Verification of an Air-Traffic Control System with Probabilistic Real-time Model-checking

Tran Thi Bich Hanh and Dang Van Hung

28.4.2008

Outline

- introduction
- abstract probabilistic timed model
- PRISM Model for ATC
- verification results
- conclusion

Introduction

- probabilistic real-time model-checking
  - real time systems
  - uncertain or probabilistic behaviour
- case study: Air-Traffic Control Systems (ATC)
  - operator's behaviours in ATC system
- probabilistic timed automata model
  - extended Operator Choice Model (OCM)
- probabilistic real time computation tree logic (PCTL)
- verification and analysis using the tool PRISM

Recapitulation – ATC

- task: to keep a safe separation distance and manage the flow of air traffic
- safety is a crucial issue
- human operators, human decision errors
- timing and probabilistic properties

Operator Choice Model

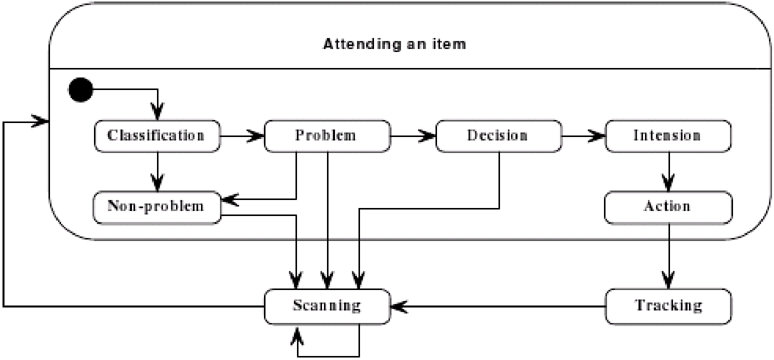


Figure 1: The Operator Choice Model

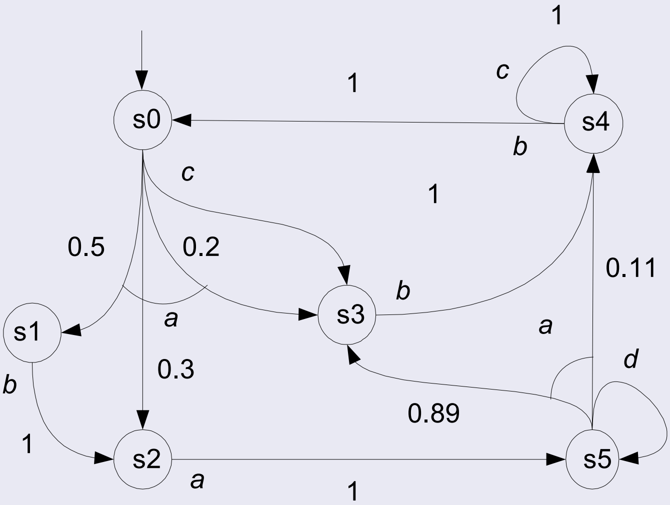
Modelling and Verification Problem

- OCM provides a framework for describing the opertor's behaviour in ATC
- real ATC time and probability aspect:
  - how much time it takes for the operator to solve the problem
  - probabilistic choice made at every state
- time and probability is authors' guess
- precise data should be obtained using realistic statistic data from experts

Abstract Probabilistic Timed Model

Markov Decision Process - MDP

- a formalism combining nondeterminism and probability



Abstract Probabilistic Timed Model

Markov Decision Process - MDP

- a tuple $(S, s_0, L, Steps)$
  - S is a finite set of states
  - $s_0 \in S$ is an initial state
  - $L : S \longrightarrow 2^{AP}$ is a function assigning to each state a set of atomic propositions which are true in that state
  - $Steps : S \longrightarrow 2^{Dist(S)}$ is a function assigning to each state $s \in S$ a finite, non-empty set of discrete probability distributions on S

- a path
- probability of a finite path
- an adversary (policy, scheduler)

Abstract Probabilistic Timed Model

Clocks, clock valuations, zones

- C a finite set of clocks taking values from the time domain R – non-negative reals
- a clock valuation $v : C \to R$
- a zone is a conjunction of atomic constraints of the form $x = c$, $x \leq c$ or $x \geq c$, where $x \in C$ and $c \in N$
- a clock valuation v satisfies the zone ζ: $v \models \zeta$
- Z_C the set of all zones over C

Abstract Probabilistic Timed Model

Probabilistic Timed Automata

- a tuple $A = (S, s_0, C, \Sigma, inv, prob)$
  - S is a finite set of states
  - $s_0 \in S$ is an initial state of A
  - C is a finite set of clocks
  - Σ is a finite set of events
  - $inv : S \rightarrow Z_C$ is a function mapping each state to an invariant condition
  - $prob \subseteq S \times Z_C \times \Sigma \times Dist(S \times 2^C)$ is the probabilistic edge relations

