NUST

Defining futures

Concordia University
Hardware Verification Group

Formal Reliability Analysis of Wireless Sensor Network Data Transport Protocols using HOL

Waqar Ahmed[1], Osman Hasan[1] and Sofiene Tahar[2]

[1]National School of Sciences and Technology, Pakistan

[2]Concordia University, Canada

CWN 2015

Abu Dhabi, UAE

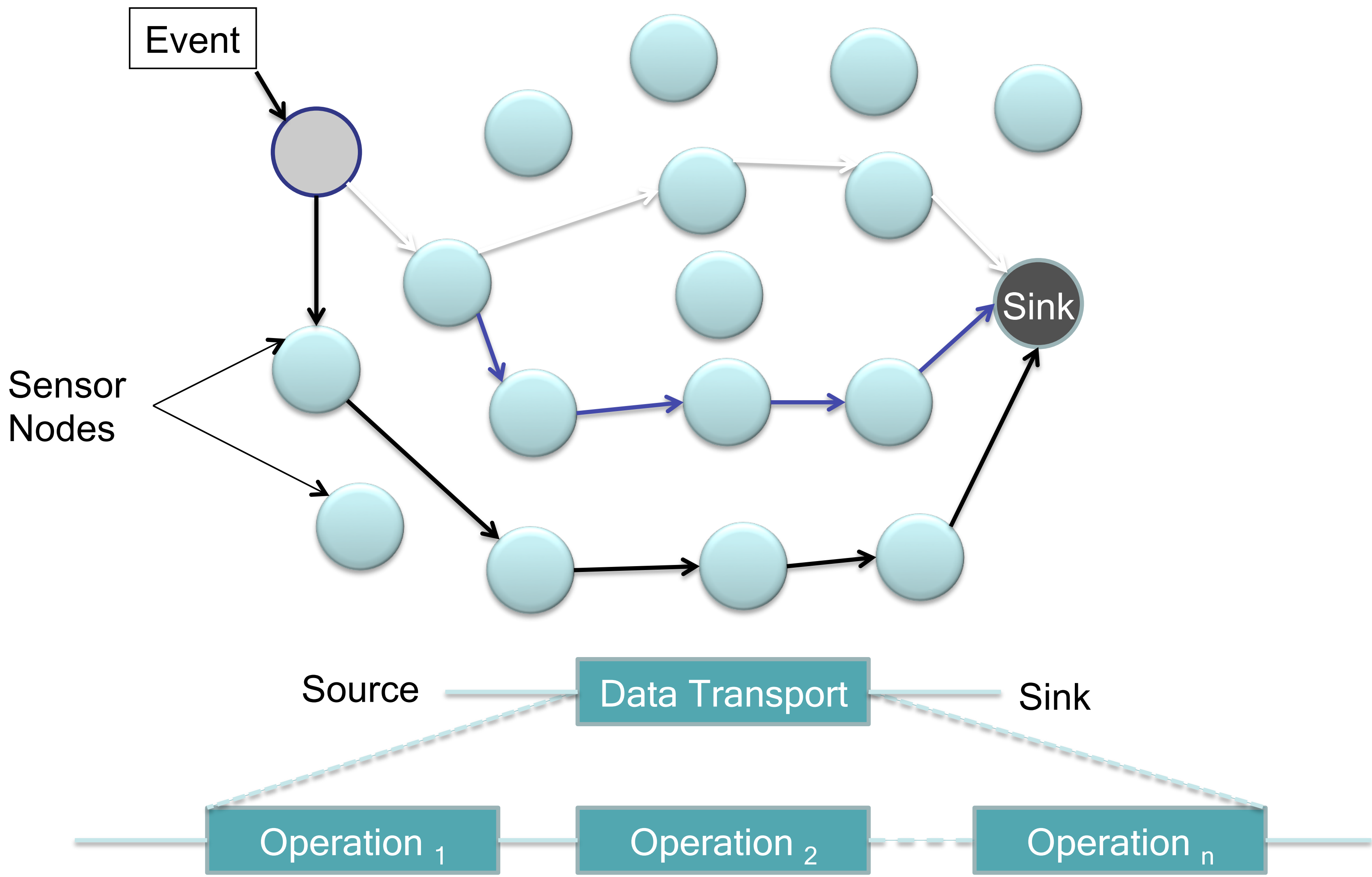
Oct 19, 3015

SAVE

Outline

- Motivation
- Methodology
- Formalizations
- Case Studies
- Conclusions

Data Transport Protocols in WSN

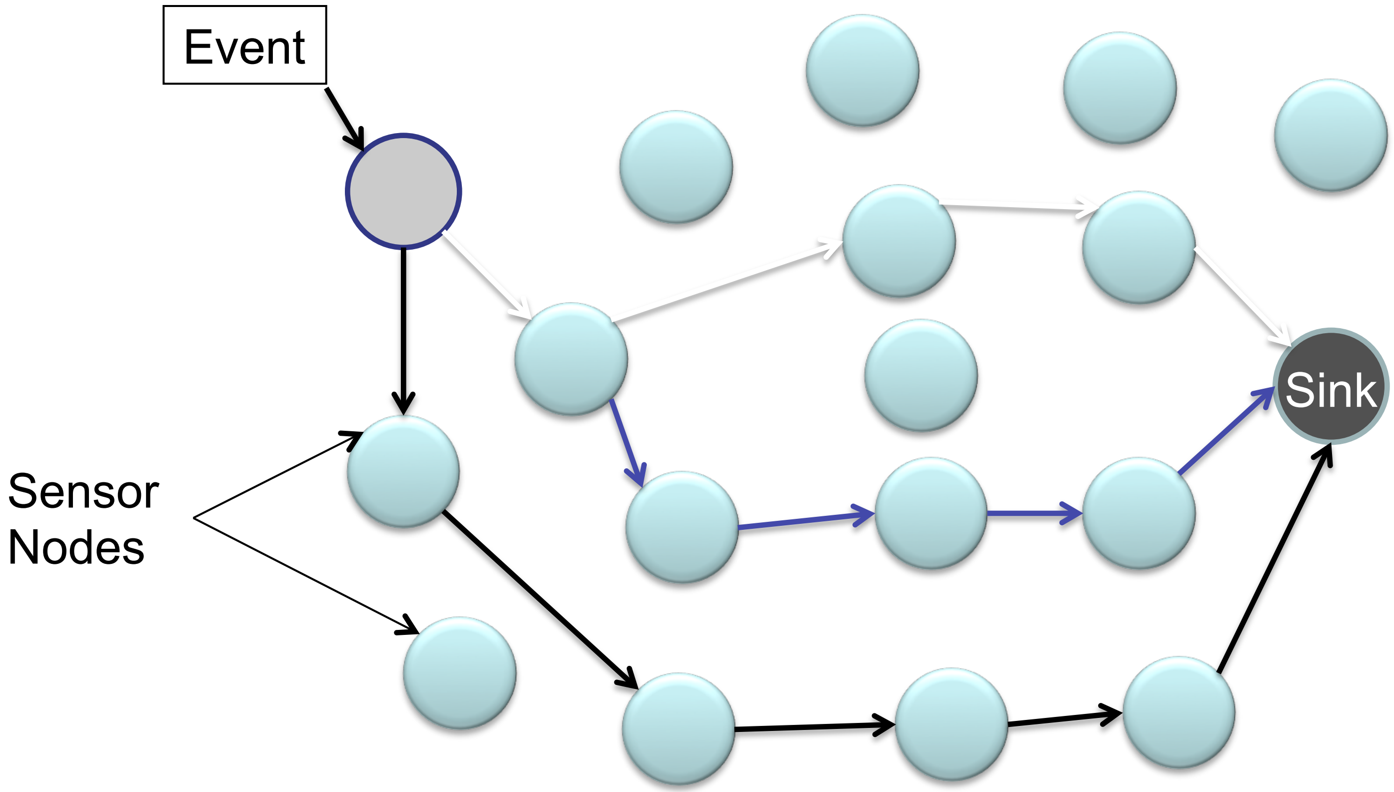


Data Transport Protocols in WSN

