A Security Aware Routing Approach for Networks-on-Chip

Priscila Giovanella Vivian

Advisor: Prof. Ph.D. César Augusto Missio Marcon

Co-Advisor: Prof. Ph.D. Martha Johanna Sepúlveda Flórez

Pontifical Catholic University of Rio Grande do Sul
Faculty of Informatics
Computer Science Graduate Program

July 20, 2016

Index

Index

Introduction I

- The Network-on-Chip (NoC) has been widely adopted as a paradigm capable of providing a reliable and scalable interconnection in MPSoCs [?], [?]
- The concern for data protection appears as a design requirement of MPSoCs
- Protection usually occurs at either:
  - *Application Level*, e.g., using data encryption or source authentication; or
  - *Communication Level*, e.g., detecting abnormal communication behavior in the system.

Introduction II

- NoCs have been shown to aid in the overall MPSoC protection [?], [?], [?], by implementing security services at communication level

Index

Objectives

- The definition of a routing model that is capable of considering system security requirements to define safe routing paths
- The creation of an abstract model that enables the implementation and the verification of the routing technique
- The validation and evaluation of the routing algorithm for different security configurations
- The adaptation of an existing NoC simulation platform to employ this new routing model for behavior evaluation

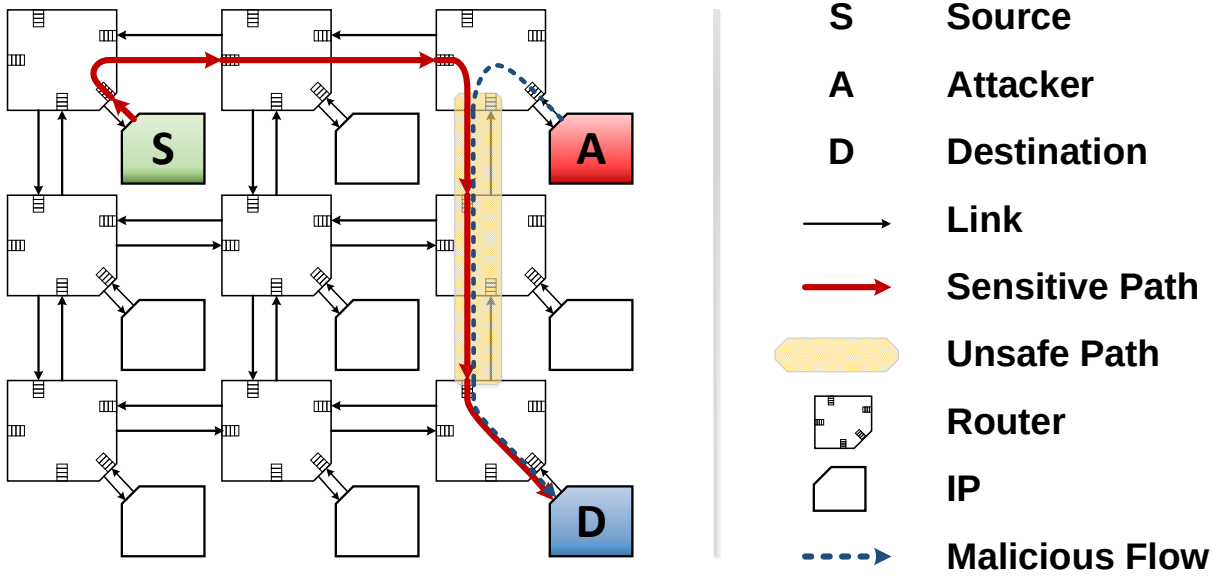
Index

Research

- This work is based on two premises:
  - (i) that sensitive applications communicate over the NoC in MPSoCs, and are therefore vulnerable to interference by malicious applications; and
  - (ii) that protection from software attacks is achieved by communication level protection; e.g., by defining safe communication paths for sensitive applications
- Therefore, a routing algorithm that is capable of defining safe routing paths for sensitive applications should enhance the overall system protection

Index

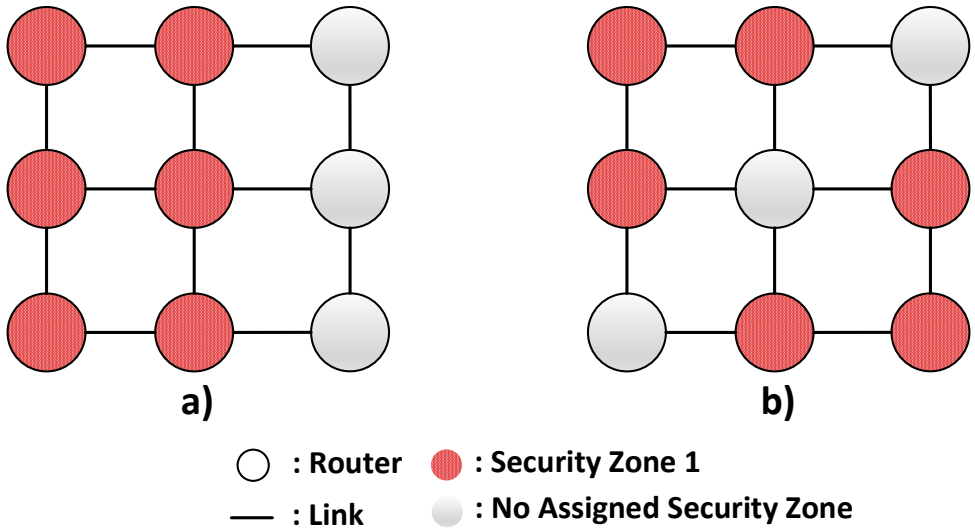
Threat Model



- The NoC is considered secure, meaning that an attacker cannot tamper its resources
- An attacker, aware of the sensitive path, can disrupt communication between a source and a destination
- We consider that an attacker can either generate a *DoS* or *Timing Attack* on the sensitive path

