Securing Multiprocessor System-on-Chip

Arnab Kumar Biswas and S. K. Nandy.
Department of Electronic Systems Engineering, Indian Institute of Science.

Motivation and proposed solutions

- Security issues are emerging as a serious problem in modern day MPSoCs.
- Attacks against these systems are becoming more critical and sophisticated.
- We have designed and implemented different hardware based solutions both at circuit level and system level of an MPSoC design.

Problem Statement at Circuit Level

- Presence of noise voltage in input signal coming from outside world can disturb normal circuit operation inside a chip causing false logic reception.
- If the disturbance is caused intentionally, the security of any chip may be compromised causing Glitch/Transient attack.

Proposed Input Receiver

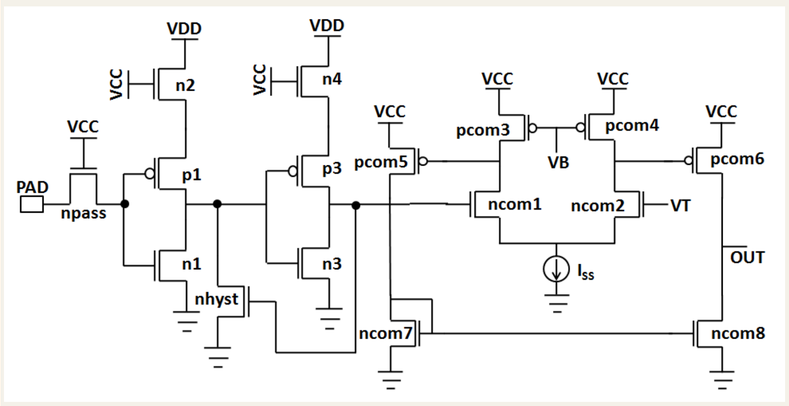

Figure 1

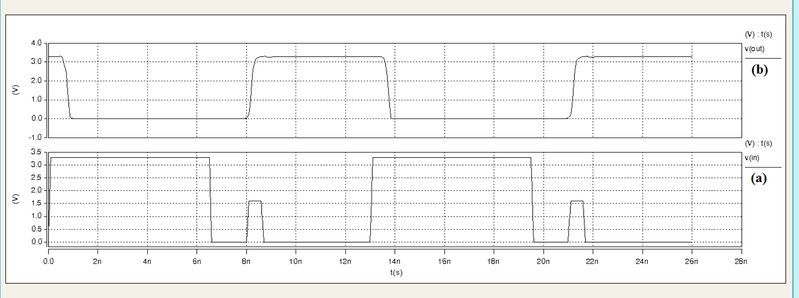

Figure 2: (a) Input voltage with noise pulse at logic zero, (b) Output voltage without any false peak.

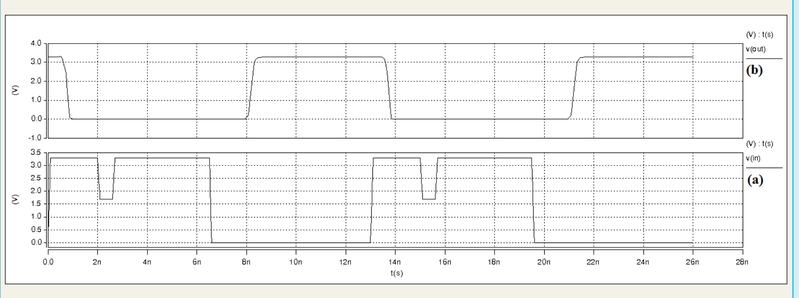

Figure 3: (a) Input voltage with noise pulse at logic one, (b) Output voltage without any false peak.

Table 1: Comparisons with prior works.

	Conventional receiver [5]	Receiver reported in [19], [20]	Proposed Receiver
Voltage range	1.8 V - 5 V	0.9 V - 5 V	0.9 V - 5 V
Technology	0.35 µm	0.35 µm	0.35 µm
V_{DD}	3.3 V	3.3 V	3.3 V
Amount of hysteresis	X	X	1.045 V
N_{ML}	0.7165 V	0.128 V	1.285 V
N_{MH}	1.15 V	2.3 V	3.06 V
Max. freq. of operation	80 MHz	50 MHz	500 MHz
Avg. power dissipation	15.5 mW	16.15 mW	9.2 mW

