Xu GUO, 2022. Fairness analysis of extra-gain guilty of a non-repudiation protocol. *Frontiers of Information Technology & Electronic Engineering*, 23(6):893-908. https://doi.org/10.1631/FITEE.2000353

Fairness analysis of extra-gain guilty of a non-repudiation protocol

Key words: Non-repudiation; Fairness analysis; Probabilistic model checking; PRISM

Corresponding author: Xu GUO
E-mail: guox@sdju.edu.cn
ORCID: https://orcid.org/0000-0003-0803-8620

Motivation

- With the wide application of blockchain, fairness requirements appear in almost all the application scenarios, such as double payment and hard fork, which are caused by block conflicts and can directly affect the integrity and effectiveness of E-commerce transactions.
- Non-repudiation service is one of the vital security services in blockchain technology. It is a challenge for non-repudiation protocols to ensure fairness.
- Probabilistic model checking technique shows great potential in quantitative analysis for fairness.

Main idea

- Details of the original non-repudiation protocol are chosen. The main contents are retained and some details are ignored.
- A probabilistic timed automata (PTA) model of non-repudiation protocol is built.

Method

- The verified properties are described in terms of probabilistic computation tree logic.
- Three versions are considered: the two parties fully abide by the protocol; the receiving party violates the protocol and has certain deception; the computing power of the receiver is improved, and messages can be decoded within the prescribed time to further forge evidence.