Abstract Probabilistic Timed Model

Semantics

- an infinite-state MDP, states are pairs (s, v), s state and v is a clock valuation satisfying $inv(s)$
- initial state (s, Θ), $\Theta(x) = 0 \ \forall x \in C$
- two types of transitions:
  - state change due to elapse of time, $inv(s)$ still satisfied
  - $(s, \zeta, \sigma, p) \in prob$ discrete transition from s, which is enabled by the zone ζ to the state s' on event σ with the probability $p(s', \lambda)$, where λ is the set of resetting clocks

Probabilistic Timed Automata

- parallel composition of two probabilistic timed automata

Probabilistic real time Computation Tree Logic (PCTL)

- $\varphi ::= a|\neg\varphi|\varphi \wedge \varphi|P_{\bowtie\lambda}[\psi]$
- $\psi ::= X\varphi|\varphi U_{\leq t}\varphi|\varphi W_{\leq t}\varphi$

where φ is a state formula, ψ is a path formula,
$\bowtie \in \{<, >, \leq, geq\}$, $\lambda \in [0, 1]$ and $t \in N$

Modelling ideas

- array of N Boolean variables to record the real state of N pairs of aircraft
- is/is not in conflict
- operator has to spend some time to complete each activity (state in a system)
- probability the operator makes right choice is high (0.99)
- variables expressing time and probability

Variable	Description	Value
N	number of pairs in the system	1,2,3 or 6
ts	duration of scanning	0.1 s
p_cpk_low	probability to misclassify a non-conflict to a problem or vice-versa	0.01
...	...	...

The model

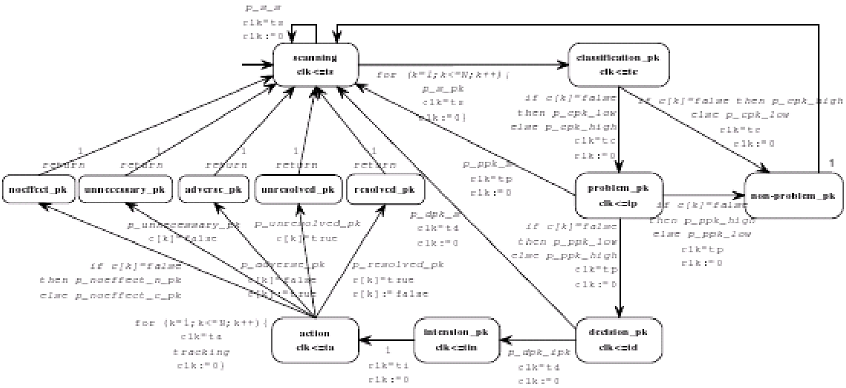


Figure 2: OCM Probabilistic timed automaton

PRISM model

- MDP
- PRISM modelling language, state-based language
- a model is a parallel composition of a number of modules which can interact with each other
- PCTL
- PRISM property specification language
- automated verification

Experimental Results

Conflict free

with probability 1, eventually there have been no conflict in the system

$$P_{\geq 1}[\mathit{true}\ U\ \mathit{resolved\_all}]$$

where $\mathit{resolved\_all} := \bigwedge_{i=1}^{N}(c_i = \mathit{false})$
true, but unbounded

Experimental Results

Deadline effect

is the probability for the system to have no conflict within tim T greater than λ ?

$$P_{\geq\lambda}[\mathit{true}\ U_{\leq T}\ \mathit{resolved\_all}]$$

where $\mathit{resolved\_all} := \bigwedge_{i=1}^{N}(c_i = \mathit{false})$
analysis depending on different scenarios

Experimental Results

Work load effect

1 conflict, varying the number N of pairs of aircraft: 1,3,6

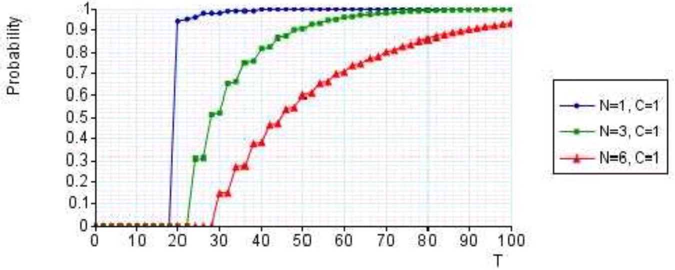


Figure 5: Probability of resolving all conflicts - Varying number of non-conflicts

Experimental Results

Work load effect

3 pairs, varying the number C of conflicts: 1,2,3

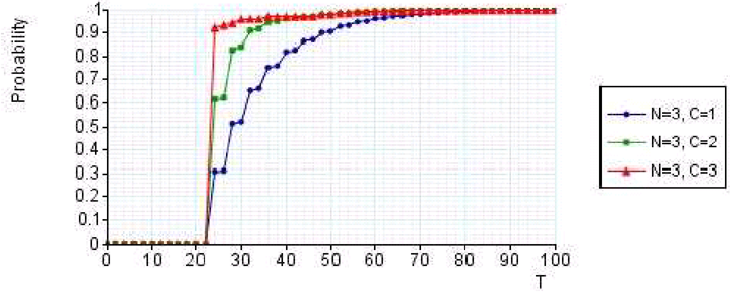


Figure 6: Probability of resolving all conflicts - Varying number of conflicts

Experimental Results

Misclassification

probabilities for the operator to have misclassification within an interval $[0, T]$

