Newcastle University

Distributed Interlocking

Formal distributed protocol development for reservation of railway subsections

Paulius Stankaitis, Alexei Iliasov, Tsutomu Kobayashi, Yamine Ait-Ameur, Alexander Romanovsky, Fuyuki, Ishikawa

Newcastle University, UK

National Institute of Informatics, Japan

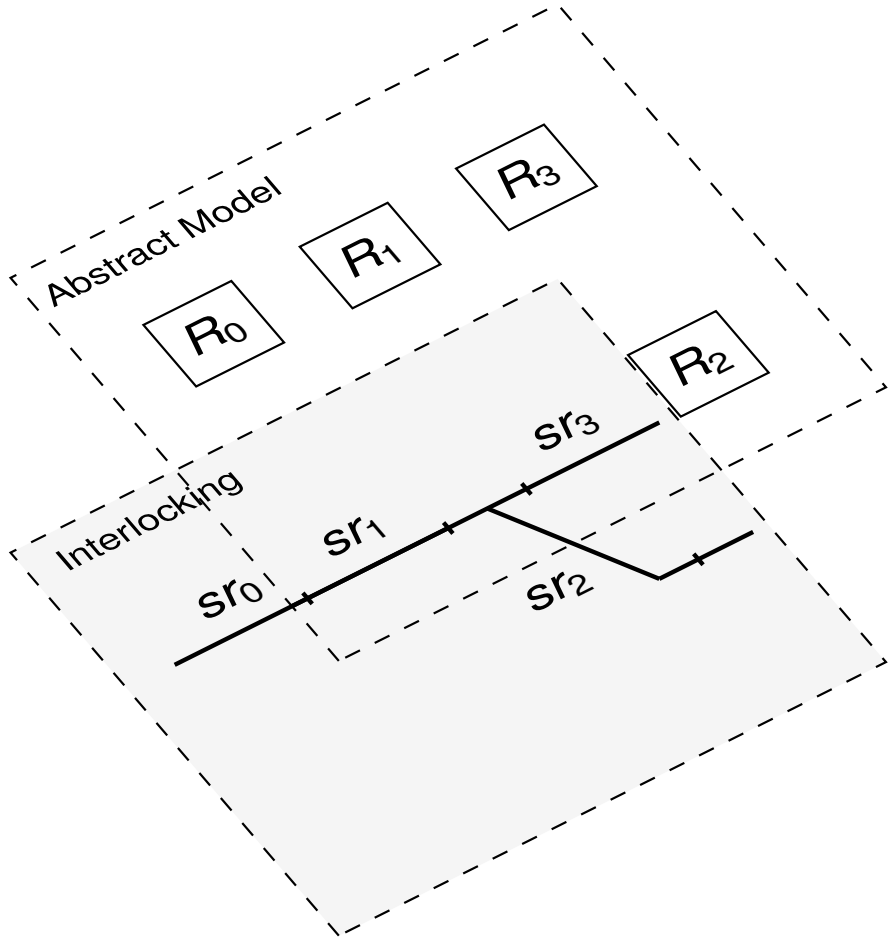
INPT–ENSEEIHT, France

School of Computing

June 17, 2019

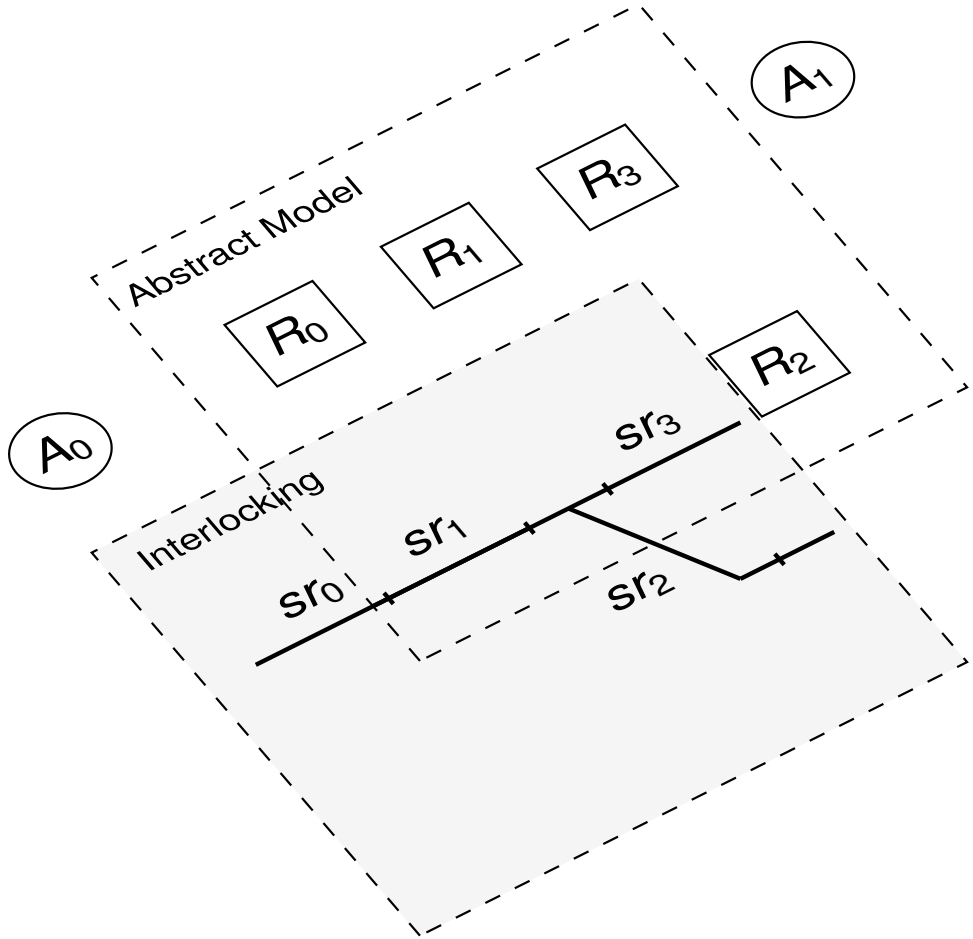
Newcastle University
School of Computing

Multifaceted Protocol Verification: Distributed Interlocking



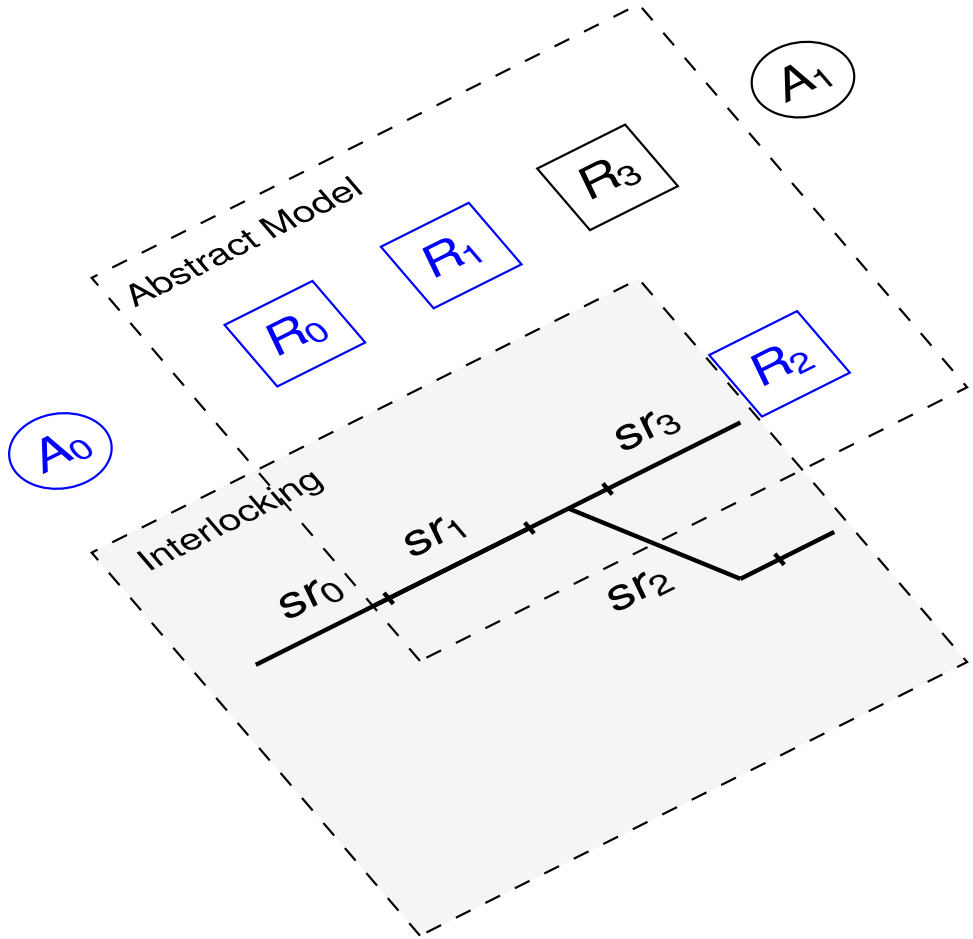
Newcastle University
School of Computing

