UNIVERSITÉ Concordia UNIVERSITY

Concordia University Hardware Verification Group

Formalization of Normal Random Variables

M. Qasim, O. Hasan, M. Elleuch, S. Tahar

Hardware Verification Group

ECE Department, Concordia University, Montreal, Canada

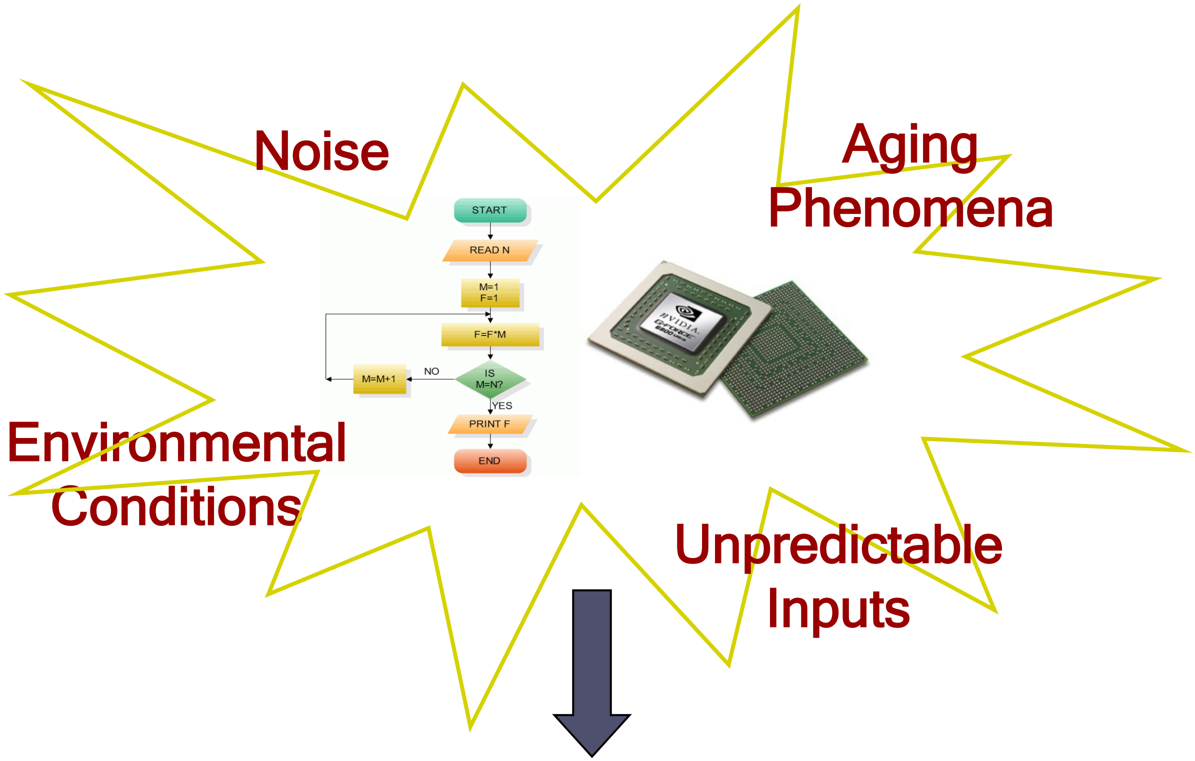
CICM 16

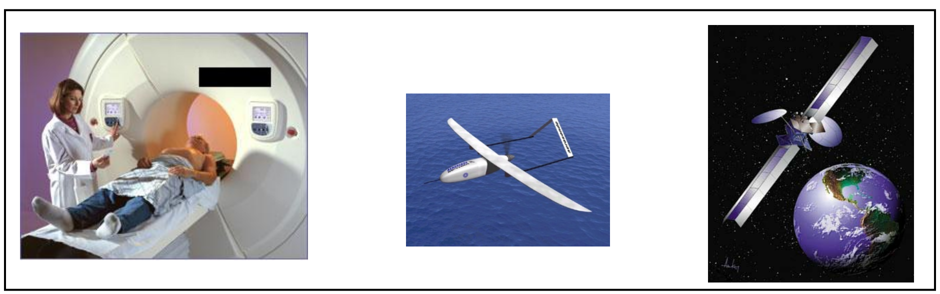
