification of Properties 3 to 5 for the risky requestee by varying parameter dt.



(a) Prioritized choice (risky rep. = *high*, cautious rep. = *low*)

(b) Probabilistic choice (risky rep. = *high*, cautious rep. = *low*)

Figure 6: DTMC analysis: verification of Property 3 with mixed reputations.

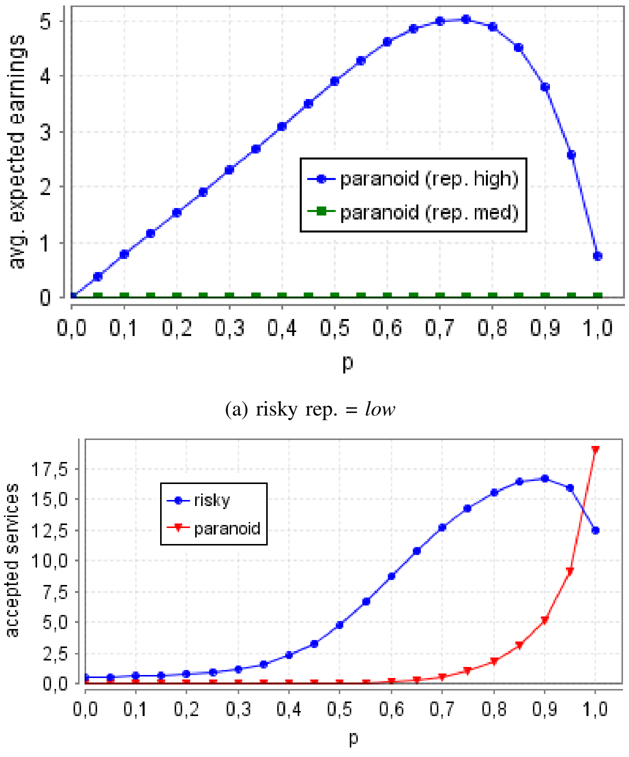
Property 5 for the paranoid requestee in two possible cases depending on its initial reputation. Apparently surprising, a paranoid requestee with reputation *med*, when put in competition with the other requestees (whose reputation is *low*), does not obtain any reward. This result is motivated by the fact that, initially, the paranoid requestee does not accept any request until a sufficiently high number of positive recommendations is received, because its service trust level is higher than its dispositional trust. Moreover, such requests are accepted by the other requestees, which gain reputation, thus causing preemption over the paranoid requestee during the prioritized discovery phase. In order to observe some request served by the paranoid requestee, it is necessary to set its initial reputation to *high*. In this case, we evaluate also Property 3 (see Fig. 7b). Notice that the paranoid requestee accepts a very low number of services for $p < 0.9$, while it outperforms the risky requestee only for $p = 1$, the reason being that the honest requester becomes trustworthy rapidly enough to overcome the non-cooperative attitude of the paranoid requestee.

In a real-world setting, reputation of the requestees may also decrease, e.g., because the quality of the delivered service does not match the negotiated parameters. This aspect is not captured by the experiments reported so far. In order to analyze the importance of requester's feedback, we extend the cooperation model to represent the (possibly negative) change of requestee's reputation due to requester's evaluations. In particular, we model probabilistically with parameter $q \in [0, 1]$ the event of a service failure causing a negative evaluation.

Property 6. How does requestee's reputation impact the number of accepted requests in the case of fallible services?

In a pessimistic scenario, upon each served request requestee's reputation has the same probability (namely, 0.33) of remaining unchanged, being increased by 1, or being decreased by 1. In an optimistic scenario, with probability

Copyright (c) IARIA, 2012. ISBN: 978-1-61208-211-0



(a) risky rep. = *low*

(b) risky rep. = *low*, paranoid rep. = *high*

Figure 7: DTMC analysis: verification of Properties 5 and 3 with paranoid requestee.