Problem at the System Level

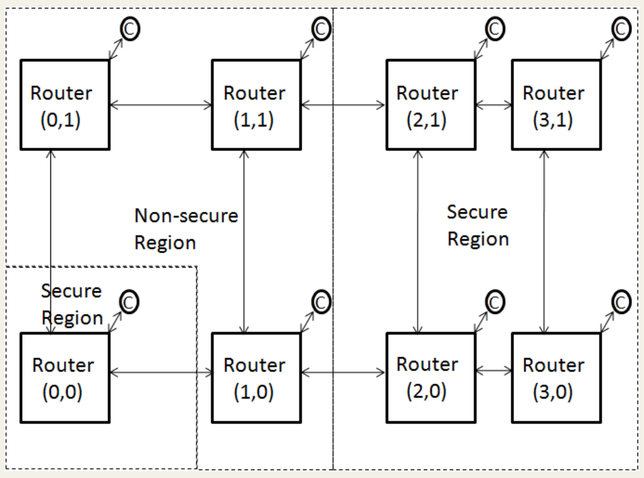

Figure 4: 2X4 NoC with two secure regions.

Effects of Router Attack Inside an NoC

- Sub-optimal routing and increased delay.
- Congestion and link overload.
- Deletion of nodes.
- Overwhelming critical node.
- Deadlock and Livelock.
- Unauthorized access to data.

Proposed Runtime Monitor

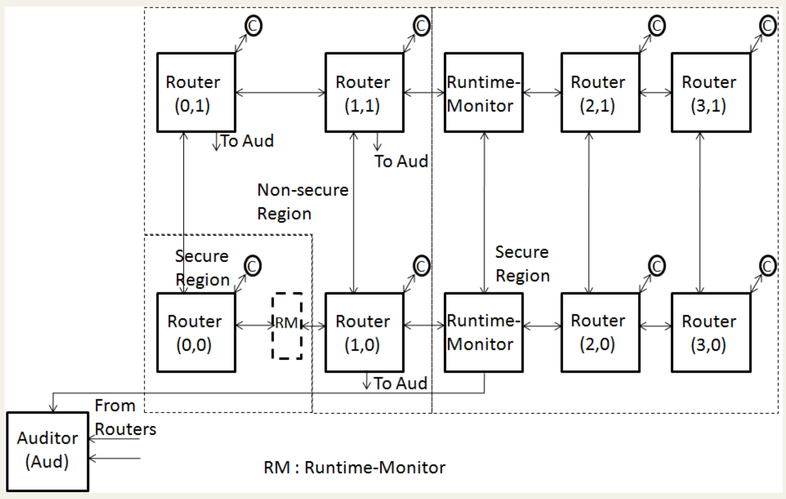

Figure 5: 2X4 NoC with two Runtime Monitors.

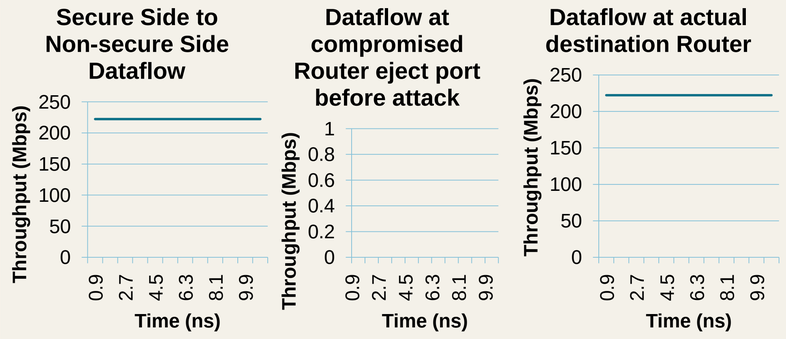

Figure 6: Dataflow during normal operation.

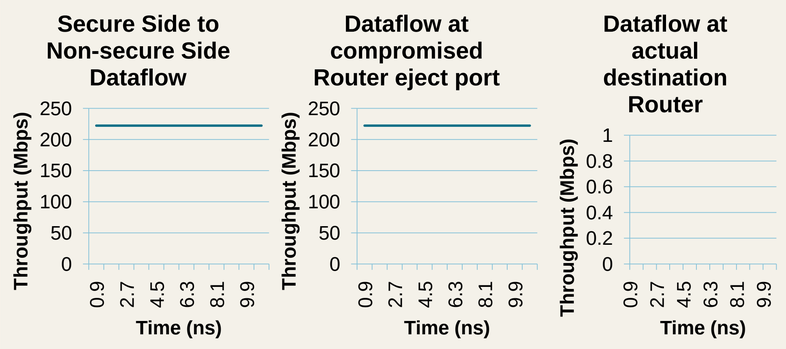

Figure 7: Dataflow after attack without Runtime Monitor in place.