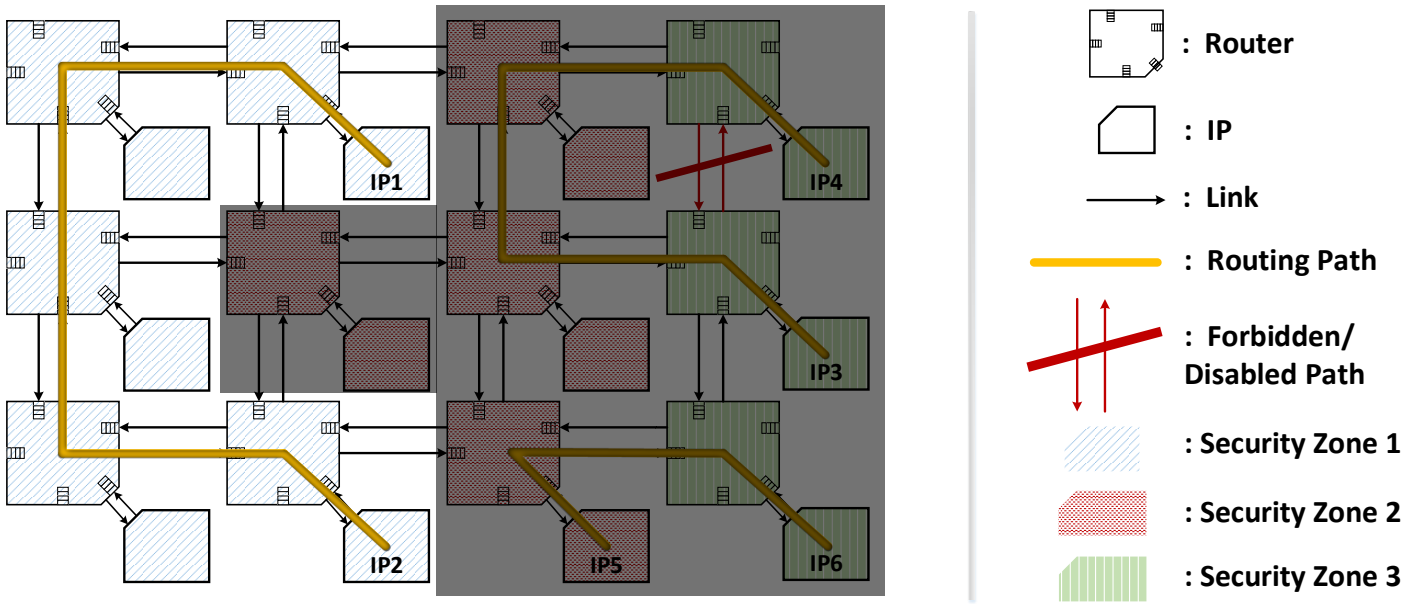
Index

Security Zones



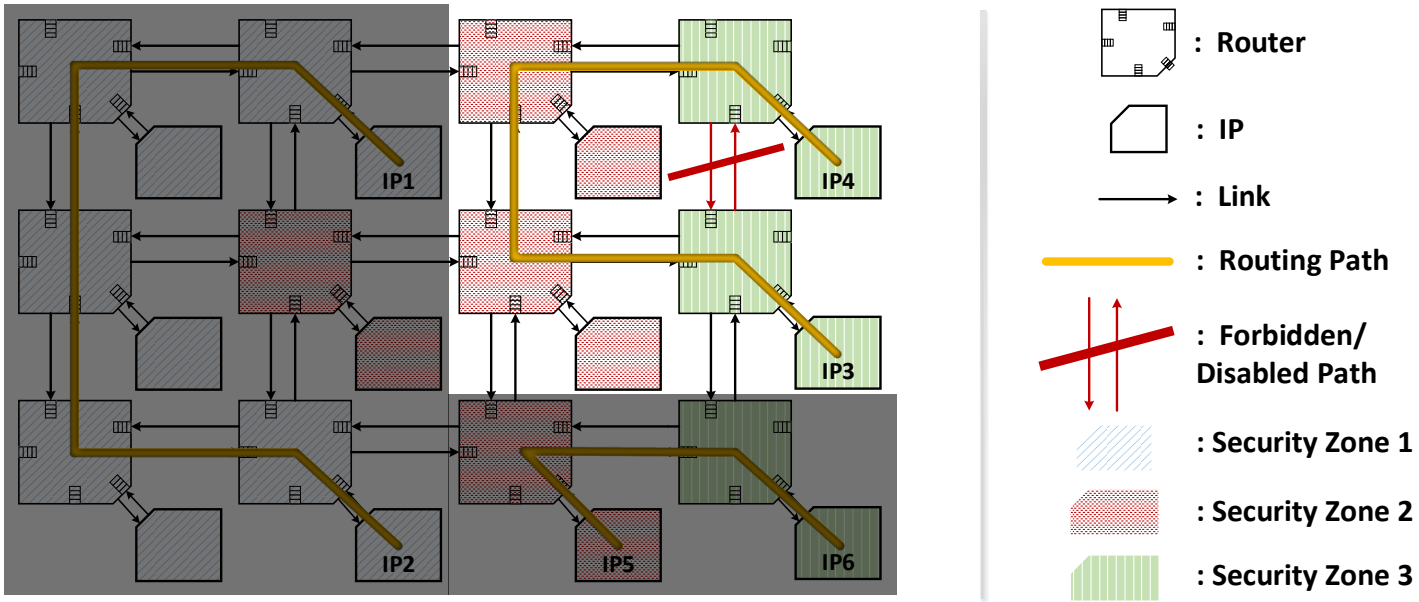
- A security zone is a physical space (continuous or disrupted) that wraps IPs that execute critical applications
- The task mapping of critical applications defines the shape of the security zone
- Certain IP blocks might not be assigned to any security zone, e.g., idle resources or shared memories

Communication in Security Zones



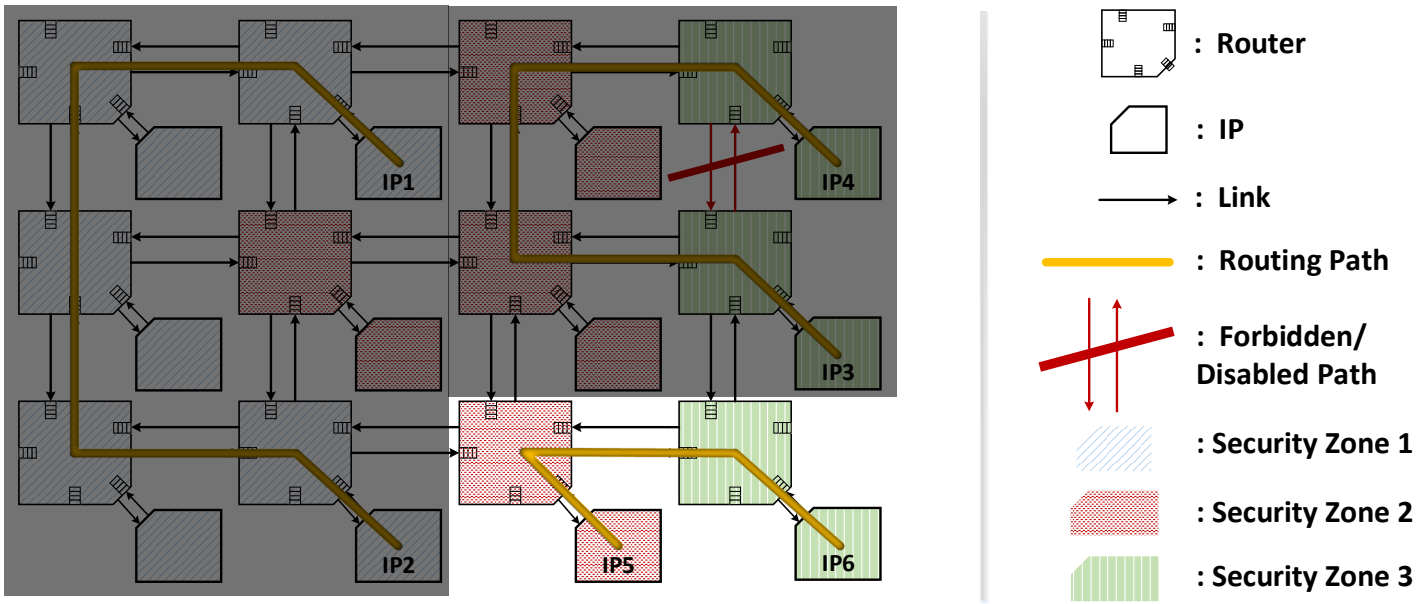
- ***Full intra-zone communication (FIZ)***: S and D are in the same SZ. The sensitive path is **completely** inside the SZ, e.g., the path from *IP1* to *IP2*

Communication in Security Zones



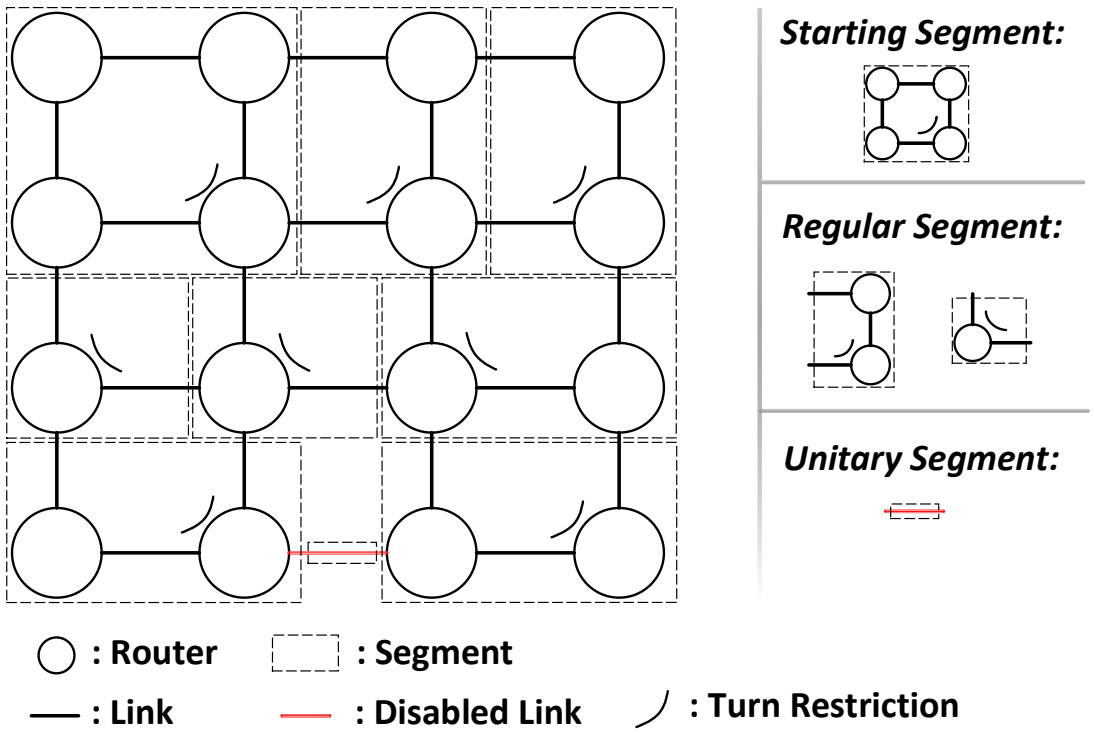
- ***Partial intra-zone communication (PIZ)***: *S* and *D* are in the same *SZ*. However, the sensitive path is **partially** inside the *SZ*. , e.g., the path from *IP3* to *IP4*