- Ensure a Reliable Communication
  - Routing
  - Filtering
  - Faults Tolerance

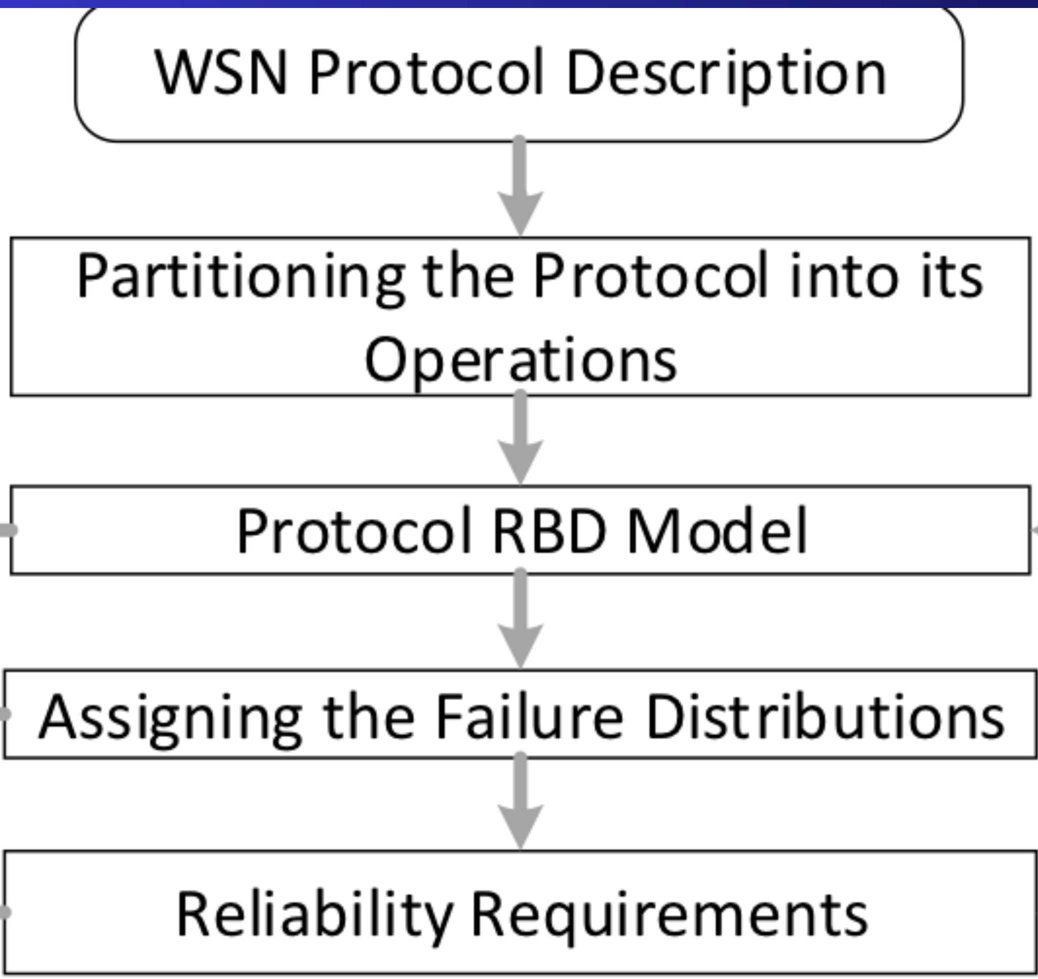
Reliability of WSN Data Transport Protocols

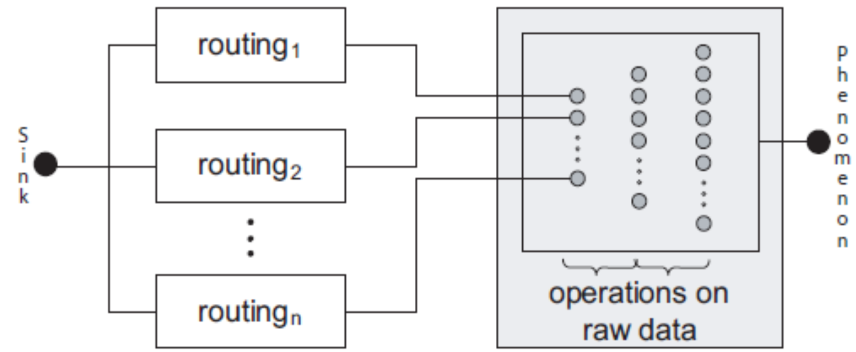
- The probability that the sensed event reaches the sink within a specified time