0.8 requestee's reputation is increased by 1, with probability 0.15 is maintained, and with probability 0.05 it is decreased by 1. We compare these two scenarios with the original one (modeling an ideal service provider) in which requestee's reputation is always incremented. Therefore, the three scenarios are characterized by $q = 0.33$, $q = 0.05$, and $q = 0$, respectively. Moreover, for the analysis we consider a honest requester, one cautious requestee with reputation *high*, one requestee with default profile and reputation *med*, and one risky requestee. In Fig. 8 we evaluate Property 6 for the risky requestee, by varying its initial reputation from 1 to 10. For $q = 0$, the risky requestee is always outperformed by the cautious requestee in every case in which its initial reputation is less than *high*. The two requestees share the same amount of services if the initial reputation of the risky requestee is *high* as well, while the risky requestee takes all the requests in the remaining cases. These results depend on the fact that the reputation level *high* of the cautious requestee never decreases. The other curves approximate such a behavior (the lower q is, the closer the approximation becomes) and reveal that the possibly negative feedback provided by the requester affects the performance of the requestees.

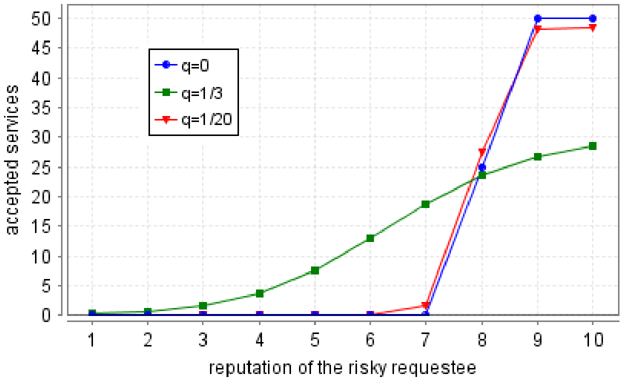


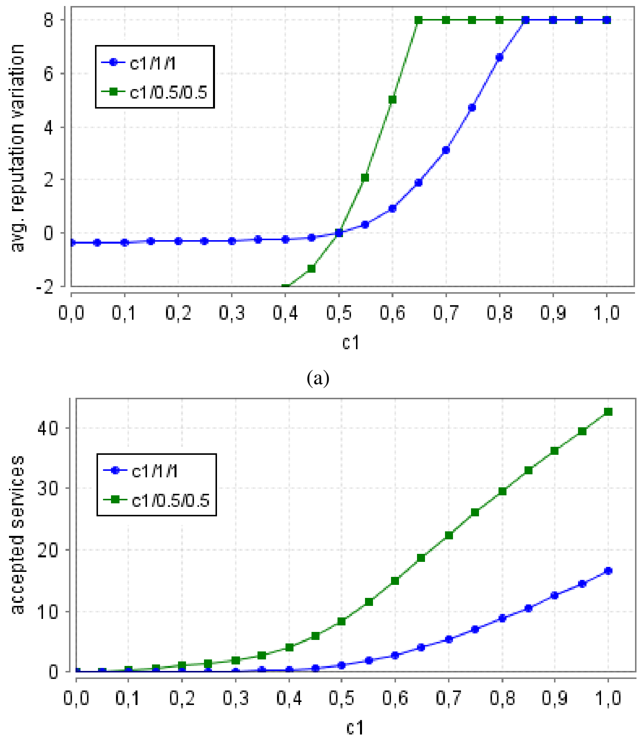
Figure 8: DTMC analysis: verification of Property 6.

In an orthogonal way with respect to the previous experiment, we now consider the case of non-cooperative requestees, which may refuse a request even if the requester is trustworthy enough to access the service. To this aim, we model probabilistically with parameter $c_i \in [0, 1]$ the cooperative attitude of requestee i, such that i accepts a trustworthy request with probability c_i and refuses it with probability $(1-c_i)$. Obviously, refusing a trustworthy request is evaluated with a reputation decrease, as opposite to the reputation increase determined by a satisfactory service.