July 28, 2016

Outline

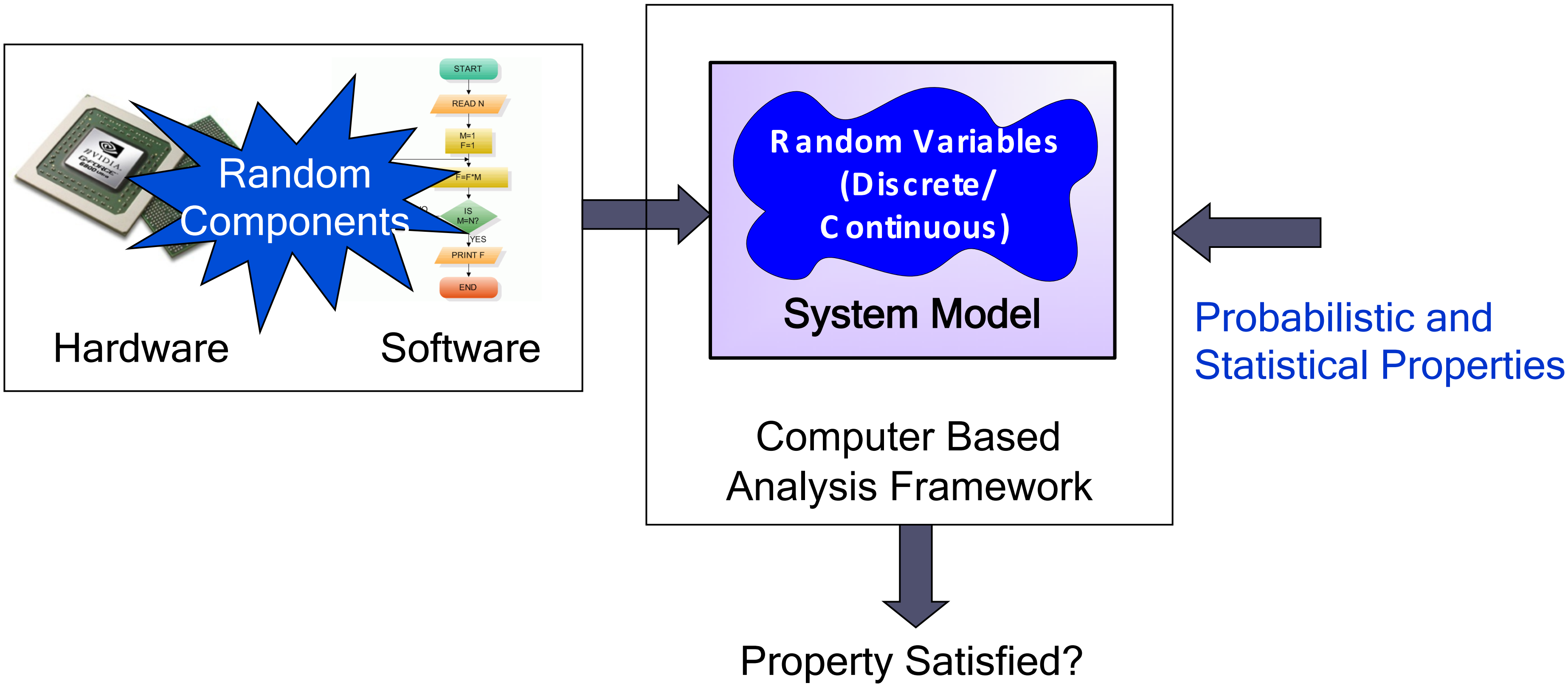
- Introduction and Motivation
- Formalization
- Case Study: Clock Synchronization in WSNs
- Conclusions

Motivation


Noise
Aging Phenomena
Environmental Conditions
Unpredictable Inputs
START
READ N
M=1
F=1
F=F*M
IS M=N?
NO
M=M+1
YES
PRINT F
END