Communication in Security Zones



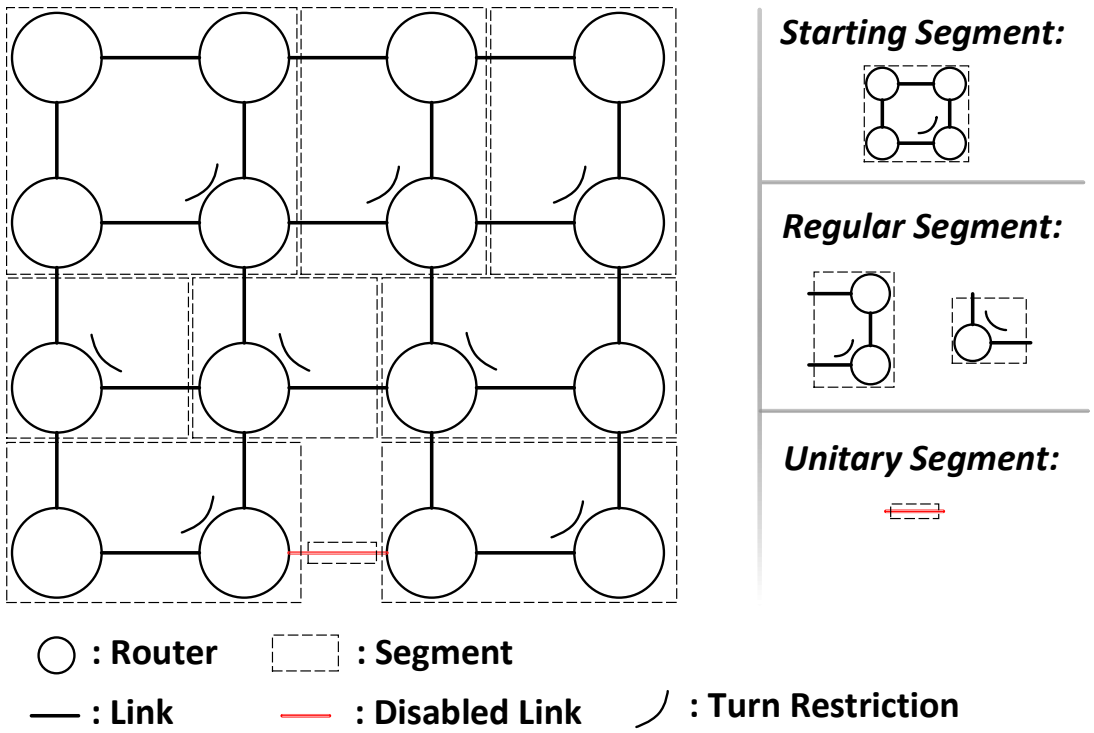
- ***Inter-zone communication (IZ)***: *S* and *D* are in different *SZ*, e.g., the path from *IP5* to *IP6*

Segment-based Routing (SBR) - Deadlock Prevention



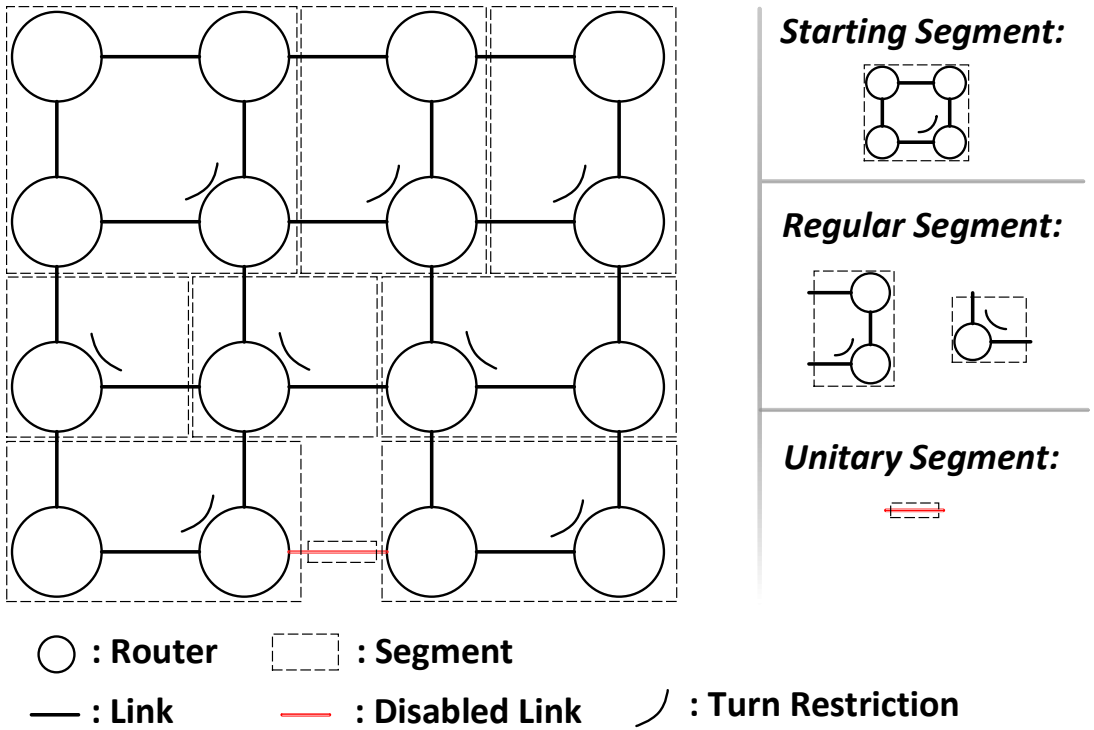
- Logically partitions the NoC into segments

Segment-based Routing (SBR) - Deadlock Prevention



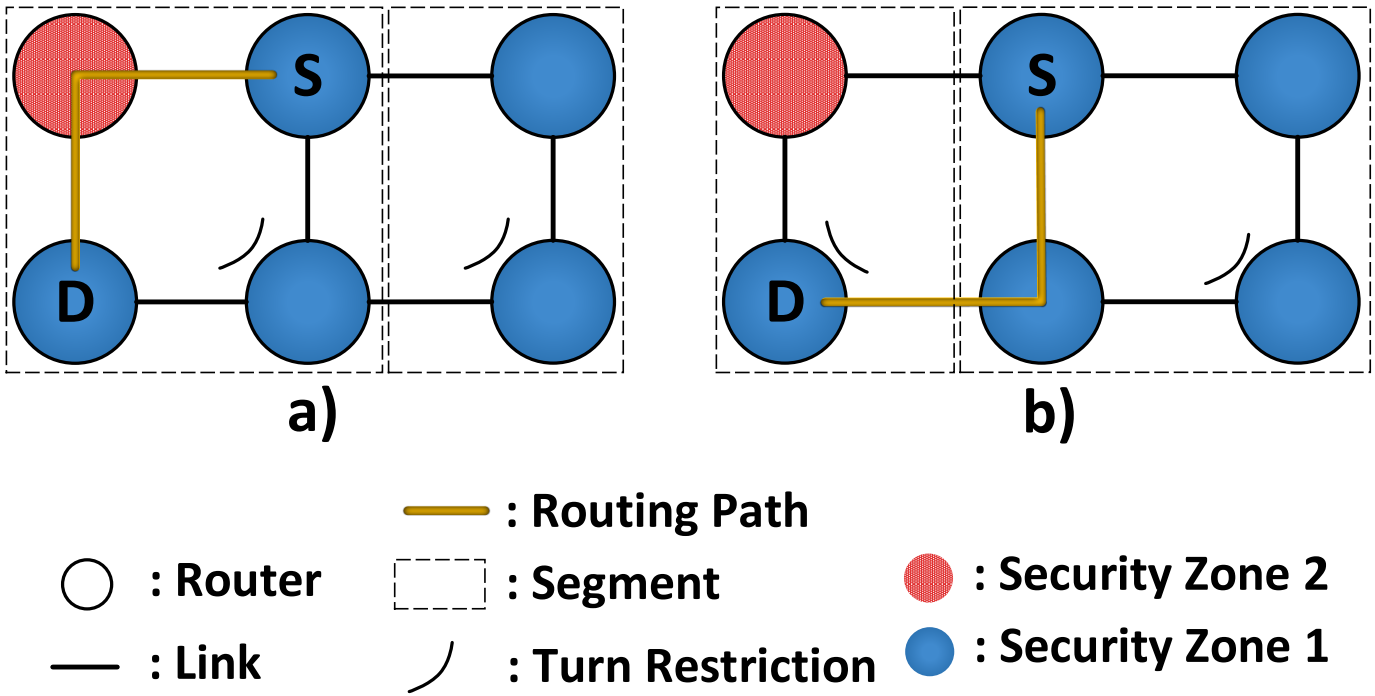
- Each segment contains a localized bidirectional turn restriction