Multifaceted Protocol Verification: Distributed Interlocking



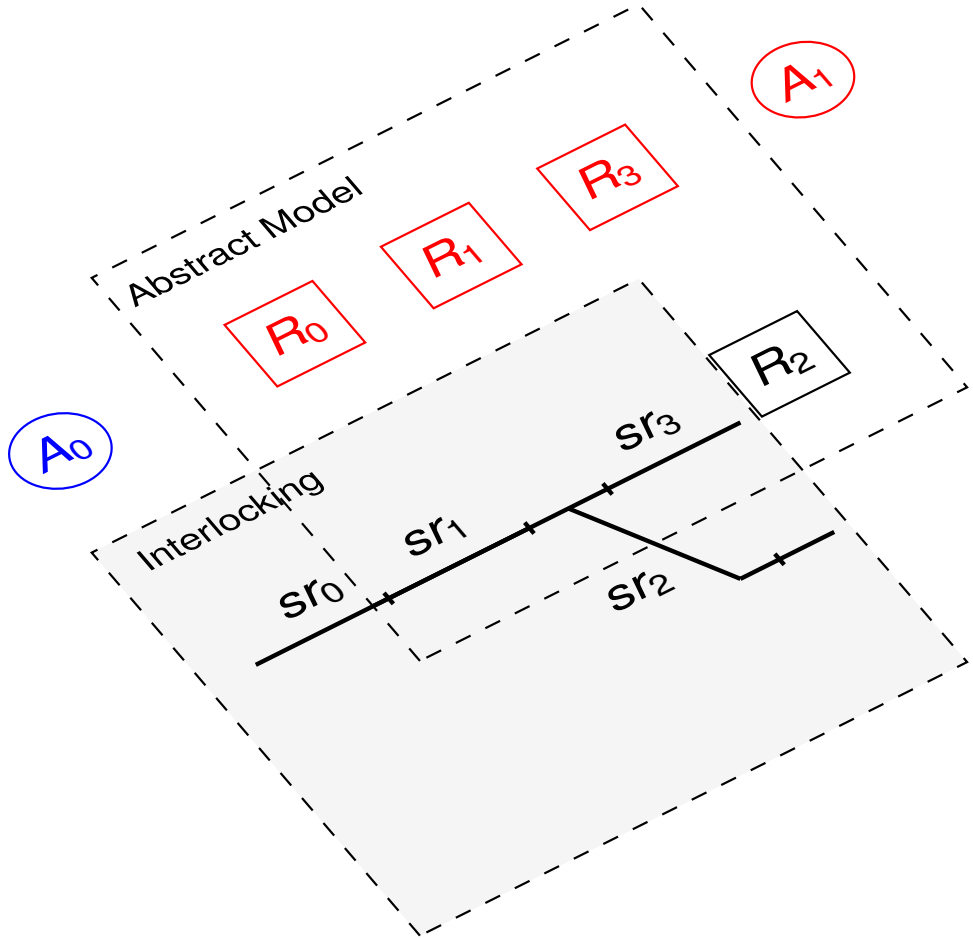
Newcastle University
School of Computing