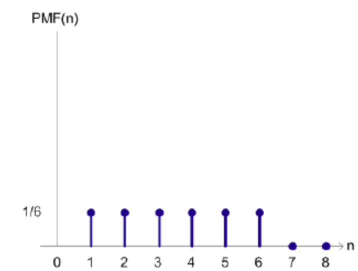
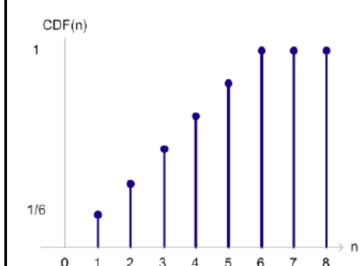
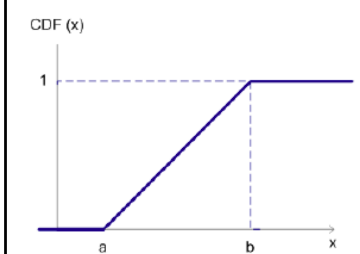
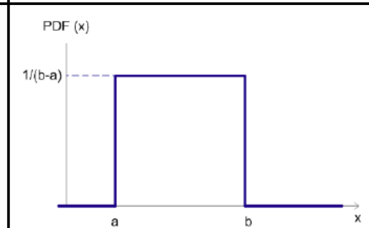
Probabilistic Analysis



Probabilistic Analysis Basics – Random Variables

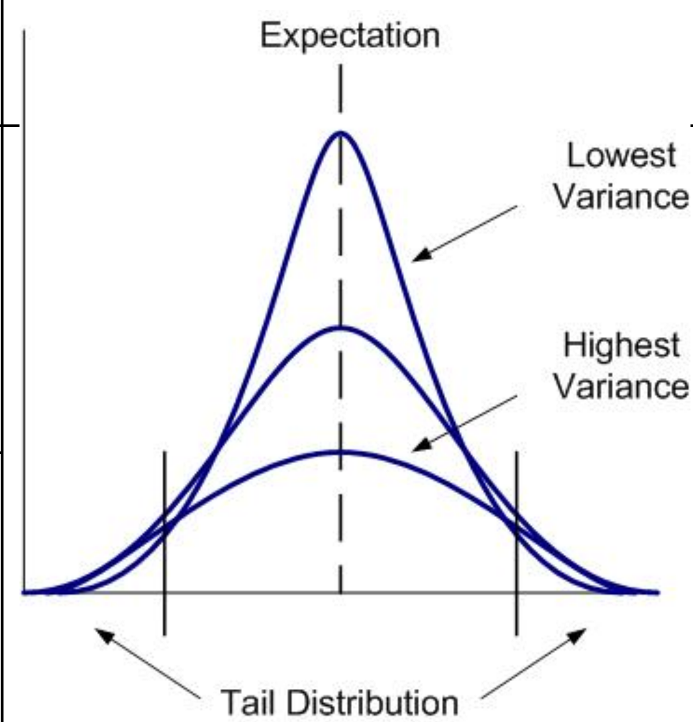
- Discrete Random Variables
  - Attain a countable number of values
  - Example
    - Dice[1, 6]
- Continuous Random Variables
  - Attain an uncountable number of values
  - Examples
    - Uniform (all real numbers in an interval [a,b])

Probabilistic Analysis Basics – Probabilistic Properties

Property	Description	Examples	
		Discrete	Continuous
Probability Mass Function (PMF)	Probability that the random variable is equal to some number *n*		
Cumulative Distribution Function (CDF)	Probability that the random variable is less than or equal to some number *n*		
Probability Density Function (PDF)	Slope of CDF for continuous random variables		