Property 7. How does requestee's reputation vary in the case of non-cooperative requestees?

For analysis purposes, we consider a honest requester and three risky requestees with initial reputation $low = 2$. In Fig. 9a we evaluate Property 7 for the first requestee as a function of parameter c_1. In particular, we report its average relative reputation variation after 50 requests in two different cases, depending on the behavior of the other two requestees. In the first case, they are fully cooperative (i.e., $c_2 = c_3 = 1$), while in the second case they are partially cooperative (i.e., $c_2 = c_3 = 0.5$). In general, the lack of cooperation has a negative impact upon reputation of the first requestee, while it converges towards the top level as c_1 increases. We also observe that the reputation variation is slower in the first case with respect to the second case. The reason is that in the first case most of services are required to the two cooperative requestees, whose reputation increases rapidly thanks to their prosocial behavior. In order to emphasize the benefits of cooperative behaviors, in Fig. 9b we evaluate Property 3 for the first requestee in the two cases above. Notice that in the second case the number of services accepted by the first requestee increases dramatically whenever its attitude to cooperate becomes higher than that of the other two requestees.

Finally, we verify how the observed results scale by considering five requestees (four risky and one cautious with the same parameters assumed in the analysis of Fig. 3). It is worth comparing the obtained results, see Fig. 10, with those of Figs. 3a and 3b. The analogy is emphasized by the



(a)

(b)

Figure 9: DTMC analysis: verification of Properties 7 and 3 with non-cooperative requestees.

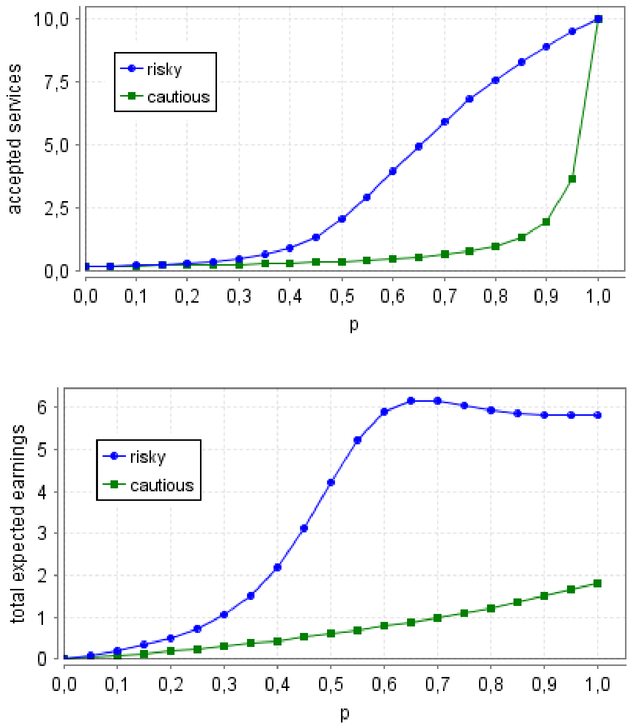


Figure 10: DTMC analysis: verification of Properties 3 and 4 with 5 requestees.

fact that the average expected earnings are exactly the same as those of Fig. 3d.

IV. Conclusion

Mixed incentive strategies, combining reputation and price-based mechanisms, have proved effective in inducing prosocial behaviors while isolating selfish or cheating nodes in a community [6]. A cooperation process entailing both trust management and virtual currency to support mixed incentive strategies has been recently proposed for user-centric wireless networks [4]. This paper has reported the results obtained by applying model checking techniques to provide formal evidence of the properties of such a process.