3 pairs, varying the number C of conflicts: 1,2,3

$$missclass\_conflict\_pk := (ck = true) U_{\leq T} non\_problem\_pk$$

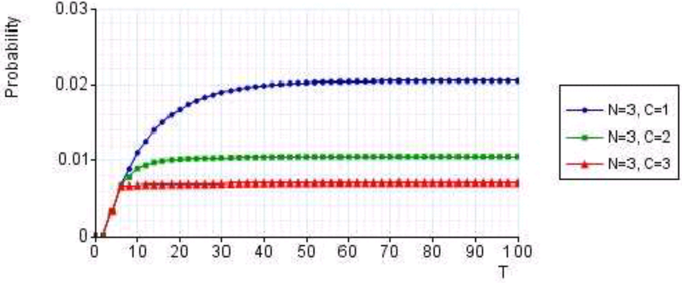


Figure 7: Probability of misclassifying a conflict pair as a non-problem

Experimental Results

Misclassification

$$missclass\_nonconflict\_pk := (ck = false) U_{\leq T} problem\_p_k$$

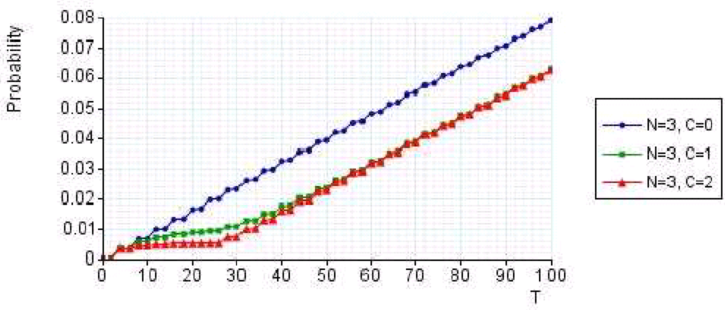


Figure 8: Probability of misclassifying a non-conflict pair as a problem

Experimental Results

Scanning effect

effect of operator's attention to conflict on the performance of the system

2 disjunct pairs, varying the number C of conflicts: 1,2

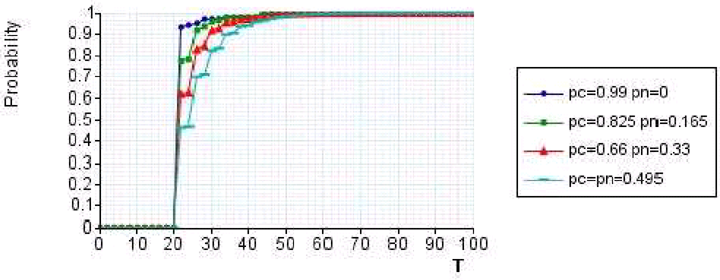


Figure 9: Probability of resolving all conflicts - 1 conflict and 1 non-conflict

Experimental Results

Scanning effect

effect of operator's attention to conflict on the performance of the system

2 disjunct pairs, varying the number C of conflicts: 1,2

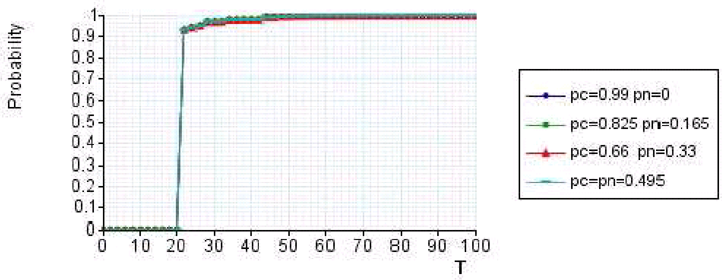


Figure 10: Probability of resolving all conflicts - 2 conflicts

Experimental Results

Task failure

probabilities of an operator's task failure within time T:

- The operator can not resolve all conflicts within time T
- Some operator's action produces adverse situations within time T
- The operator does not pay attention to a certain conflict within time T
- The operator does not have intention to response to a certain conflict within time T

expected time units R within which the operator causes the task failure probabilities more non-conflicts: the operator has to spend more time to make the right decision, but the probability for task failure increases.

Experimental Results

Task failure

N	1	3	6
$R_{adverse}$	501,952.54	500,644.38	498,648.07
$R_{resolved\_all}$	20.50	33.71	54.48
$P_{non\_resolved_T} = 1 - P_{resolved\_all_T}$	0.059	0.324	0.345
R_{scan_p1}	2.02	10.10	22.23
$P_{non\_scan\_p1_T} = 1 - P_{scan\_p1_T}$	0.01	0.304	0.342
$R_{response\_p1}$	11.29	39.95	116.75
$P_{non\_response\_p1_T} = 1 - P_{response\_p1_T}$	0.05	0.052	0.01

Table 1: Expected time and Probability of task failures

Conclusion

- ATC as a case study for safety verification with PRISM
- probabilistic timed automata: simple, close to the real-world
- probabilities artificial, but the verification results still useful

Future work

- extend model, capturing the realistic behaviour of aircraft