Probabilistic Analysis Basics – Statistical Properties

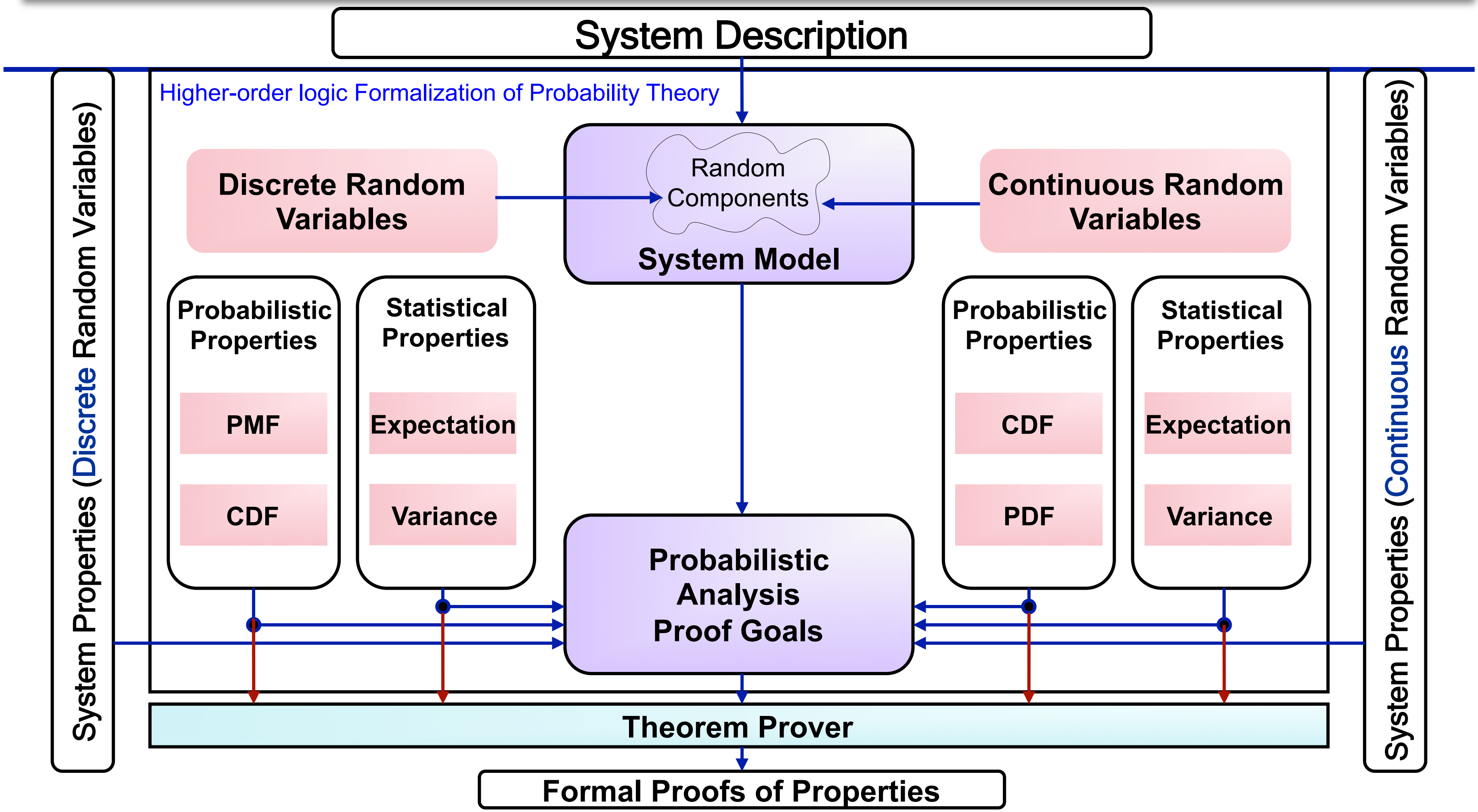
Property	Description	Illustration
Expectation	Long-run average value of a random variable	
Variance	Measure of dispersion of a random variable	



Probabilistic Analysis Approaches

	Simulation	Formal Methods	
		Model Checking	Theorem Proving
Random Components	Approximate random variable functions	Probabilistic State Machine	Random variable functions
Analysis	Observing some test cases	Exhaustive Verification	Mathematical Reasoning
Accuracy	✘	✓	✓
Expressiveness	✓	✘	✓
Automation	✓	✓	✘
Maturity	✓	✘	✘

Probabilistic Analysis using Theorem Proving



- [Hurd, 2002]: Probability Theory, Discrete Random Variables (RVs), PMF
- [Hasan, 2007]: Statistical Properties for Discrete RVs, CDF, Continuous RVs
- [Mhamdi, 2011] Probability (Arbitrary space) Lebesgue Integration, Multiple Continuous RVs Statistical Properties
- [Hölzl, 2012] Isabelle/HOL: Probability, Measure and Lebesgue Integration, Markov, Central Limit Theorem

Paper Contributions

- Formalization of Probability Density Function (PDF)
- Formalization of Normal Random Variable
  - Enormous Applications
  - Sample mean of most distributions can be treated as Normally Distributed
- Case Study: Clock Synchronization in WSNs