Multifaceted Protocol Verification: Distributed Interlocking



Newcastle University
School of Computing

Multifaceted Protocol Verification: Distributed Interlocking



Newcastle University
School of Computing

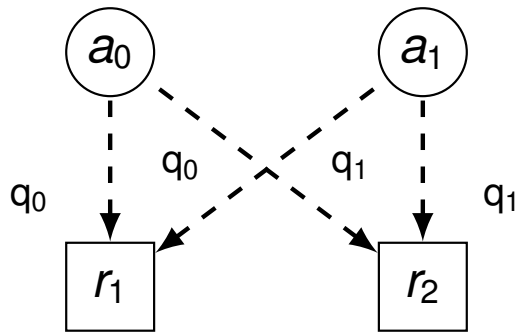
Distributed Interlocking Concept and Problems

SAF_1 | A resource will not be allocated to different agents at the same time.
SAF_2 | An agent will not be allocated a subset of its requested resources.
LIV_1 | An agent must be eventually allocated requested set of resources.
LIV_2 | Resource allocation must be guaranteed in the presence of message delays.

Figure: High-level systems safety and liveness requirements

Newcastle University
School of Computing

Distributed Resource Reservation - Problems

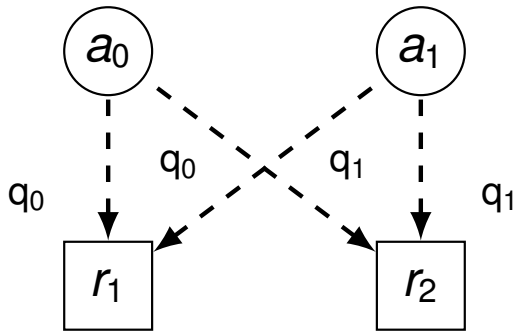


	r_1
0	
1	
2	
⋮	
n	

	r_2
0	
1	
2	
⋮	
n	

Newcastle University
School of Computing

Distributed Resource Reservation - Problems

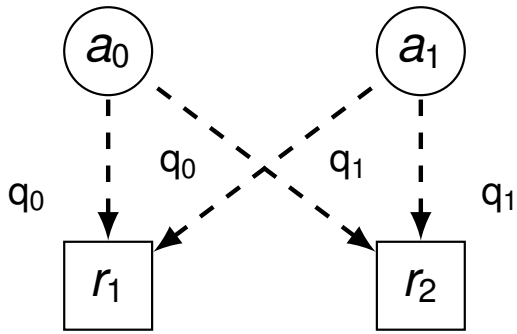


	r_1
0	a_0
1	
2	
⋮	
n	

	r_2
0	
1	
2	
⋮	
n	

Newcastle University
School of Computing

Distributed Resource Reservation - Problems

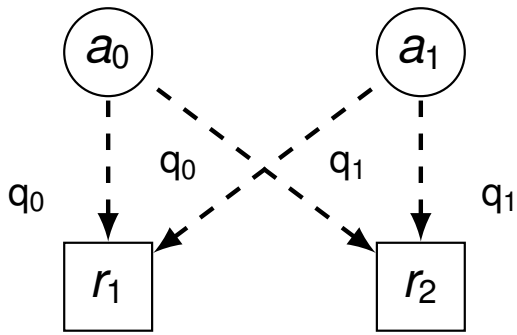