Method

Models for the originator and recipient

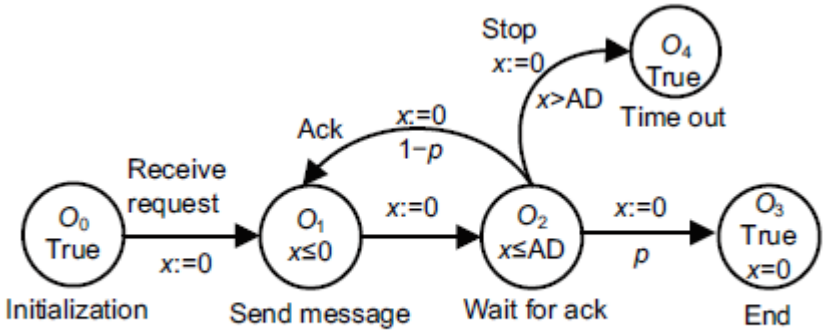

Fig. 2 An originator model

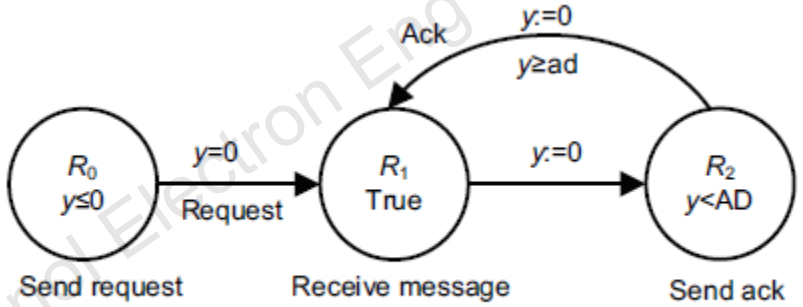

Fig. 3 An honest recipient model

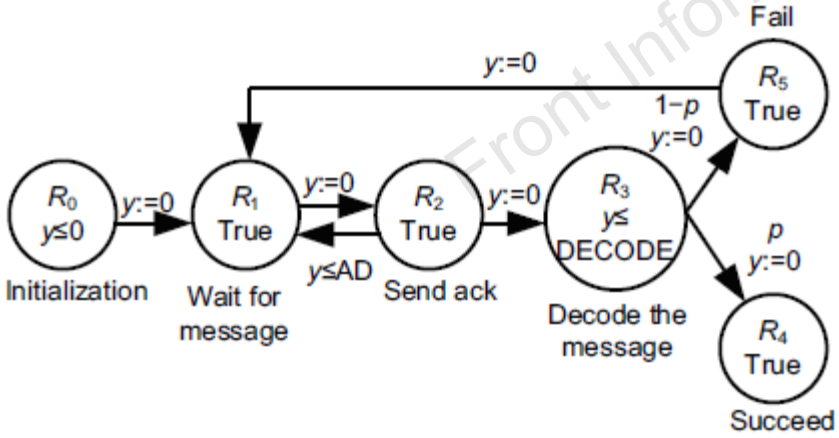

Fig. 4 A simple malicious recipient (SMR) model

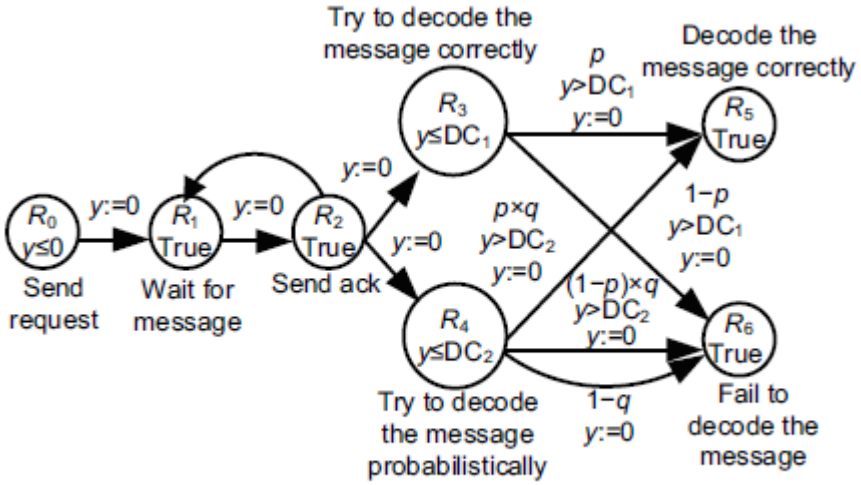

Fig. 5 A more powerful malicious recipient model

Major results

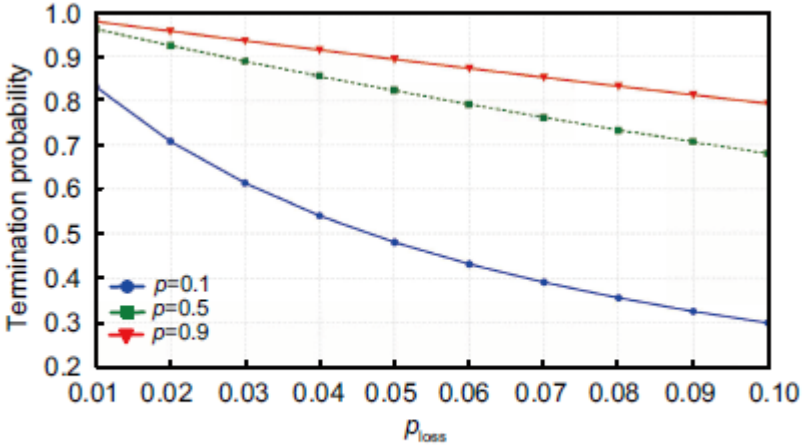

Fig. 6 Termination probability for a lossy channel

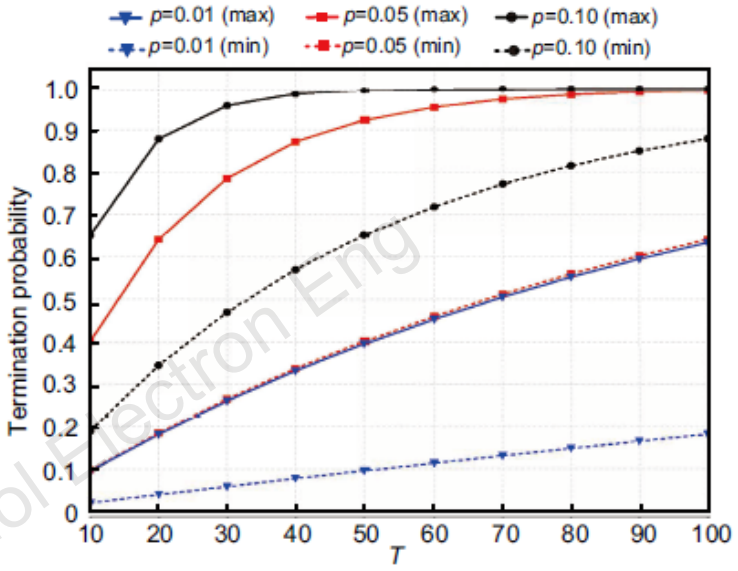

Fig. 7 Termination probability within T time units

Table 3 The minimum and maximum probabilities for other values of p

p	Minimum probability									
	$T=10$	20	30	40	50	60	70	80	90	100
0.02	0.040	0.078	0.114	0.149	0.183	0.215	0.246	0.276	0.305	0.332
0.07	0.135	0.252	0.353	0.440	0.516	0.581	0.638	0.687	0.729	0.766
