

# Probabilistic Analysis of DoS-Resistant Network Protocols

Gul Agha, Michael Greenwald, Carl Gunter, Sanjeev Khanna, Nirman Kumar, Jose Meseguer, Koushik Sen, **Prasanna Thati**

University of Illinois at Urbana Champaign  
and  
University of Pennsylvania



# Security Models for DoS Analysis

- Unlimited capability of adversary (traditional appr)
  - Can delete, modify, and insert packets
  - Can verify safety properties, but not liveness properties
- Limit the capability of adversary
  - Adversary can only insert packets (not allowed to modify)
  - Limit bandwidth: Probability distribution for sending rates
  - Can now analyze DoS attacks
- Counter-Measures:
  - Sample packets with certain probability at receiver



# Analyzing DoS Attacks

- Formally model communication protocol
  - Probabilistic extension of rewrite theories
    - Executable -> Can generate samples through simulation
- Express performance and reliability properties in CSL
  - Liveness (packet will reach within certain time with high probability)
- Statistically verify properties
  - Use samples from simulation



# Probabilistic Models

- Associate probability with different uncertainties
  - Probability distribution for sender's bandwidth
  - Probabilities for communication failures
  - Sampling probability at the receivers
- 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



# Probabilistic Rewrite Theories (PRwTh)

- An extension of rewriting logic for modeling probabilistic systems
- Rules of the form:
  - $l : t(X) \rightarrow t'(X,Y)$  if  $C(X)$  with  $\pi(X)$
- Semantics (roughly):
  1. Non-deterministically choose a rule to apply
  2. Probabilistically choose substitution for new variables ( $Y$ ) according to the distribution  $\pi(X)$
- General semantic framework that subsumes several other stochastic models



# Example

sort Clock .

op clock : Nat PosReal  $\rightarrow$  Clock .

op broken : Nat PosReal  $\rightarrow$  Clock .

tick : clock(N,R)  $\Rightarrow$  if B then clock(s N, R - R/1000 )

else broken(N,R - R/1000 ) fi

with probability  $\pi_{\text{tick}}(R)$  .

tick-broken: broken(N,R)  $\Rightarrow$  broken(N,R-R/1000 )

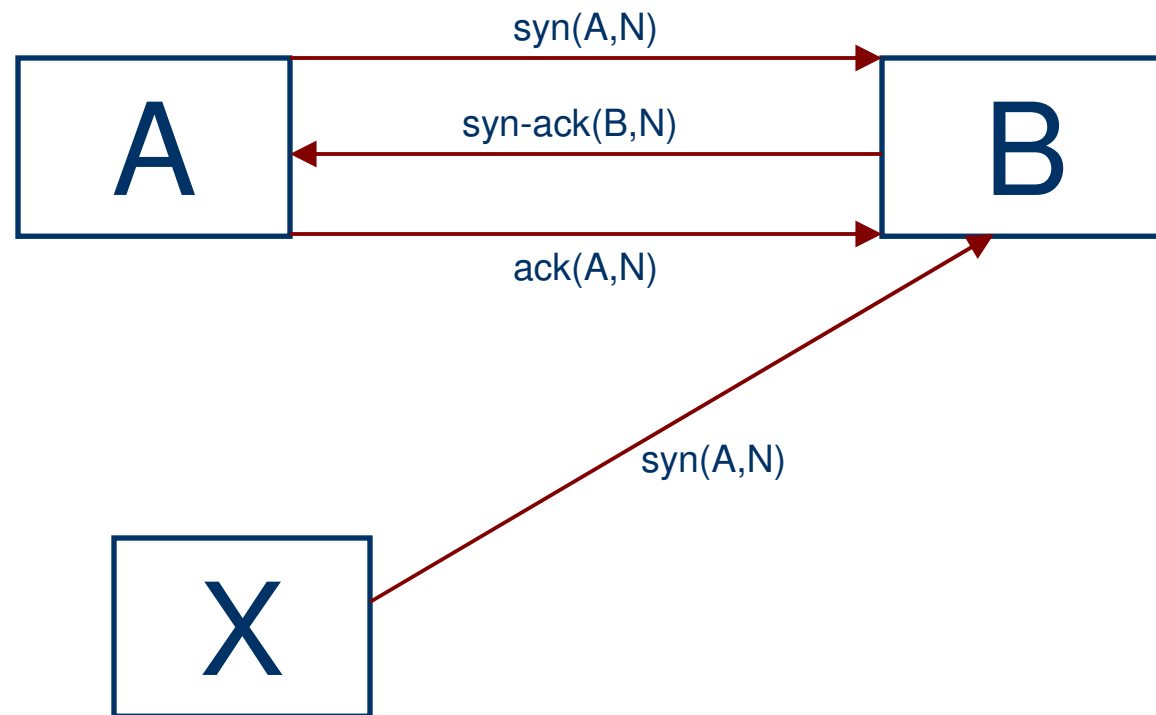
with probability 1 .

reset : clock(s N,R)  $\Rightarrow$  clock(0,R) with probability 1 .



# Case Study: TCP/IP synchronization

- Model synchronization phase of TCP/IP protocol



# Prob. Model for Dos-Resistant TCP/IP

- Sampling probability at recipient
- Probability distribution for sending rates
- Probability distribution of communication delays
- Probability distribution for communication failures



# Example rules

- Rewrite rule that limits the attacker's bandwidth

```
cr1 < X | cnt: N > => [ < X | cnt: s(N) > < toB | cntnt: SYN(X,N) > , D ]  
      if D:= sampleExpWithMean(20.0)
```



# Rule for sampling

- Rewrite rule for sampling packets at the receiver

cr1 < B | synlist: L1 > < toB | cntnt: SYN(I , N) >

=>

[ < B | synlist: if U then insert(L1 , < I , N >) else L1 fi >

if U then < to(I) | cntnt: SYNACK(B , N) > fi , D ]

if

U := sampleBerWithP(0.25) ∧

D := sampleExpWithMean(40) .