Probability Density Function

- PDF p(x) of a random variable x is used to define its distribution

$$P(x_1 < x < x_2) = \int_{x_1}^{x_2} p(x)\, dx$$

- The PDF of a random variable is formally defined as the Radon-Nikodym (RN) derivative of the probability measure with respect to the Lebesgue-Borel measure
  - RN derivative and probability measure was available in HOL4
  - Lebesgue-Borel measure
    - Ported from Isabelle/HOL [Hölzl, 2012]
    - Some theorems and tactics (e.g. SET_TAC) also ported from the Lebesgue measure theory of HOL-Light [Harrison, 2013]

Probability Density Function

- The PDF of a random variable is formally defined as the Radon-Nikodym (RN) derivative of the probability measure with respect to the Lebesgue-Borel measure

Definition: Probability Density Function

```
⊢ PDF X p = RN_deriv lborel
  (space borel, subsets borel, measurable_distr p X)
```

Normal Random Variable

- Normal PDF

$$N(\mu, \sigma) = \frac{1}{\sigma\sqrt{2\pi}} \exp^{(-\frac{(x-\mu)^2}{2\sigma^2})}$$

where μ represents its mean and σ is the standard deviation

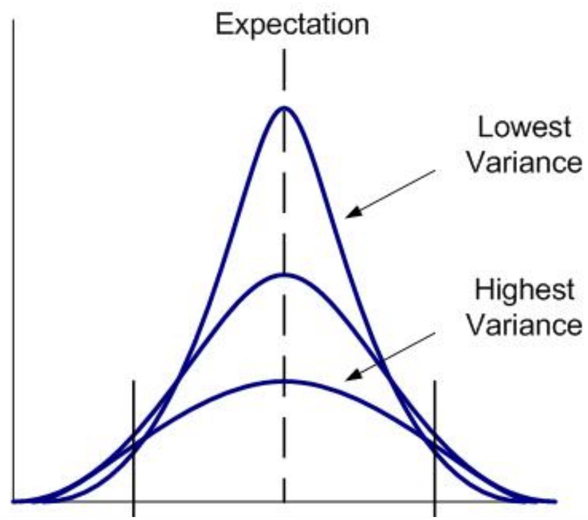
Definition: Normal Random Variable

$\vdash$ normal_rv X p μ σ =
  random_variable X p borel $\wedge$ (measurable_distr p X = normal_pmeasure μ σ)

- X is a real random variable, i.e., it is measurable from the probability space (p) to Borel space

- The distribution of X is that of the Normal random variable

Normal Random Variable - Properties



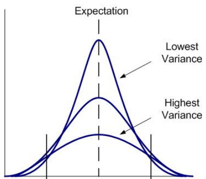
Theorem: PDF of a Normal random variable is non-negative

$\vdash \forall X\ p\ \mu\ \sigma.\ \texttt{normal\_rv}\ X\ p\ \mu\ \sigma \Rightarrow \forall x.\ 0 \leq \texttt{PDF}\ p\ X\ x$

Theorem: PDF over the whole space is 1

$\vdash \forall X\ p\ \mu\ \sigma.\ \texttt{normal\_rv}\ X\ p\ \mu\ \sigma \Rightarrow (\texttt{integral lborel}\ (\texttt{PDF}\ p\ X) = 1)$

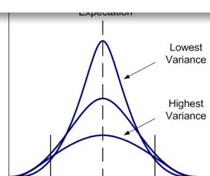
Normal Random Variable - Properties



$$\int_{\mu-a}^{\mu} PDF\ p\ X\ dx = \int_{\mu}^{\mu+a} PDF\ p\ X\ dx$$

Theorem: PDF of a Normal random variable is symmetric around its mean

$\vdash \forall$X p μ σ a. normal_rv X p μ σ $\Rightarrow$
pos_fn_integral lborel
(λx. PDF p X x * indicator_fn {x | μ-a $\leq$ x $\wedge$ x $\leq$ μ} x) =
pos_fn_integral lborel
(λx. PDF p X x * indicator_fn {x | μ $\leq$ x $\wedge$ x $\leq$ μ+a } x)



$$\int_{-\infty}^{\mu} p(x)\,dx = \int_{\mu}^{\infty} p(x)\,dx = \frac{1}{2}$$

Theorem: PDF of a Normal random variable is symmetric around its mean

$\vdash \forall$X p μ σ. normal_rv X p μ σ $\wedge$ A = {x | x $\leq$ μ} $\wedge$ B = {x | μ $\leq$ x} $\Rightarrow$
(pos_fn_integral lborel (λx. PDF p X x * indicator_fn A x) = 1 / 2) $\wedge$
(pos_fn_integral lborel (λx. PDF p X x * indicator_fn B x) = 1 / 2)