	r_1
0	a_0
1	
2	
⋮	
n	

	r_2
0	a_1
1	
2	
⋮	
n	

Newcastle University
School of Computing

Distributed Resource Reservation - Problems

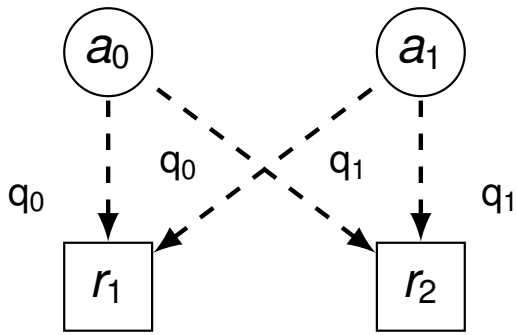


	r_1
0	a_0
1	a_1
2	
⋮	
n	

	r_2
0	a_1
1	
2	
⋮	
n	

Newcastle University
School of Computing

Distributed Resource Reservation - Problems

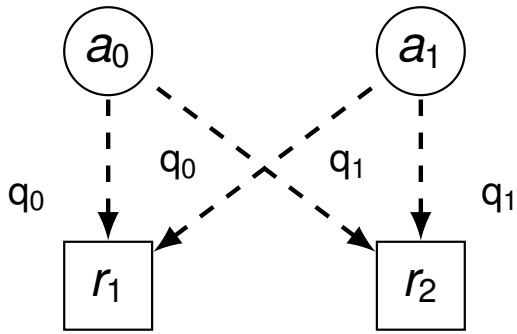


	r_1
0	a_0
1	a_1
2	
⋮	
n	

	r_2
0	a_1
1	a_0
2	
⋮	
n	

Newcastle University
School of Computing

Distributed Resource Reservation - Problems

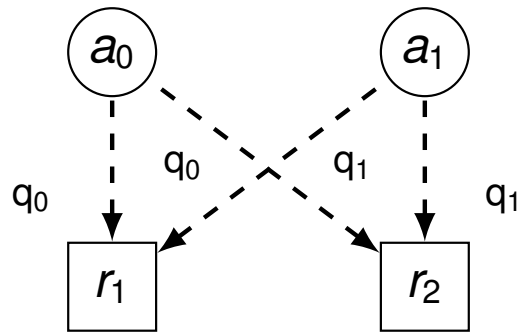


	r_1
0	a_0
1	a_1
2	
⋮	
n	

	r_2
0	a_1
1	a_0
2	
⋮	
n	

Newcastle University
School of Computing

Distributed Resource Reservation - Problems



	r_1
0	a_0*
1	a_1*
2	a_0
3	a_1
⋮	

	r_2
0	a_1*
1	a_0*
2	a_0
3	a_1
⋮	

Newcastle University
School of Computing

2-Stage Distributed Interlocking Protocol

	r_0	r_1	r_2	r_3	
dl_0	0	0	0	0	
	1	1	1	1	
dl_1	2	2	2	2	dl_2
dl_3	3	3	3	3	
	4	4	4	4	dl_4
	5	5	5	5	

Figure: Each dl_n only belongs to a single agent. Multiple distributed lanes can have the same index, but they cannot overlap (e.g. dl_1 and dl_2). Request pools are non compact structures.