Segment-based Routing (SBR) - Deadlock Prevention



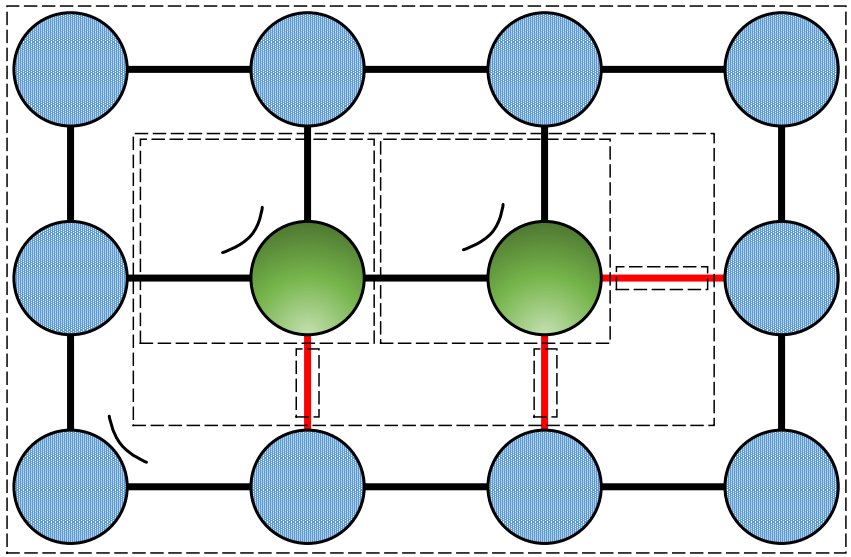
- Guarantees global deadlock freedom and reachability (as long as the NoC is connected)

SBR-Security Zone Awareness (SBR-SZA)



- Traditional SBR might place turn restrictions that causes ***PIZ*** routing

SBR-Security Zone Awareness (SBR-SZA)



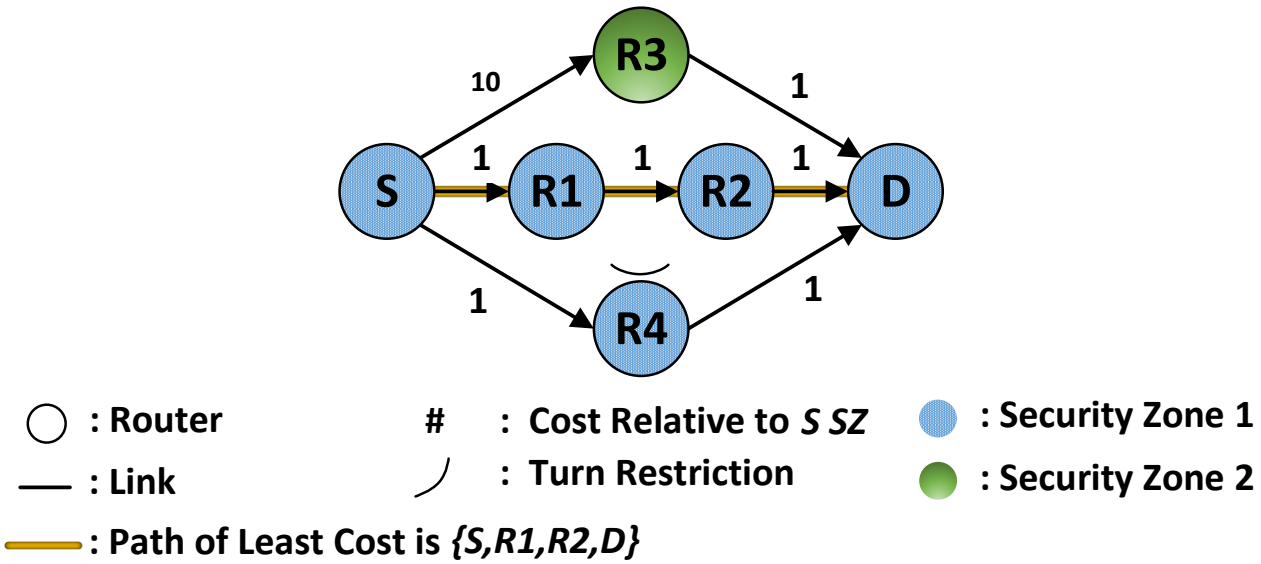
- SBR-SZA aims to create segments that tailor to security zone shapes

Region-based Routing (RBR) - Routing Algorithm

- Populates the routing tables of NoC routers, considering the turn restrictions of SBR
- Groups routing entries to greatly reduce table size (interval routing and port/destination sets)
- There are three steps in RBR computation:
  - *Routing Computation*: computes all source and destination pairs
  - *Region Computation*: joins entries based on input and output ports
  - *Region Merge*: merges overlapping regions to reduce routing entries