Normal Random Variable - Properties

If $X_i \sim N(\mu_i, \sigma_i^2)$ *is a finite set of independent Normal random variables, and* $Z = \Sigma\ X_i$ *then,* $Z \sim N(\Sigma\ \mu_i,\ \Sigma\ \sigma_i^2)$.

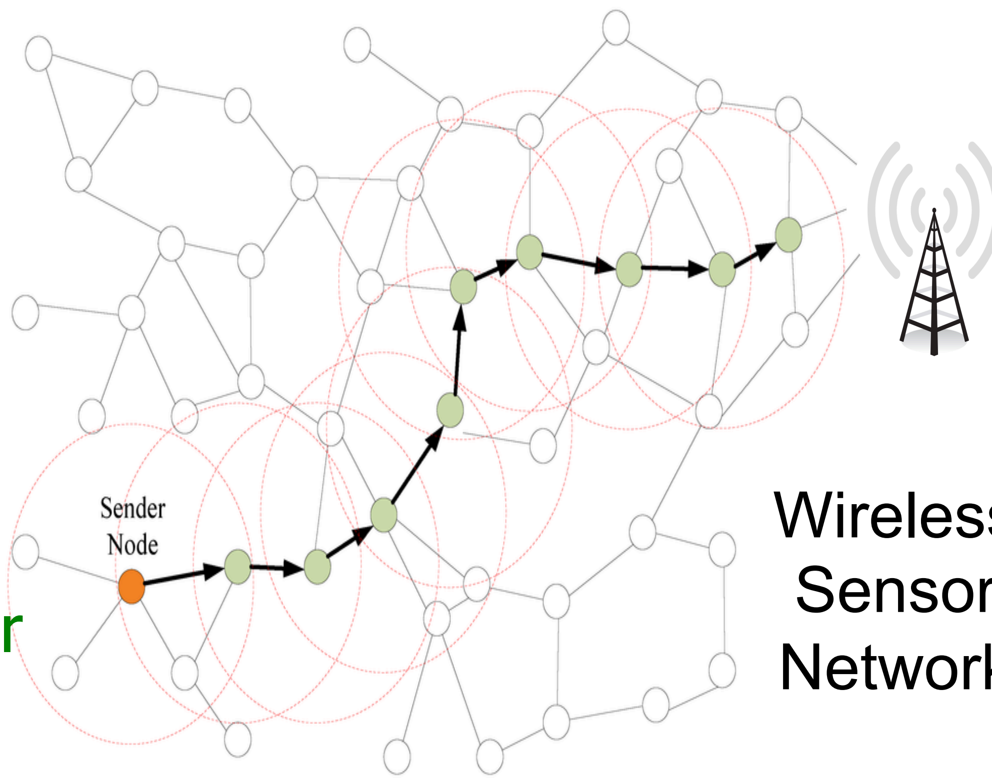
Theorem: Summation of Normal Random Variables

$\vdash \forall$p X μ σ I. prob_space p $\wedge$ FINITE I $\wedge$ I $\neq$ {} $\wedge$
indep_vars p (λi. borel_triplet) X I $\wedge$ ($\forall$i, i $\in$ I $\Rightarrow$ 0 < σ i) $\wedge$
($\forall$i, i $\in$ I $\Rightarrow$ normal_rv (X i) p (μ i) (σ i)) $\Rightarrow$
normal_rv (λx. sum I (λx. X i x)) p (sum I μ)
(sqrt (sum I (λi. (σ i) pow 2)))

- The proofs of these properties not only ensure the correctness of our definitions but also facilitate the formal reasoning process about the Normal Random Variable