Newcastle University
School of Computing

Formal Distributed Interlocking Protocol Modelling and Verification

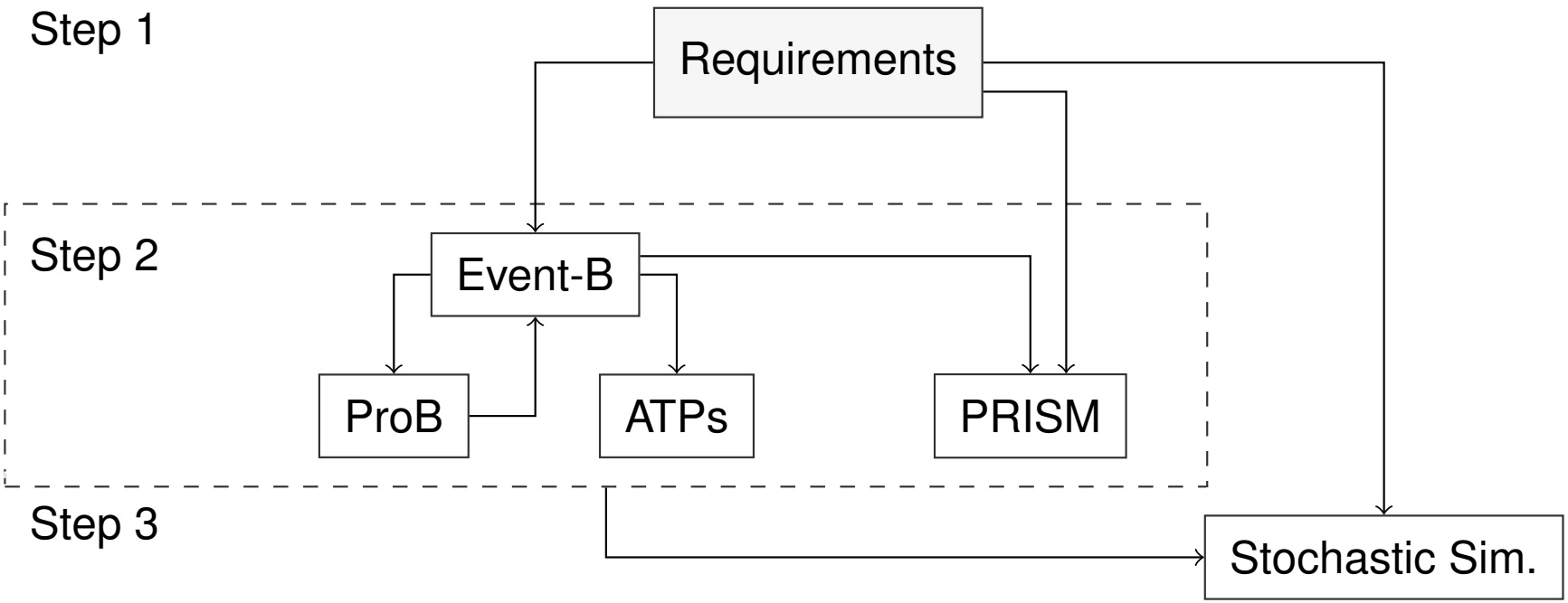


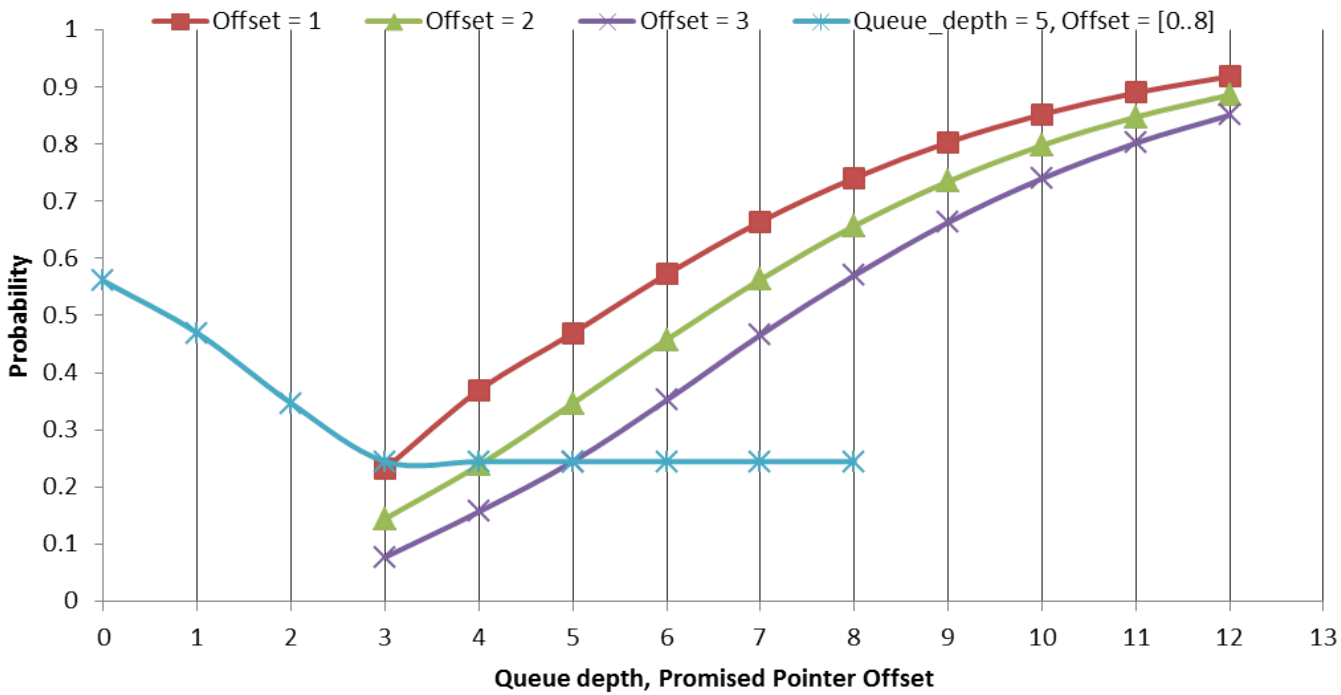
Figure: Multifaceted modelling and verification framework

Model	No. of POs	Aut. Discharged	Int. Discharged
context c_0	0	0	0
context mes.	9	9	0
machine m_0	12	12	0
machine m_1	23	21	2
machine m_2	59	43	16
machine m_3	43	32	11
machine m_4	103	57	46
Total	249	174	75