0.20	0.360	0.590	0.738	0.832	0.893	0.931	0.956	0.972	0.982	0.988
0.40	0.640	0.870	0.953	0.983	0.994	0.998	0.999	1.000	1.000	1.000
0.60	0.840	0.974	0.996	0.999	1.000	1.000	1.000	1.000	1.000	1.000

p	Maximum probability									
	$T=10$	20	30	40	50	60	70	80	90	100
0.02	0.183	0.332	0.455	0.554	0.636	0.702	0.757	0.801	0.838	0.867
0.07	0.516	0.766	0.887	0.945	0.973	0.987	0.994	0.997	0.999	0.999
0.20	0.893	0.988	0.999	1.000	1.000	1.000	1.000	1.000	1.000	1.000
0.40	0.994	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
0.60	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Major results

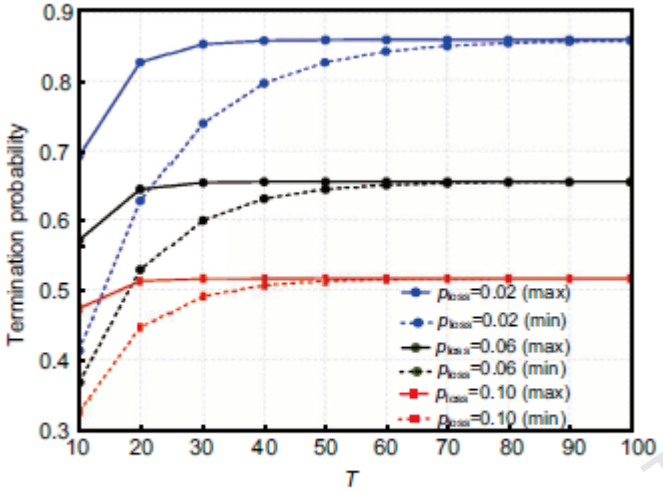

Fig. 8 Termination probability within T time units for lossy channels ($p = 0.25$)

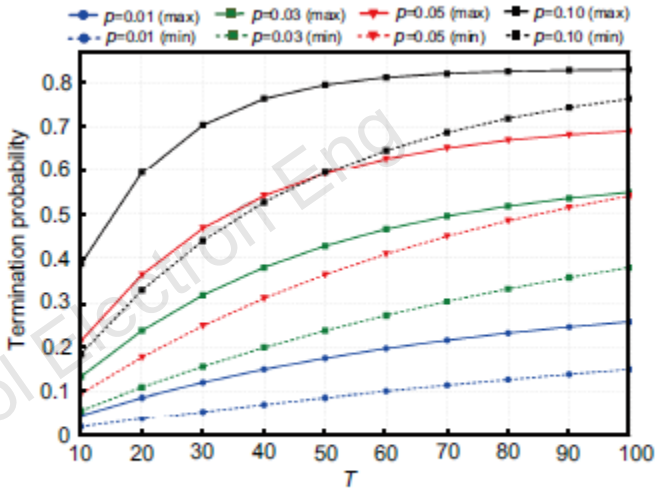

Fig. 9 Termination probability within T time units for lossy channels (p_{loss}=0.01)