Application: Probabilistic Clock Synchronization in WSNs

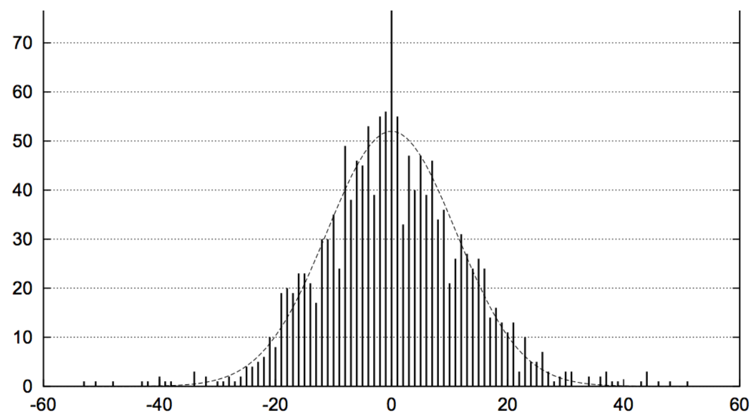
- Synchronizing receivers with one another
  - Randomness in Message delivery latency
  - Probabilistic bounds on clock synchronization error
    - single hop
    - & multi-hop networks



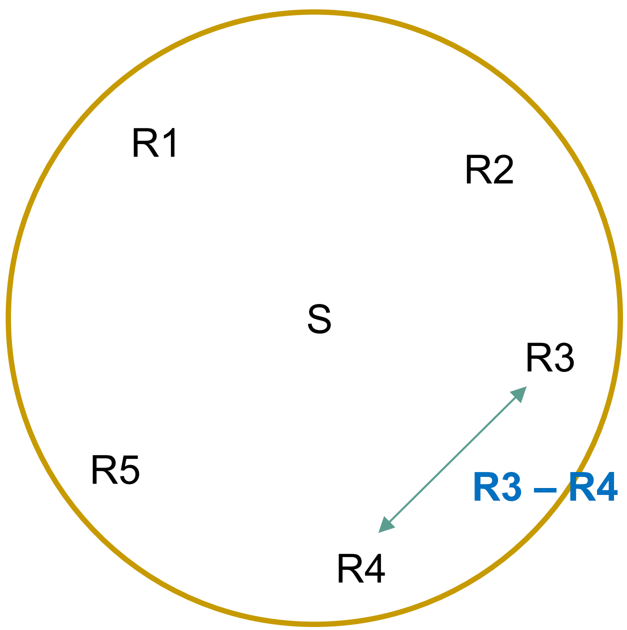
Wireless Sensor Network

Capturing the Randomness in the Latency

- Multiple pulses are sent from the sender to the set of receivers
- The difference in reception time at the receivers is plotted



Pairwise difference in packet reception time – Normally Distributed with mean = 0



Error Bounds - Single Hop

$$P(|\epsilon| \leq \epsilon_{max}) = 2\ erf\left(\frac{\sqrt{n}\epsilon_{max}}{\sigma}\right)$$

ϵ is the synchronization error

ϵ_{max} is the maximum allowable error

n is the minimum number of synchronization messages

$$erf\ (z) = \frac{\int_0^z \exp^{-\frac{x^2}{2}} \mathrm{d}x}{\sqrt{2\pi}}$$

Theorem: Probability of synchronization error for single hop network

```
⊢ ∀p X μ σ n Emax. prob_space p ∧ (I = (1 .. n)) ∧
   (0 < σ) ∧ (0 < n) ∧ (∀i. i ∈ I ⇒ sync_error (X i) p μ σ) ∧
   (Z = (λx. sum I (λi. X i x) / n)) ∧ (μ = 0) ∧ 0 ≤ Emax ⇒
   (prob_sync_error p Z {x | -Emax ≤ x ∧ x ≤ Emax} =
    2 * err_func (Emax * sqrt n / σ))
```

Conclusions

- Probabilistic Theorem Proving
  - Exact Answers
  - Useful for the analysis of Safety critical application
- Our Contributions
  - Formalization of Probability Density Functions and Normal random variables
  - Case Study
    - Clock Synchronization in WSNs
- Future Work
  - More Applications - Probabilistic Round off Error Bounds in Computer Arithmetic

Thank you!