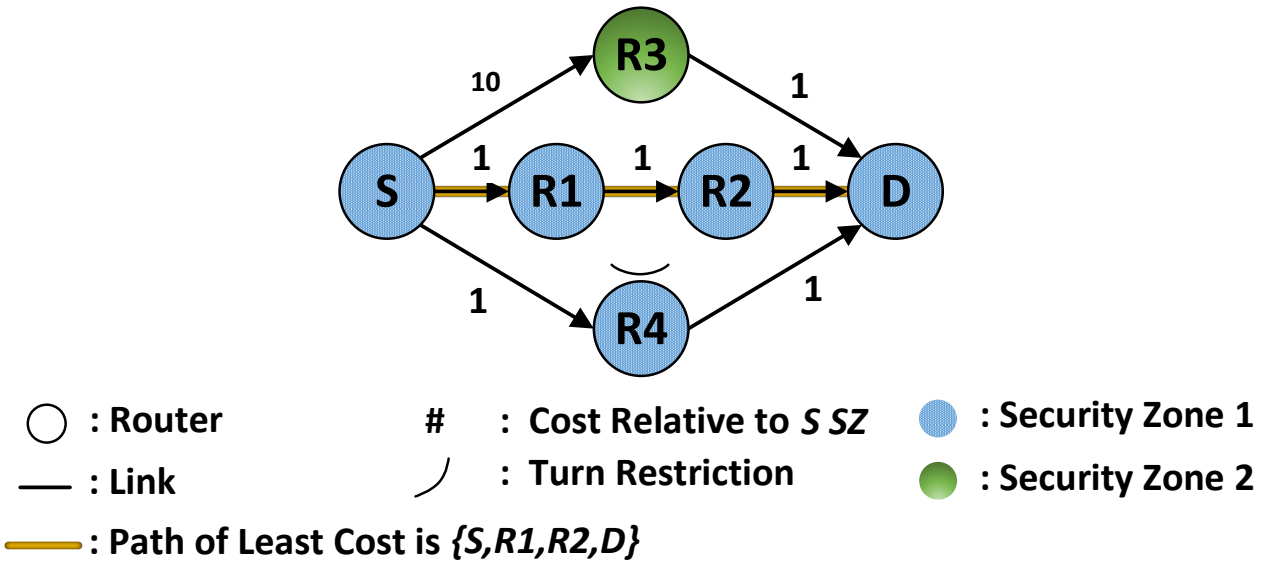
Index

Modeling



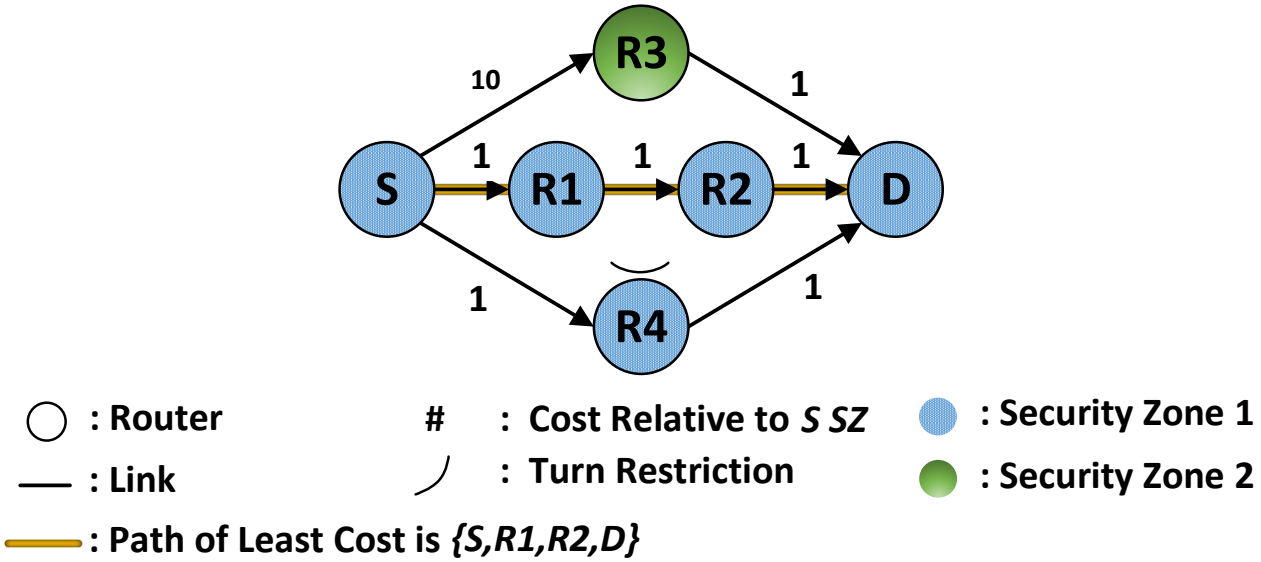
- The NoC is modeled as a graph, with IP/Routers as vertices and links as edges

Modeling



- Each vertex belongs to a security zone, and each edge has a positive weight that is set according to the path-finding iteration

