

Statistical Model-Checking of “Black-Box” Systems

VESTA

Koushik Sen

University of Illinois at
Urbana-Champaign, USA

Joint work with **Gul Agha** and **Mahesh
Viswanathan**



Motivation

- Network protocols
 - Delays in communication
 - Failures in communication
 - Malicious participants
- Large and Geographically Distributed Systems
 - Interact with unpredictable and hostile environment
 - Failure of a component

Probabilistic in Nature



Probabilistic Model

- Stochastic Modeling
 - Associate probability with different uncertainties
 - Probability distribution for time (delay)
 - Probabilities for failures
 - Formal Probabilistic Models
 - Discrete-Time Markov Chains (DTMC)
 - Continuous-Time Markov Chains (CTMC)
 - Markov Decision Processes (MDP)
 - Generalized Semi-Markov Processes (GSMP)
 - Probabilistic Rewrite Theories (PRwTh)

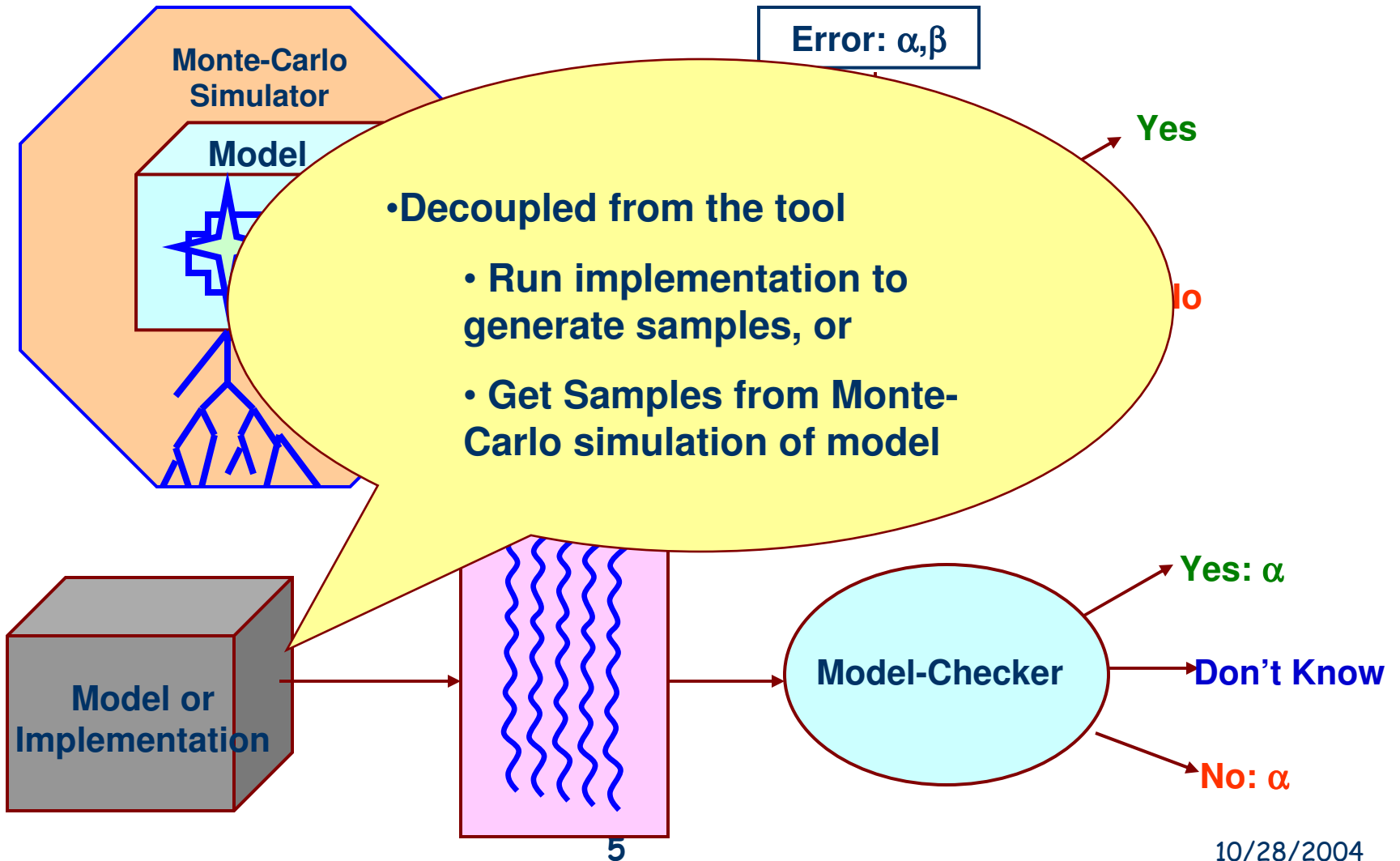


Probabilistic Analysis

- Specify performance and reliability properties in some probabilistic logic
 - Probabilistic Computation Tree Logic (PCTL)
 - Continuous Stochastic Logic (CSL)
- Model-Check against the property
 - Numerical (PRISM, ETMCC)
 - Accurate, Computationally intensive
 - Statistical (ProVer, SMART, **VESTA**)
 - Approximate, Scalable



Statistical Approaches



Continuous Stochastic Logic

- $P_{<0.5}(\diamond^{<10} \text{ full})$
 - Probability that queue becomes full in 10 units of time is less than 0.5
- $P_{>0.98}(\neg \text{ retransmit } U^{<200} \text{ receive})$
 - Probability that a message is received successfully within 200 time units without any need for retransmission is greater than 0.98



Model-Checking Idea

- To verify a formula $P_{\leq p}\psi$ set up two **statistical hypothesis tests**
 - Test 1:
 - $H_0 : (\# \text{ of true})/(\# \text{ of samples}) \leq p - \delta_1$ [say "YES" and calculate p-value]
 - $H_1 : (\# \text{ of true})/(\# \text{ of samples}) > p - \delta_1$
 - Test 2:
 - $H_0 : (\# \text{ of true})/(\# \text{ of samples}) \geq p + \delta_2$ [say "NO" and calculate p-value]
 - $H_1 : (\# \text{ of true})/(\# \text{ of samples}) < p + \delta_2$
- If $p - \delta_1 < (\# \text{ of true})/(\# \text{ of samples}) < p + \delta_2$
 - [say "I don't know"]



On Nested Formulas

- Evaluate Satisfaction of nested Probabilistic formulas

- Yes
- No
- I don't know

Resolve in adversarial fashion

- "Yes" when verifying a formula of the form $P_{\leq p}\Psi$
- "No" when verifying a formula of the form $P_{\geq p}\Psi$



Evaluation

- Tandem Queuing Network
- Cyclic Polling System
- Grid World Example
 - Answers matched the numerical model-checker
 - P-value (α) of the order 10^{-8}
 - Very high confidence in our result
 - 4-times faster than ProVer and PRISM
- Disadvantage: Space requirement is high
 - Required to store all samples before model-checking



Discussion

- Verify probabilistic properties of various network protocols
 - Earlier intractable due to large state space
- Integrate with PMaude
 - Use PMaude to model and simulate systems
- Use Machine learning to make the technique more practical
- Use Machine Learning to verify Liveness properties