In summary, cooperation incentives work properly for both the requester and the requestee. On one hand, a honest behavior of the requester is motivated by a higher number of accepted services at a lower average cost with respect to the results obtained by a possibly cheating requester. On the other hand, both the reputation and the cooperative attitude of the requestee have a positive impact upon the amount of delivered services and the related earnings. This relation is exacerbated whenever the requester adopts a prioritized model for choosing the requestee during the discovery phase. Moreover, from the viewpoint of the requestee, cautious choices for the values of dispositional trust, minimum trust level required to access the service, and all the configuration parameters affecting the trust adjustment, impair directly the trading volume and indirectly the reputation if in the same network cooperative requestees are active.

The formal approach adopted in this work is currently under development in order to build a design tool to be used to assist the design and configuration of mixed incentive strategies in real-world user-centric networks. In particular, we are considering variants of the formal model taking into account more requestee's profile combinations and configuration parameter settings. This extended study is intended to integrate the overview provided in this work with a complete sensitivity analysis. We conclude by observing that the perspective provided in this paper is under consideration for being adopted by the ULOOP Consortium [14].

Acknowledgment

The research leading to these results has received funding from the EU IST Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number 257418, project ULOOP User-centric Wireless Local Loop.

References

[1] C.H. Declerck, C. Boone, and G. Emonds. *When Do People Cooperate? The Neuroeconomics of Prosocial decision Making*. Working paper of the Faculty of Applied Economics, University of Antwerp, 2011.

[2] S. Marsh. *Formalizing Trust as a Computational Concept*. PhD Thesis, Department of Mathematics and Computer Science, University of Stirling, 1994.

[3] S. Greengard. *Social Games, Virtual Goods*. Communications of the ACM, Vol. 54, No. 4, pp. 19-22, 2011.

[4] A. Bogliolo, P. Polidori, A. Aldini, W. Moreira, P. Mendes, M. Yildiz, C. Ballester, and J.-M. Seigneur. *Virtual Currency and Reputation-Based Cooperation Incentives in User-Centric Networks*. IEEE Int. Wireless Communications and Mobile Computing Conference (IWCMC-2012), Cyprus, 2012.

[5] A. Jøsang. *Trust and Reputation Systems*. In A. Aldini and R. Gorrieri, eds., Foundations of Security Analysis and Design IV (FOSAD'07), LNCS 4677:209–245, Springer, 2007.

[6] Z. Li and H. Shen. *Game-Theoretic Analysis of Cooperation Incentives Strategies in Mobile Ad Hoc Networks*. IEEE Transactions on Mobile Computing, 2012.

[7] V. Srivastava, J. Neel, A. MacKenzie, R. Menon, L. DaSilva, J. Hicks, J. Reed, and R. Gilles. *Using Game Theory to Analyze Wireless Ad Hoc Networks*. IEEE Communications Surveys and Tutorials 7(4), pp. 46–56, 2005.

[8] V. Forejt, M. Kwiatkowska, G. Norman, and D. Parker. *Automated Verification Techniques for Probabilistic Systems*. In M. Bernardo and V. Issarny, eds., Formal Methods for Eternal Networked Software Systems (SFM'11), LNCS 6659:53–113, Springer, 2011.

[9] M. Kwiatkowska, G. Norman, and D. Parker. *Stochastic Model Checking*. In M. Bernardo and J. Hillston, eds., Formal Methods for Performance Evaluation (SFM'07), LNCS 4486:220–270, Springer, 2007.

[10] R. Alur and T. Henzinger. *Reactive Modules*. Formal Methods in System Design, 15:7–48, 1999.

[11] W.-J. Stewart. *Introduction to the Numerical Solution of Markov Chains*. Princeton, 1994.

[12] R. Segala. *Modelling and Verification of Randomized Distributed Real Time Systems*. Ph.D. thesis, MIT Press, 1995.

[13] C. Baier and J.-P. Katoen. *Principles of Model Checking*. MIT Press, 2008.

[14] ULOOP. *EU IST FP7 ULOOP: User-Centric Wireless Local Loop*. http://uloop.eu, 2010-2013.