- Reliability depends on the reliability of operations

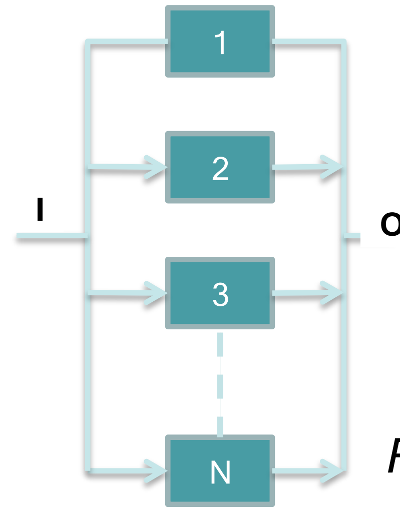
Reliability of WSN Data Transport Protocols





n = number of source nodes

Parallel Structure



$$R_R(t) = e^{-\lambda t}$$

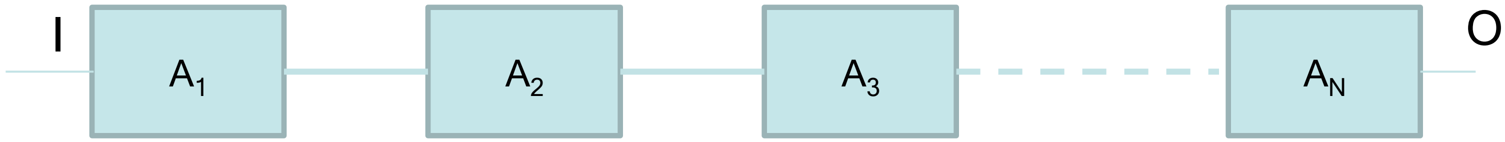
$$R_{ESRT} = 1 - (1 - R_R)^n$$

Reliability Block Diagrams

- Used to asses the reliability of a complex system
  - Partition the system into sub-blocks and connectors (RBD)
  - Find the failure rates of sub-blocks
  - Judge the failure characteristics of the overall system
    - failure rates of individual components
    - RBD configuration

- The overall system failure happens if all the paths for successful execution fail
  - Add more parallelism to meet the reliability goals

Series Reliability Block Diagram



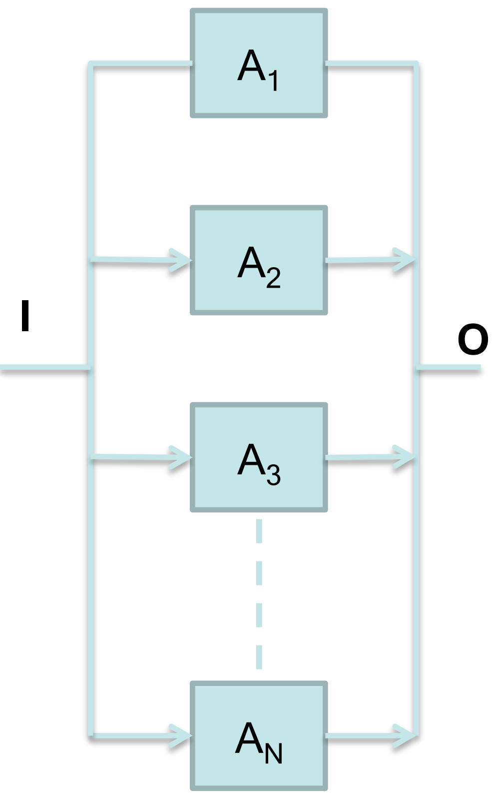
- The overall system is reliable only if all of its components are functioning reliably

$$R_{series}(t) = Pr(A_1(t) \cap A_2(t) \cap A_3(t) \cdots \cap A_N(t)) = \prod_{i=1}^{N} R_i(t)$$

Where $A_i(t)$ are the mutually independent events corresponding to *i serially-connected* components