Table: Event-B protocol model proof statistics

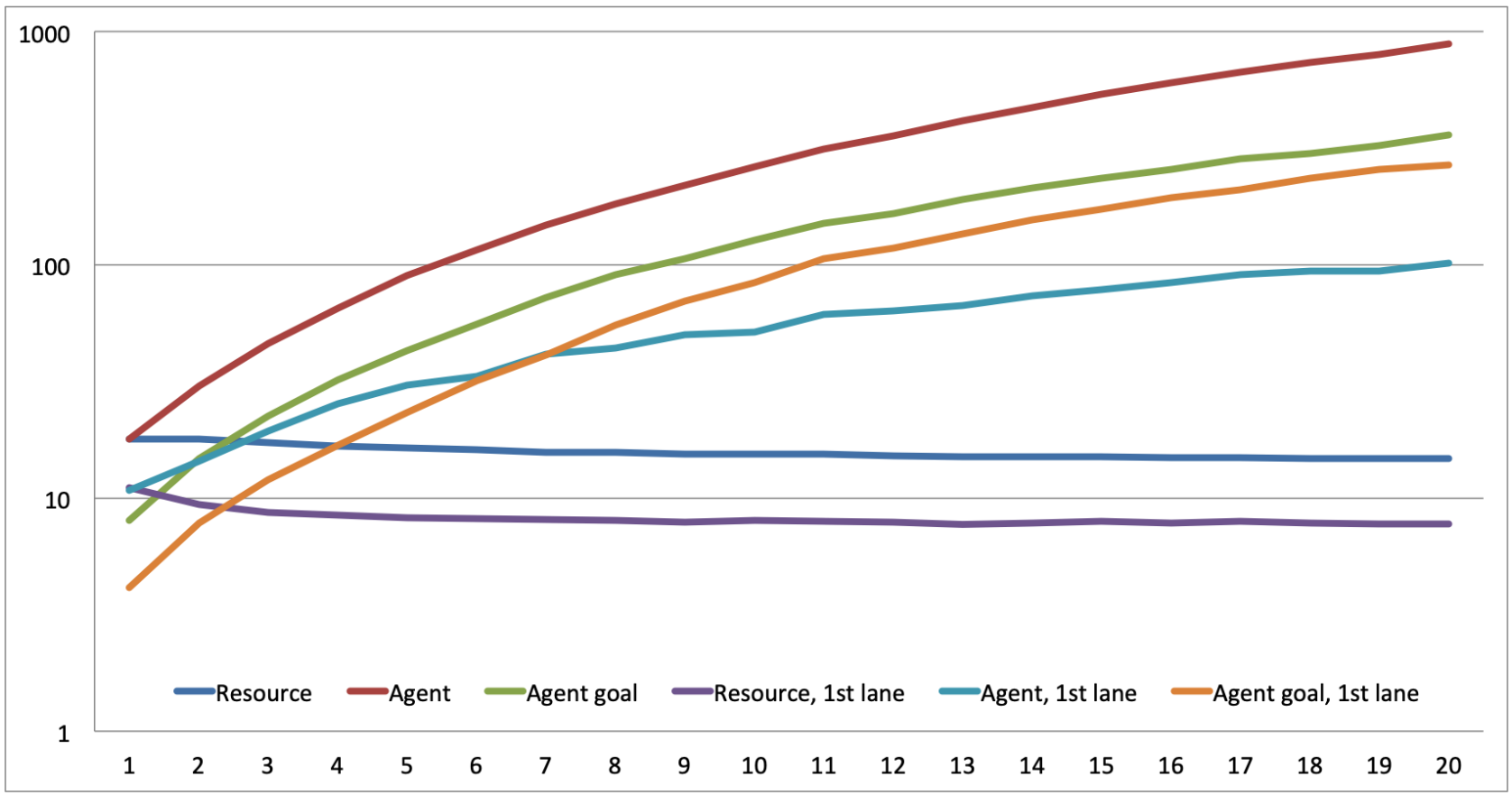
Newcastle University
School of Computing