Table 4 Minimum termination probability for other values of p and p_{loss}

p	p_{loss}	Minimum termination probability									
		$T = 10$	20	30	40	50	60	70	80	90	100
0.01	0.01	0.019	0.037	0.055	0.071	0.086	0.100	0.114	0.126	0.138	0.149
	0.05	0.017	0.031	0.042	0.050	0.057	0.063	0.067	0.071	0.074	0.076
	0.09	0.015	0.025	0.032	0.037	0.040	0.042	0.043	0.044	0.045	0.045
0.05	0.01	0.095	0.177	0.248	0.309	0.363	0.409	0.449	0.484	0.514	0.541
	0.05	0.084	0.145	0.191	0.224	0.248	0.266	0.280	0.289	0.297	0.302
	0.09	0.074	0.120	0.148	0.166	0.176	0.183	0.187	0.190	0.192	0.193
0.10	0.01	0.184	0.328	0.440	0.527	0.594	0.647	0.688	0.720	0.744	0.764
	0.05	0.164	0.271	0.343	0.390	0.421	0.441	0.455	0.463	0.469	0.473
	0.10	0.140	0.214	0.254	0.275	0.286	0.292	0.295	0.297	0.298	0.298

Major results

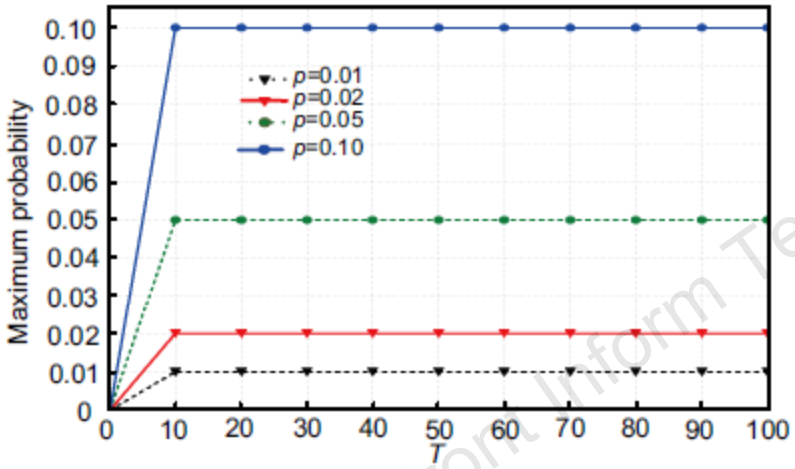

Fig. 11 Maximum probability that the message can be deciphered within T time units