Parallel Reliability Block Diagrams

Parallel Structure

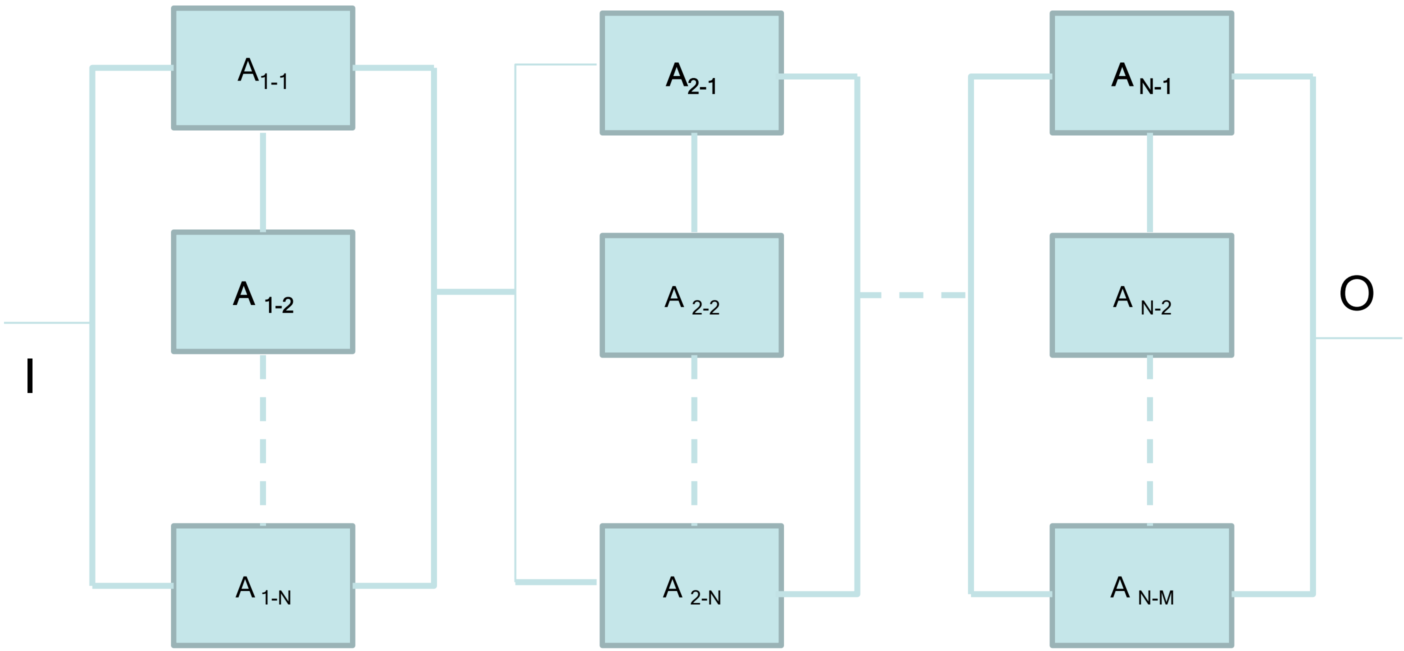


- The overall system reliability mainly depends on the component with the maximum reliability

$$R_{parallel}(t) = Pr(A_1 \cup A_2 \cup A_3 \cdots \cup A_N) = 1 - \prod_{i=1}^{N}(1 - R_i(t))$$

Where $A_i(t)$ are the mutually independent events corresponding to *i parallel-connected* components

Parallel- Series Reliability Block Diagrams



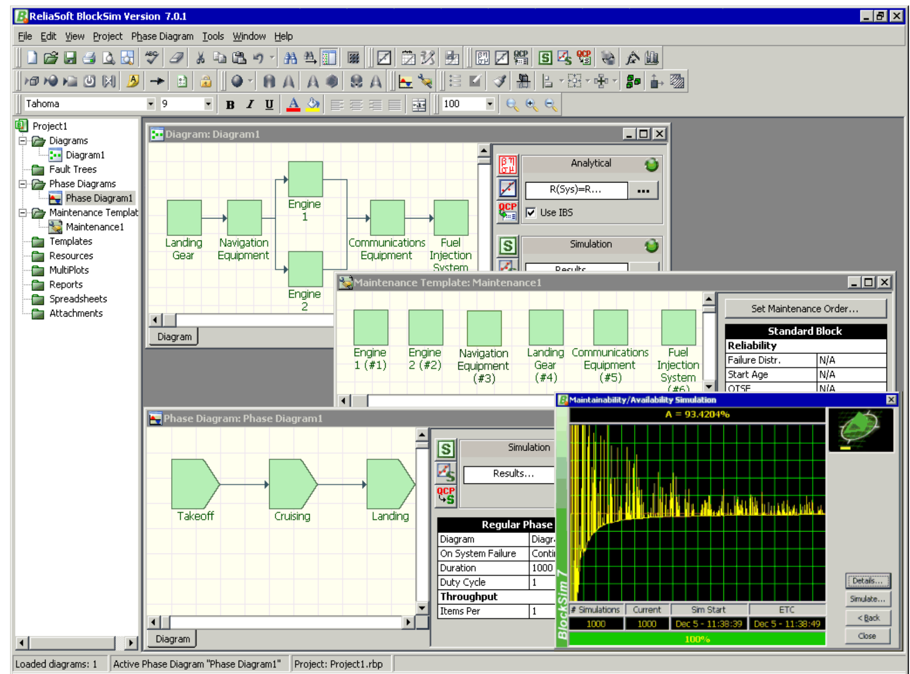
$$R_{Parallel-Series} = Pr\left(\bigcup_{i=1}^{M} \bigcap_{j=1}^{N} A_{ij}\right) = 1 - \prod_{i=1}^{M}\left(1 - \prod_{j=1}^{N}(R_{ij}(t))\right)$$