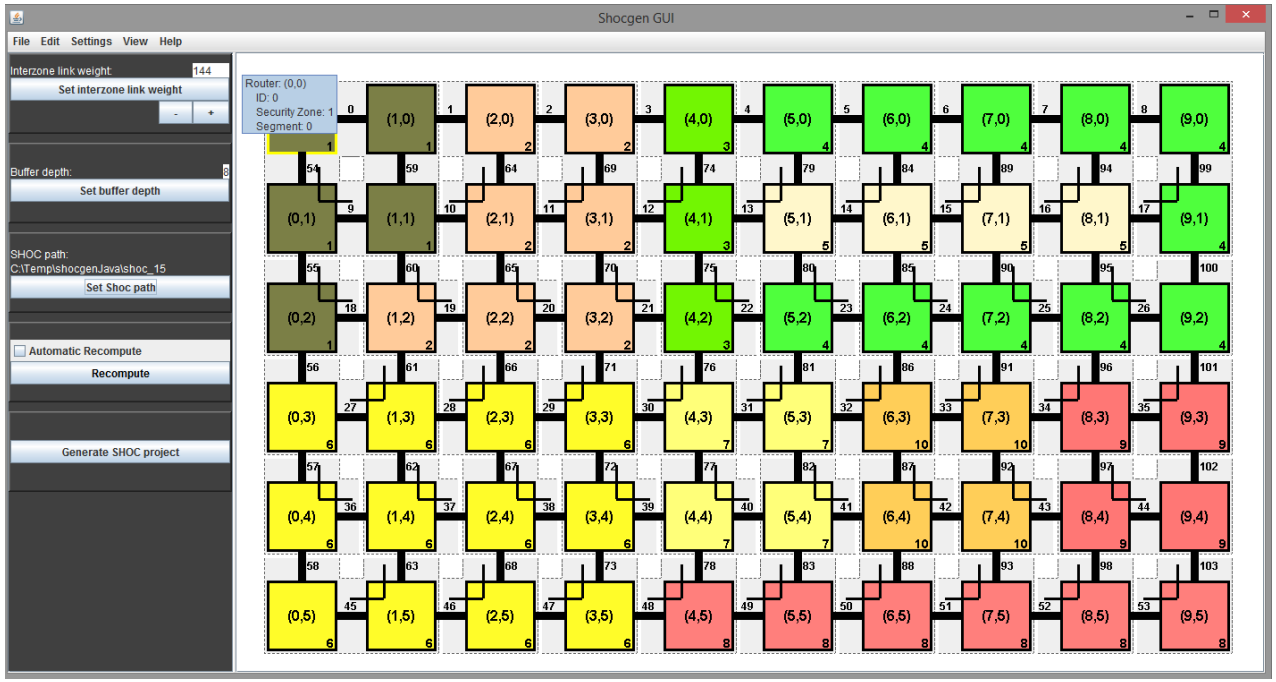
Modeling



- Edge weight can represent the cost to employ encryption to a sensitive packet

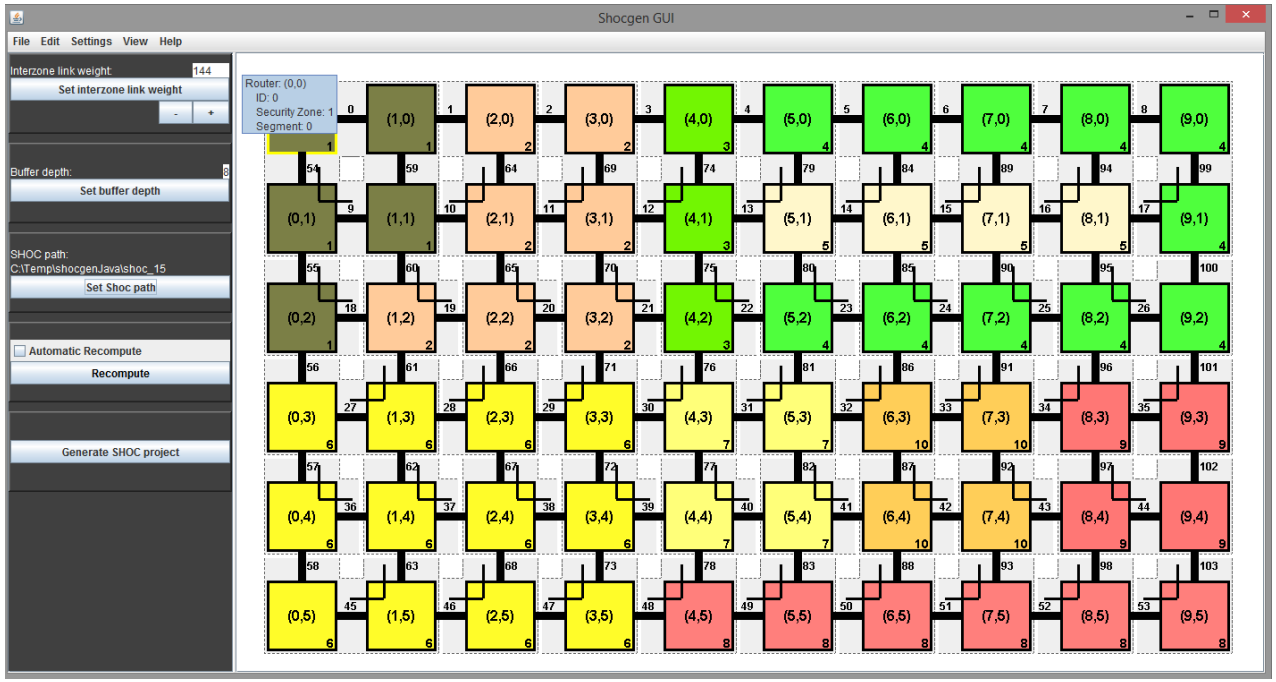
Index

NoC Configuration Tool



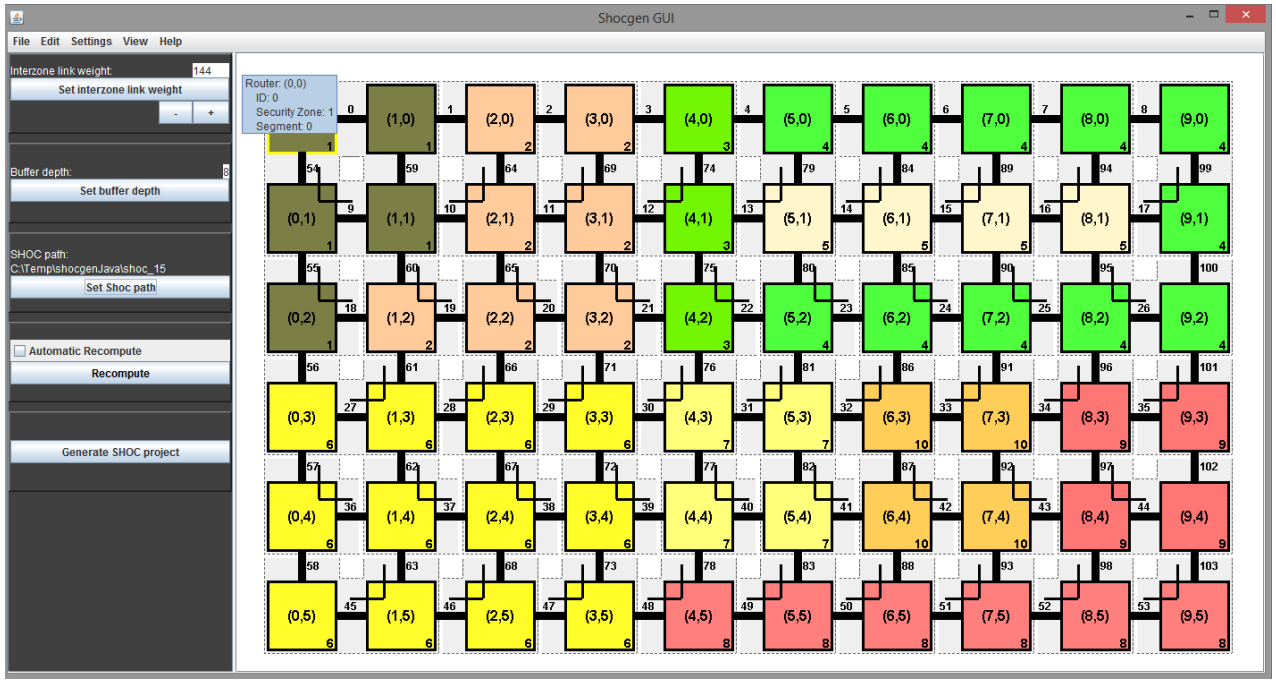
- Graphical configuration tool to generate and compute scenarios at *design time*

NoC Configuration Tool



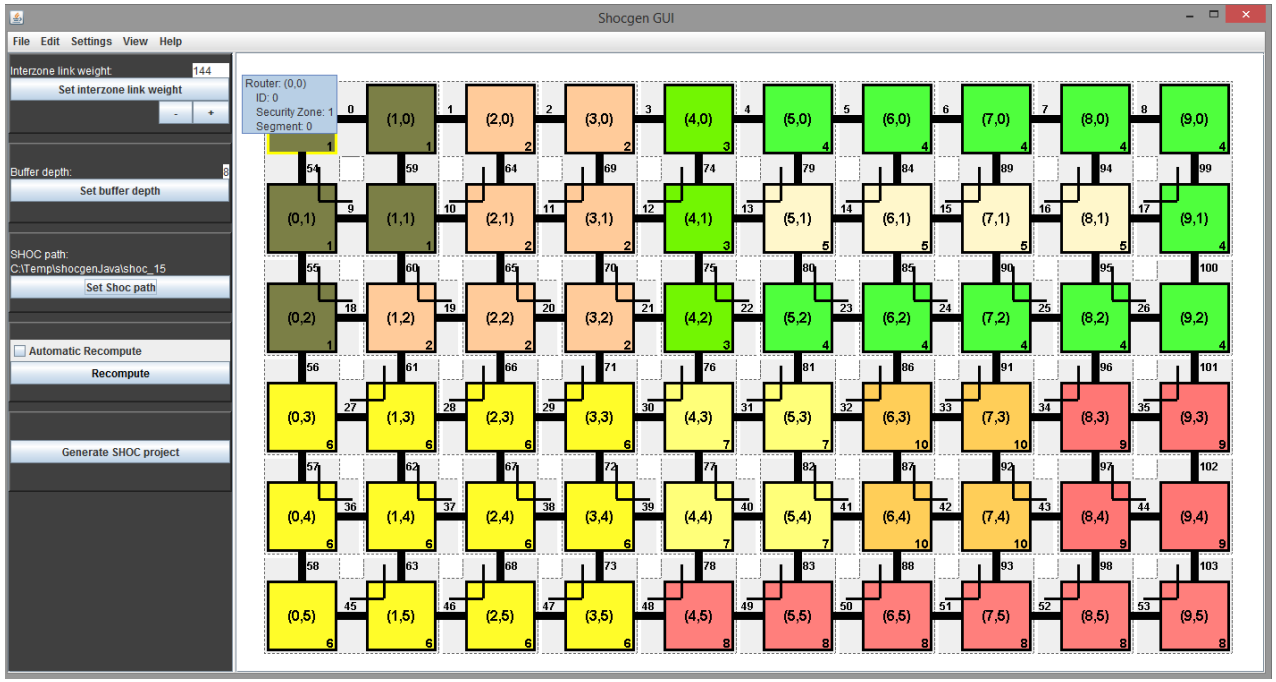
- Implements SBR and RBR algorithms to populate routing entries

NoC Configuration Tool



- Performs routing entries, ***FIZ/PIZ*** routing paths, and latency evaluations

NoC Configuration Tool



- Outputs the generated configuration to a SystemC simulation platform

Index

Evaluation Criteria

Scenario	NoC Dimension (Columns *X* Rows)	SBR Seeds	Segmentation Modes	Configurations per Scenario
NASA NAS	13x13	169	*SBR* / *SBR-SZA*	338
Synth 1	6x4	24	*SBR* / *SBR-SZA*	48
Synth 2	10x6	60	*SBR* / *SBR-SZA*	120
			Total:	506

- Three scenarios evaluated: 2 synthetic and 1 based on a real application communication dependency trace
- Evaluation consists of four preliminary steps
  - Seed for segment computation
  - SBR computation
  - RBR computation
  - Evaluation of obtained configuration

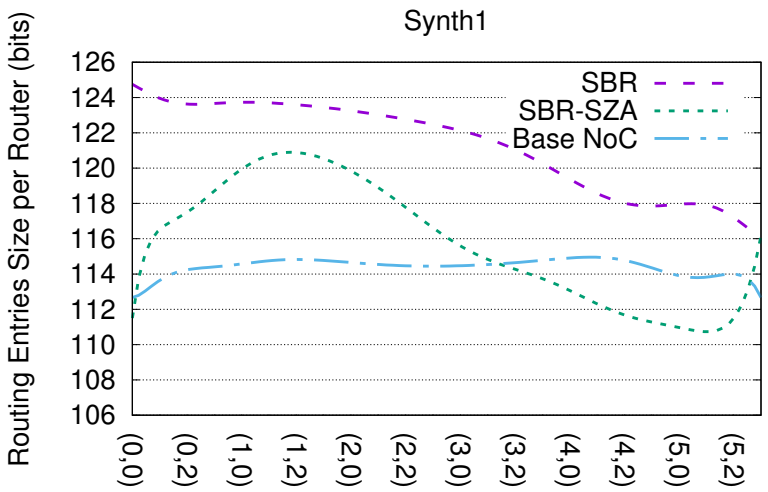
Evaluation Criteria

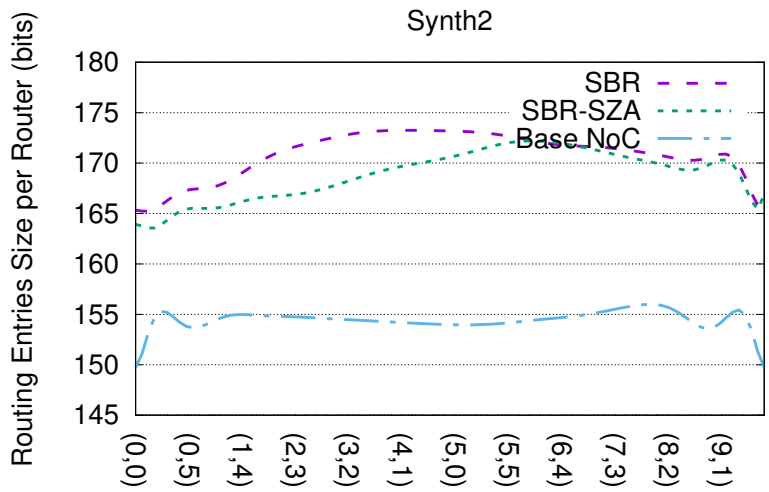
Scenario	NoC Dimension (Columns X Rows)	SBR Seeds	Segmentation Modes	Configurations per Scenario
NASA NAS	13x13	169	*SBR* / *SBR-SZA*	338
Synth 1	6x4	24	*SBR* / *SBR-SZA*	48
Synth 2	10x6	60	*SBR* / *SBR-SZA*	120
			Total:	506