# PMaude (Probabilistic Maude)

- Implemented as an extension of Maude 2.0
  - Can specify probabilistic systems and perform Monte-Carlo simulation
  - Traces obtained through simulation can be used for formal statistical analysis (**VESTA**).
- [CAV'04] [QEST'04]



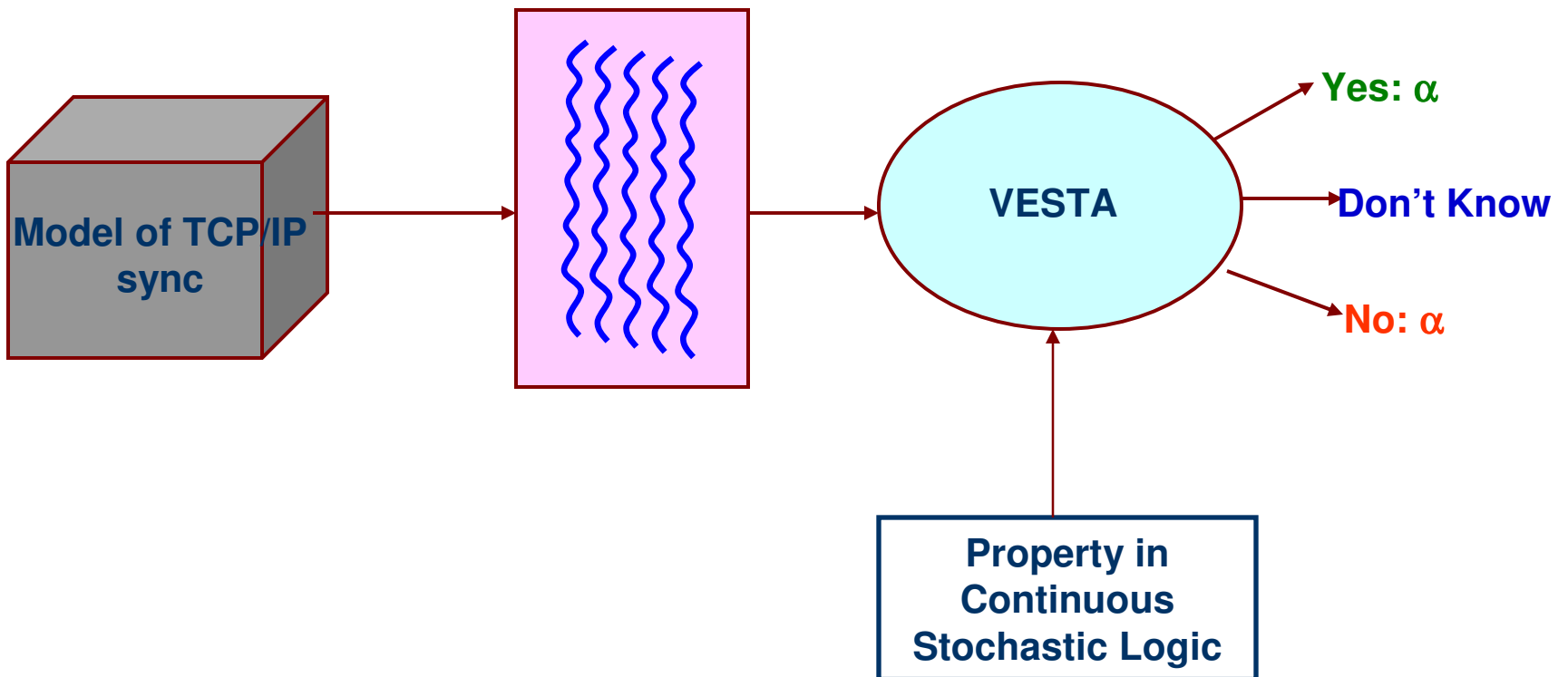
# Properties in Continuous Stochastic Logic

Time bounded or unbounded probabilistic properties

- $P_{> 0.99}(\diamond^{<100} \text{ synchronized})$ 
  - Probability that synchronization succeeds in 100 units of time is greater than 0.99
- $P_{< 0.01}(\diamond \text{ buffer\_size} \geq \text{MAX\_SIZE})$ 
  - Probability that the buffer at the receiver eventually becomes full is less than 0.01



# Statistical Verification



# Verification 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  $P_{\geq p}\Psi$



# Conclusion

- Probabilistic rewrite theories is a high-level specification language to model probabilistic protocols
- Samples obtained from Monte-Carlo simulation can be used for statistical verification
- Verify correctness of DoS resistant version of network protocols formally



# Motivation

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

Probabilistic in Nature



# Operational Semantics of PRwTh

- Rules of the form:
  - $l : t(X) \rightarrow t'(X,Y)$  if  $C(X)$  with  $\pi(X)$
- Steps in probabilistic rewriting:
  1. Non-deterministically choose a rule to apply
  2. Probabilistically choose substitution for new variables ( $Y$ ) according to the distribution  $\pi(X)$



# Salient Features of PRwThs

- Expressive power
  - PNS, DTMC
  - GSMP, CTMC
  - Object Based distributed systems
- General Semantic framework
  - Interoperation of tools!



# Future Work

- Specify other DoS resistant network protocols in details in PMaude and analyze them