Paper-and-Pencil Proof Methods

- Construct a mathematical model of the system
- Mathematically verify that the protocol exhibits the desired reliability characteristics
- Accurate
- Scalability
- Error-Prone

Simulation

- Construct a computer based model of the system
- Analyze the behavior of the system model under a number of test cases to deduce properties of interest



- Easy to use
- May lead to wrong conclusions

WSN Protocol Reliability Analysis Accuracy

- Extremely Important

Great Duck Island

Formal Verification

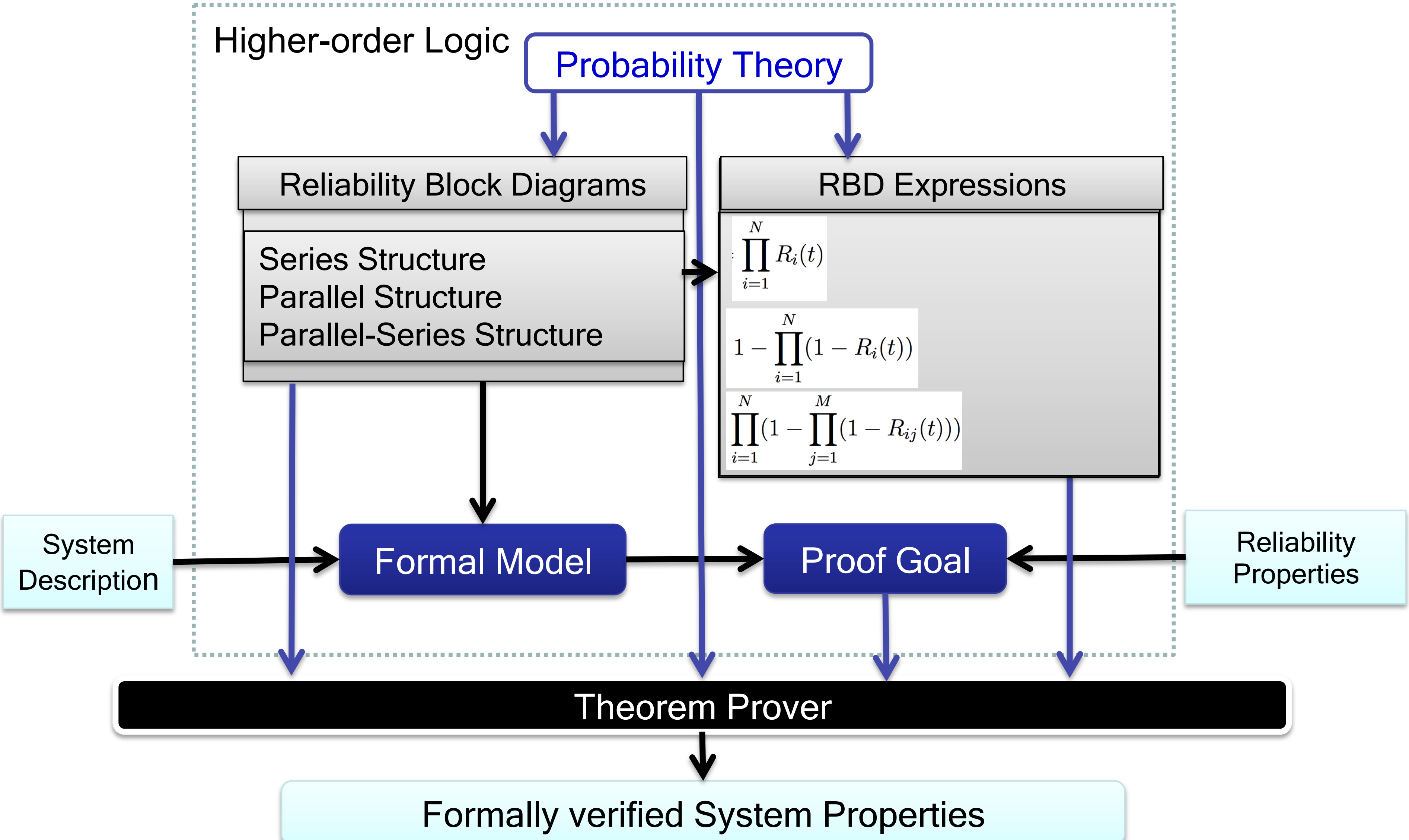
- Bridges the gap between Paper-and-pencil proof methods and simulation