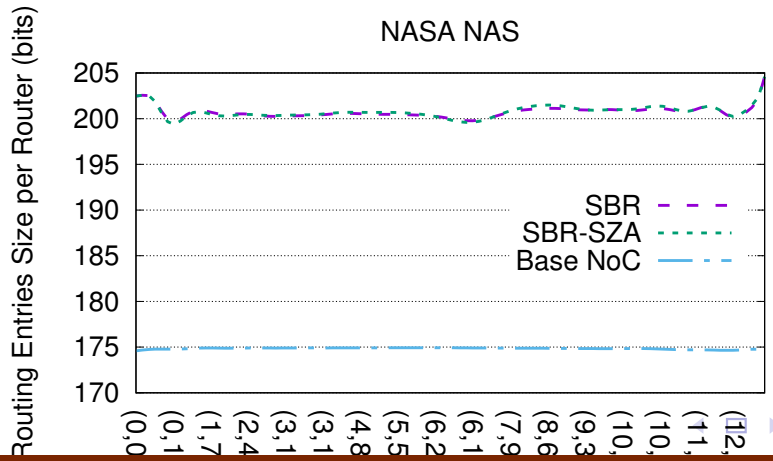
- Three evaluations were performed:
  - Routing table scalability
  - ***FIZ/PIZ*** occurrences
  - Latency estimation

Index

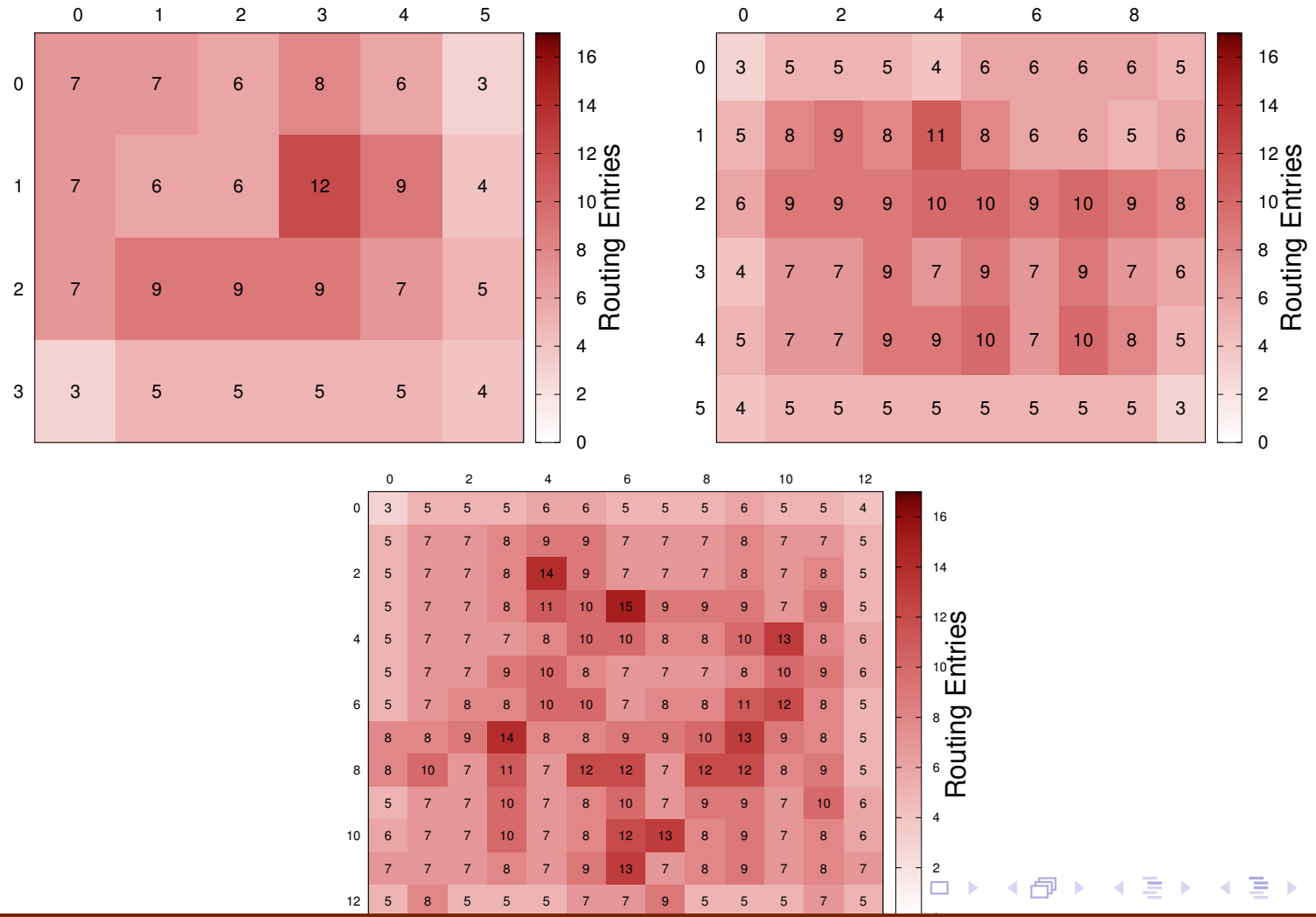
Routing Table Scalability - Average Routing Tables Size



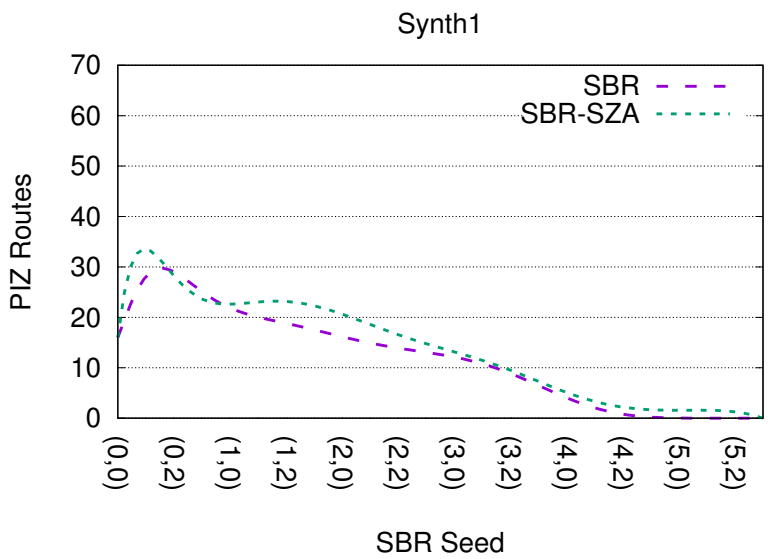


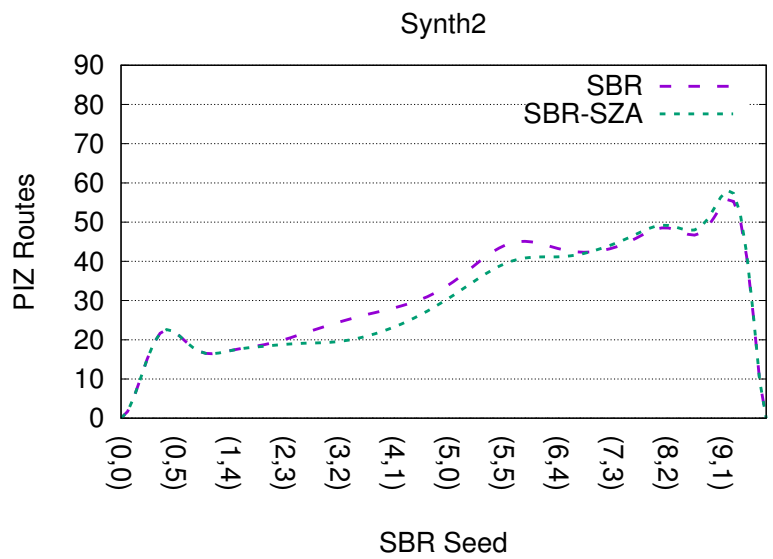


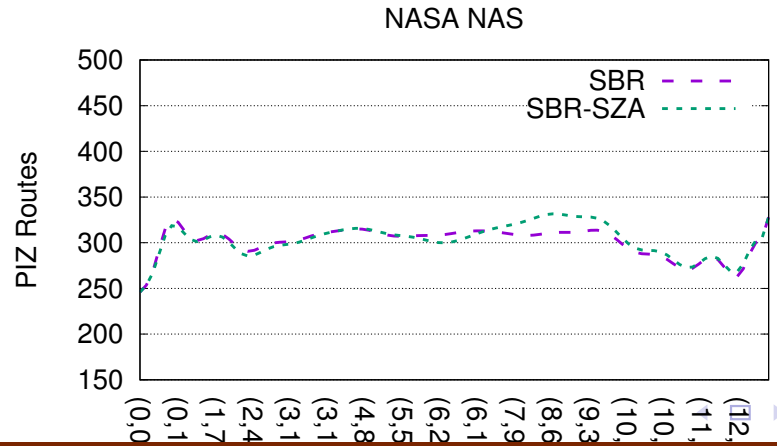
Routing Table Scalability - Optimal Configuration Heatmap