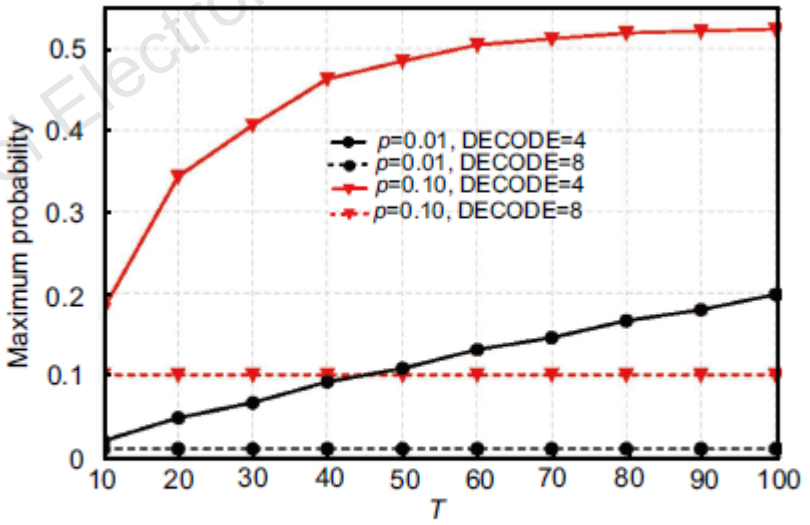

Fig. 12 Maximum probability that the recipient can decipher the message in DECODE time units

Major results

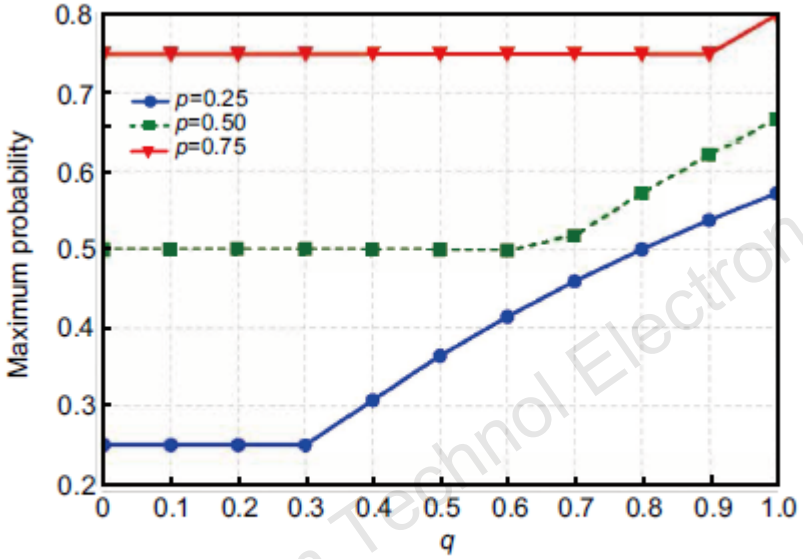

Fig. 13 Maximum probability that the recipient can decode the message as q varies

Table 5 Maximum probability for other certain cases

p	Maximum probability									
	q=0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
0.01	0.091	0.167	0.231	0.287	0.334	0.376	0.413	0.446	0.476	0.503
0.02	0.091	0.167	0.232	0.287	0.336	0.378	0.415	0.448	0.478	0.505
0.05	0.091	0.168	0.233	0.290	0.339	0.382	0.420	0.455	0.485	0.513
0.10	0.100	0.169	0.236	0.294	0.345	0.390	0.429	0.465	0.497	0.526
0.30	0.300	0.300	0.300	0.312	0.370	0.423	0.470	0.513	0.552	0.588
0.70	0.700	0.700	0.700	0.700	0.700	0.700	0.700	0.700	0.709	0.769