- Shares their advantages
  - As precise as a mathematical proof can be
  - Computers are used for book-keeping
- Not as straightforward to use as simulation

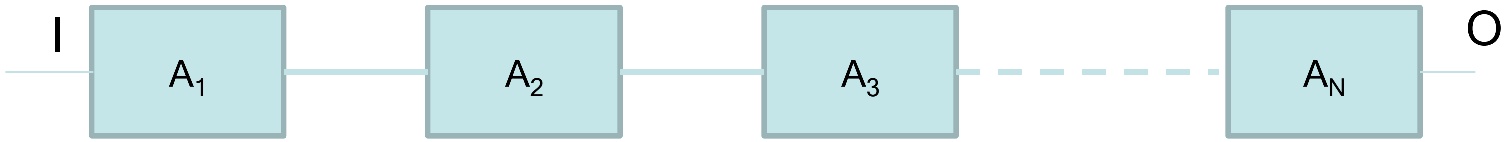
Reliability Analysis Techniques

Criteria	Paper-and-Pencil Proof	Simulation	Model Checking	Higher-order-logic Proof Assistants
Expressiveness	✓	✓	✗	✓
Accuracy	✓ ?	✗	✓	✓
Automation	✗	✓	✓	✗ ✓

Formal Reliability Analysis Methodology



Formalization of Series RBD



Definition 1: ⊢ ∀ p L. series_struct p L = inter_list p L

$$R_{series}(t) = Pr(A_1(t) \cap A_2(t) \cap A_3(t) \cdots \cap A_N(t)) = \prod_{i=1}^{N} R_i(t)$$

Theorem 1: ⊢ ∀ p L. prob_space p ∧ (events p = POW (p_space p)) ∧
1 ≤ LENGTH L ∧ mutual_indep p L ⇒
(prob p (series_struct p L) = list_prod (list_prob p L))

Other RBDs

Definition 2: $\vdash \forall$ L . parallel_struct L = union_list L

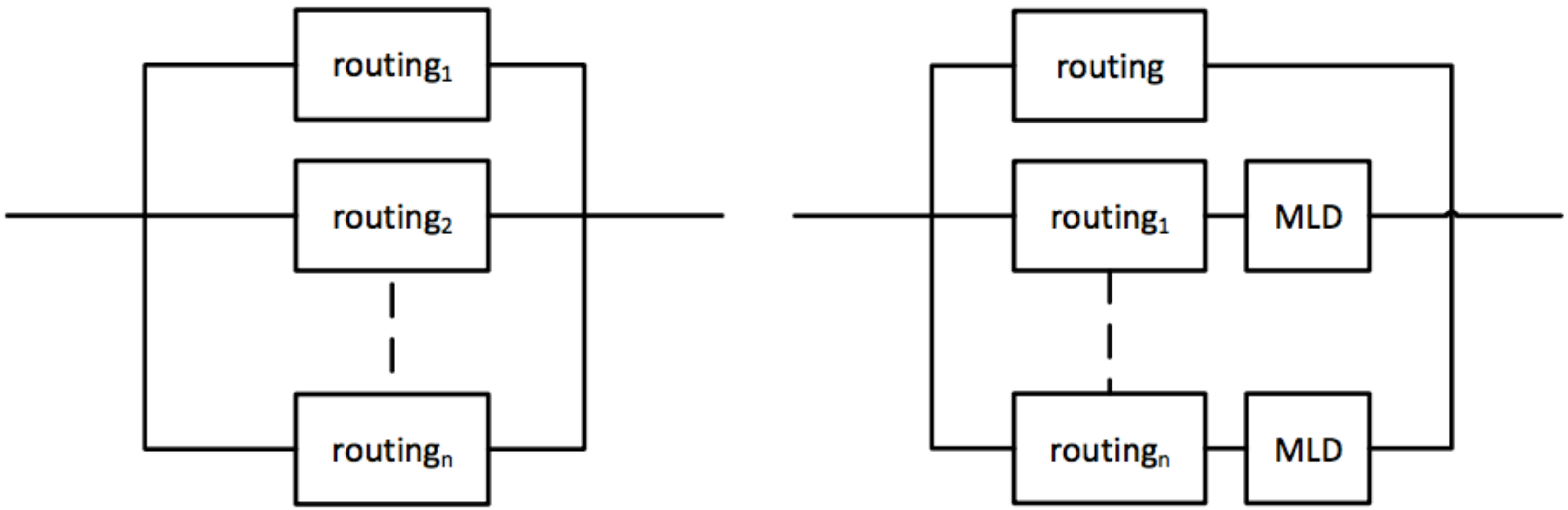
Theorem 2: $\vdash \forall$ p L. (prob_space p) $\wedge$
(events p = POW (p_space p)) $\wedge$
(1 $\leq$ LENGTH L) $\wedge$ (mutual_indep p L) $\wedge$
($\forall$ x'. MEM x' L $\Rightarrow$ x' $\in$ events p) $\Rightarrow$
(prob p (parallel_struct L) =
1 - list_prod (one_minus_list (list_prob p L)))