Multifaceted Protocol Verification: Distributed Interlocking



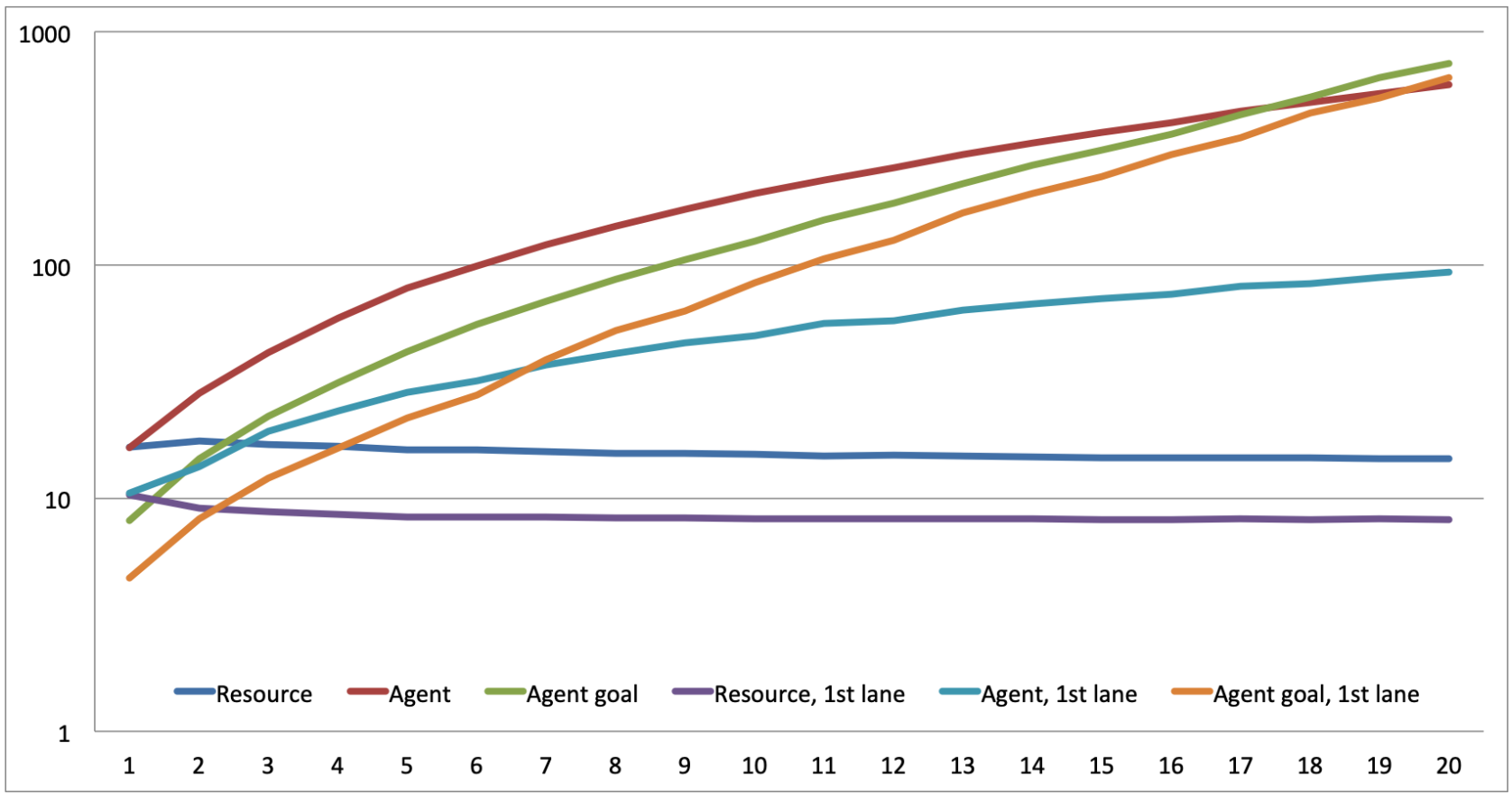
Newcastle University
School of Computing

Multifaceted Protocol Verification: Distributed Interlocking



Newcastle University
School of Computing

Multifaceted Protocol Verification: Distributed Interlocking



Newcastle University
School of Computing

Summary

- Formally developed using Event-B mod. language.
- Subtle deadlock scenarios were discovered with the ProB model checker.
- Correctness and deadlock freedom was proved by discharging proof obligations.
- Stage 1 was probabilistically simulated with PRISM model checker.
- Stage 1's performance was stochastically assessed.