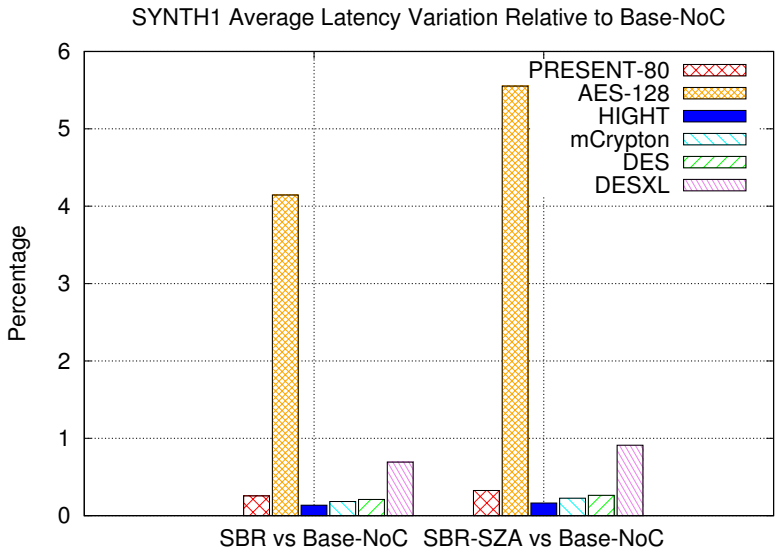
FIZ Occurrences

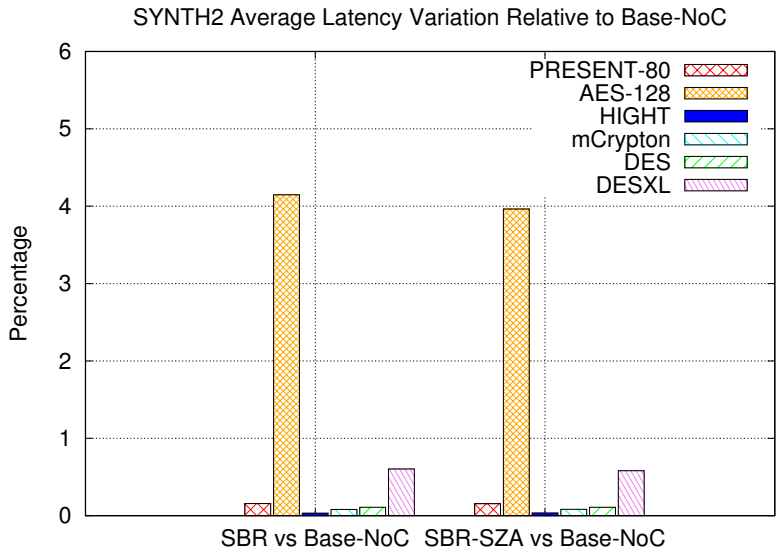


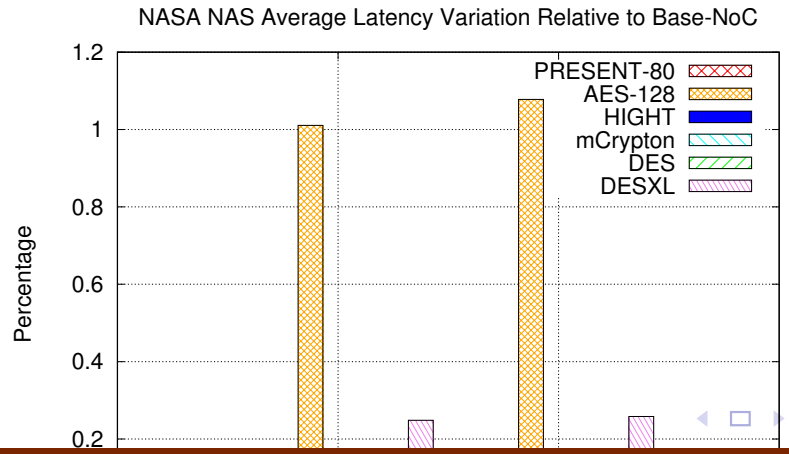




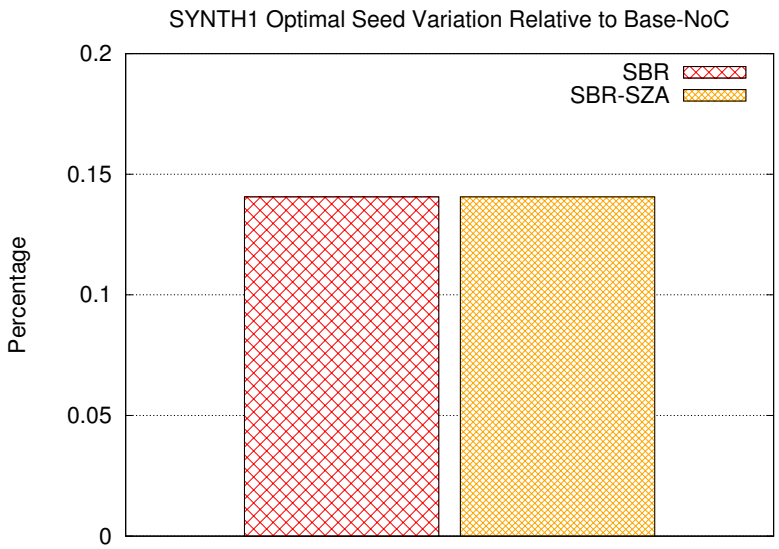
Latency Variation

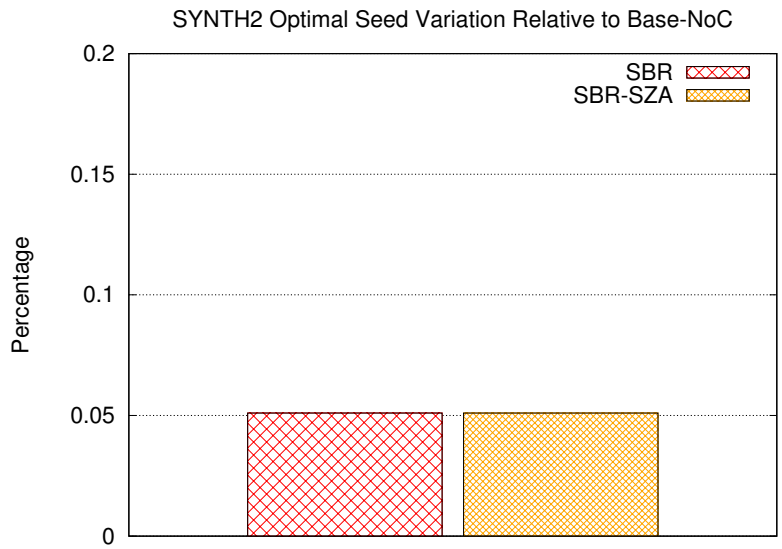






Latency Variation - FIZ Communication





Index

Work Schedule

Activities	2016						2017		
	07	08	09	10	11	12	01	02	03
Study of Related Work	■	■	■	■	■	■	■	■	
SA Writing	■								
SA Presentation	■								
Dissertation Writing				■	■	■	■		
Paper submission and writing	■	■	■	■	■	■	■	■	
Creation of Configuration Scenarios and Traffic Generators	■	■	■	■	■	■			
Model Evaluation and Result Analysis	■	■	■	■	■	■			
Master's Degree Defense									■

Questions?