Major results

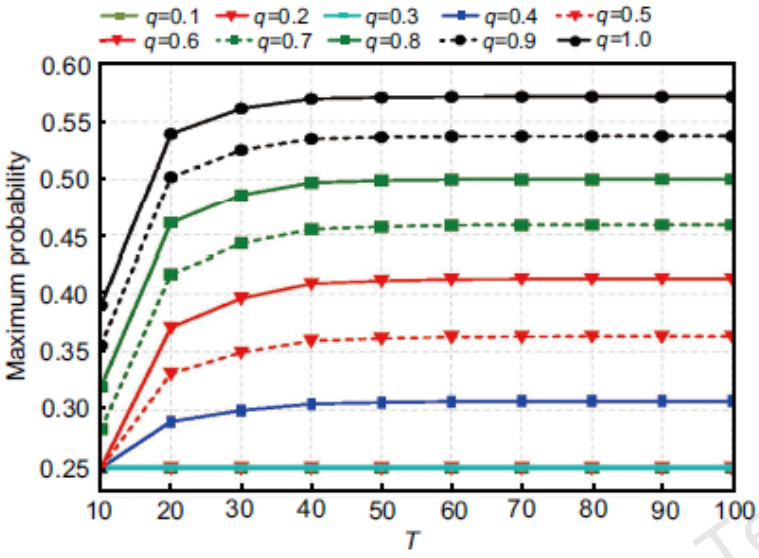

Fig. 14 Trends of the maximum probability where $T \in [10,\ 100]$

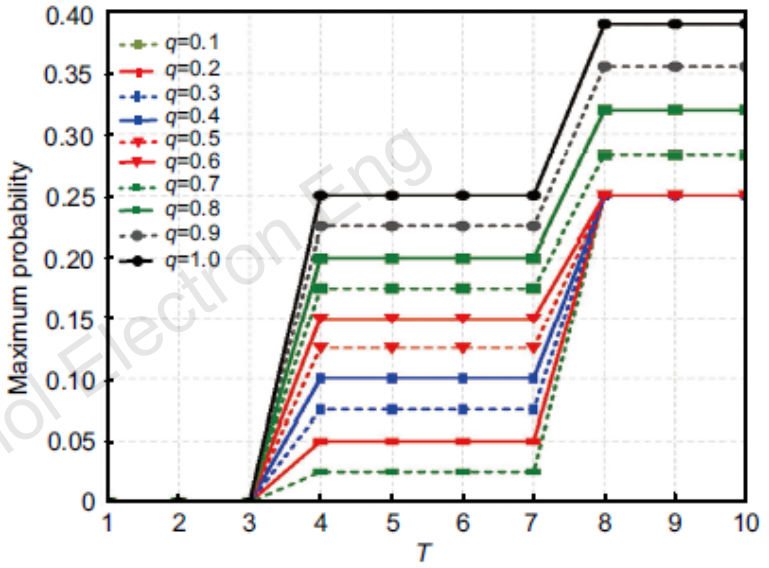

Fig. 15 Trends of the maximum probability where $T \in [1,\ 10]$

Table 6 Maximum termination probability for other cases of p

p	T	q=0.1	q=0.2	q=0.3	q=0.4	q=0.5	q=0.6	q=0.7	q=0.8	q=0.9	q=1.0
0.01	4	0.001	0.002	0.003	0.004	0.005	0.006	0.007	0.008	0.009	0.010
	7	0.001	0.002	0.003	0.004	0.005	0.006	0.007	0.008	0.009	0.010
	10	0.010	0.010	0.010	0.010	0.010	0.012	0.014	0.016	0.018	0.020
0.05	4	0.005	0.010	0.015	0.020	0.025	0.030	0.035	0.040	0.045	0.050
	7	0.005	0.010	0.015	0.020	0.025	0.030	0.035	0.040	0.045	0.050
	10	0.050	0.050	0.050	0.050	0.050	0.058	0.067	0.076	0.086	0.095
0.10	4	0.010	0.020	0.030	0.040	0.050	0.060	0.070	0.080	0.090	0.100
	7	0.010	0.020	0.030	0.040	0.050	0.060	0.070	0.080	0.090	0.100
	10	0.100	0.100	0.100	0.100	0.100	0.111	0.129	0.146	0.164	0.181

Conclusions

- This paper studied the fairness guarantee quantitatively through probabilistic model checking. E-fairness was measured by modeling the protocol in probabilistic timed automata and verifying the appropriate property specified in the probabilistic computation tree logic.
- The analysis proposed insights for choosing suitable values for different parameters associated with the protocol so that a certain degree of fairness can be obtained.

Xu GUO received his PhD degree from East China Normal University, Shanghai, China, in 2019. He is currently a lecture in the College of Electronics and Information, Shanghai Dianji University, Shanghai, China. His research interests include formal verification and software engineering.