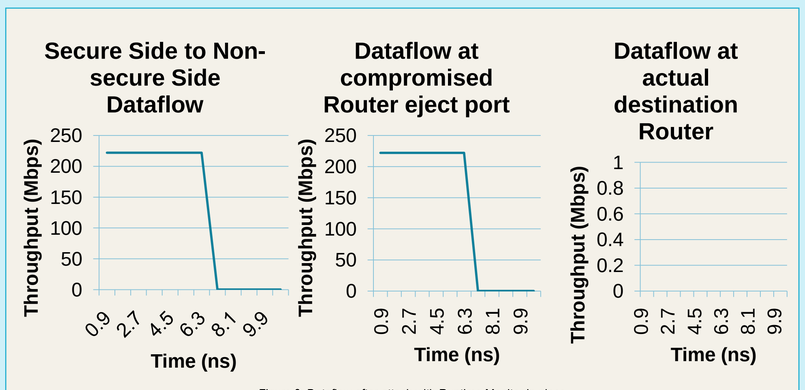

Figure 8: Dataflow after attack with Runtime Monitor in place.

Problem at the Application Level and Our Solutions

- Various software attacks are launched exploiting buffer overflow vulnerability.
- Buffer overflow is possible if writing to an unauthorized location in the memory is not prevented.
- We propose four access control mechanisms based on the Role Based Access Control (RBAC) Model.

Proposed Central, Hybrid, and Local Access Control

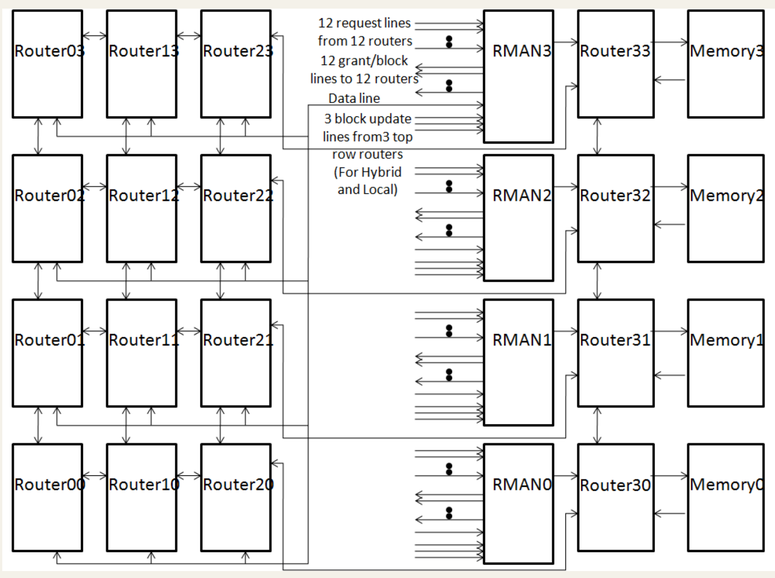

Figure 9: 4X4 NoC with four shared memories and four RMANs. Here RMAN denotes Resource Access Manager.

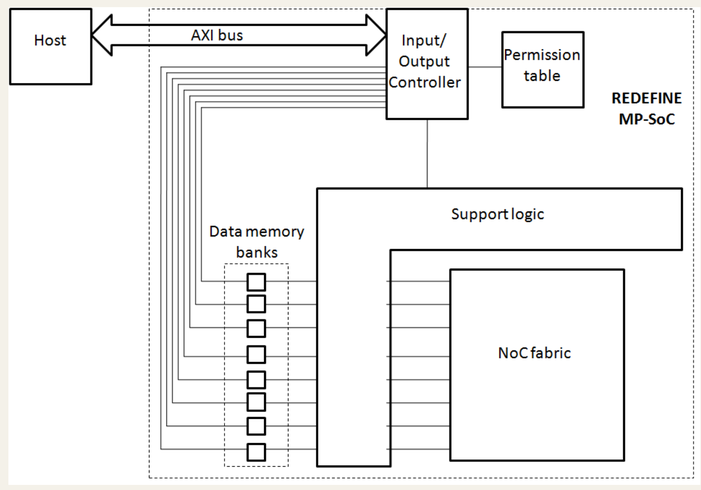

Figure 10: Modified Local access control mechanism in REDEFINE MPSoC.

Table 2: Comparisons with previous works.

	Our implementation in REDEFINE	[Diguet et al. 2007]	[Fiorin et al. 2008]	[Porquet et al. 2011]
Granularity of access control	Role based	PE based	Kernel/user per PE	Multiple software stack per PE
Router area	46477 µm^2	Not reported	126500 µm^2 [a]	Not reported
Operating frequency	625 MHz	Not reported	1 GHz [b]	Not reported

a: The number is obtained after taking (4 port router area + minimum NI area). Area is scaled down by 2 from the reported number to scale down from 130 nm to 65 nm technology node for proper comparison.

b: Frequency is scaled up by 2 from the reported number to scale down from 130 nm to 65 nm technology node for proper comparison.