Definition 3: $\vdash \forall$ p L. parallel_series_struct p L =
parallel_struct (list_inter_list p L)

Theorem 3: $\vdash \forall$p L. (prob_space p) $\wedge$
(events p = POW (p_space p)) $\wedge$
($\forall$z. MEM z L $\Rightarrow$ ~NULL z) $\wedge$ (mutual_indep p (FLAT L)) $\wedge$
($\forall$x'. MEM x'(FLAT L) $\Rightarrow$ x' $\in$ events p) $\Rightarrow$
(prob p (parallel_series_struct p L) =
1 − list_prod (one_minus_list(list_rel_list_prod p L)))

Case Studies

- End-to-End data transport protocols
  - Event to Sink Reliable Transport (ESRT)
  - Reliable Multi-Segment Transport (RMST)



- Routing is used to identify potential routes for data transport
- Message Loss Detection (MLD) is used to retransmit transport data and is thus an essential part of reliable data transmission

Case Studies

Theorem: *Reliability of ESRT Protocol*

```
⊢ ∀ X_rout_list C_rout_list p t.
(0 ≤ t) ∧ (prob_space p) ∧
mutual_indep p
 rel_event_list p X_rout_list t ∧
∀x'. MEM x'
 (rel_event_list p X_routing_list) t ⇒
x' ∈ events p ∧
list_exp p C_routing_list X_routing_list ⇒
 prob p (ESRT_RBD p X_routing_list t) =
 1 - list_prod
  (one_minus_exp t C_routing_list)
```

Theorem: *Reliability of RMST Data Transport Protocol*

```
⊢ ∀ X_rout X_MLD C_rout C_MLD p t.
(0 ≤ t) ∧ (prob_space p) ∧
(∀z. MEM z (List_rel_event_list p
 (RMST_rv_list X_rout X_MLD) t) ⇒ ~NULL z) ∧
mutual_indep p
 (FLAT(List_rel_event_list p
  ([X_rout]::RMST_rv_list X_rout X_MLD) t)) ∧
PREIMAGE X_rout {y| y ≤ Normal t} ∈ events p ∧
PREIMAGE X_MLD {y| y ≤ Normal t} ∈ events p ∧
LENGTH (RMST_rv_list X_rout X_MLD) =
LENGTH (RMST_fail_rate C_rout C_MLD) ∧
list_list_exp p
 ([C_rout]::RMST_fail_rate C_rout C_MLD)
 ([X_rout]::RMST_rv_list X_rout X_MLD) ⇒
 prob p (RMST_RBD p X_rout X_MLD t) =
 1 - list_prod (one_minus_list
  (list_exp_sum
   ([C_rout]::RMST_fail_rate C_rout C_MLD) t)
```

- The reasoning was very straightforward - About 1000 lines of HOL code
- All the variables are universally quantified
- Guaranteed correctness due to the involvement of a theorem prover
  - All the required assumptions for are explicitly available

Conclusions

- Formal Reliability Analysis of WSN Data Transport Protocols
  - Accurate and Complete Results
- Formalization of Reliability Block Diagrams (RBDs)
  - Many other applications
- Case Studies

  Event to Sink Reliable Transport (ESRT)

  Reliable Multi-Segment Transport (RMST)
- Formal Verification is not an alternative to simulation
  - Both techniques have to play together for a successful analysis framework

Thanks!

- For More Information

  - Visit our websites
    - http://save.seecs.nust.edu.pk
    - http://hvg.ece.concordia.ca

  - Contact
    - osman.hasan@seecs.nust.edu.pk