Securing Multiprocessor System-on-Chip

By
Arnab Kumar Biswas
Department of Electronic Systems Engineering

Under guidance of
Prof. S. K. Nandy

CADL CDS

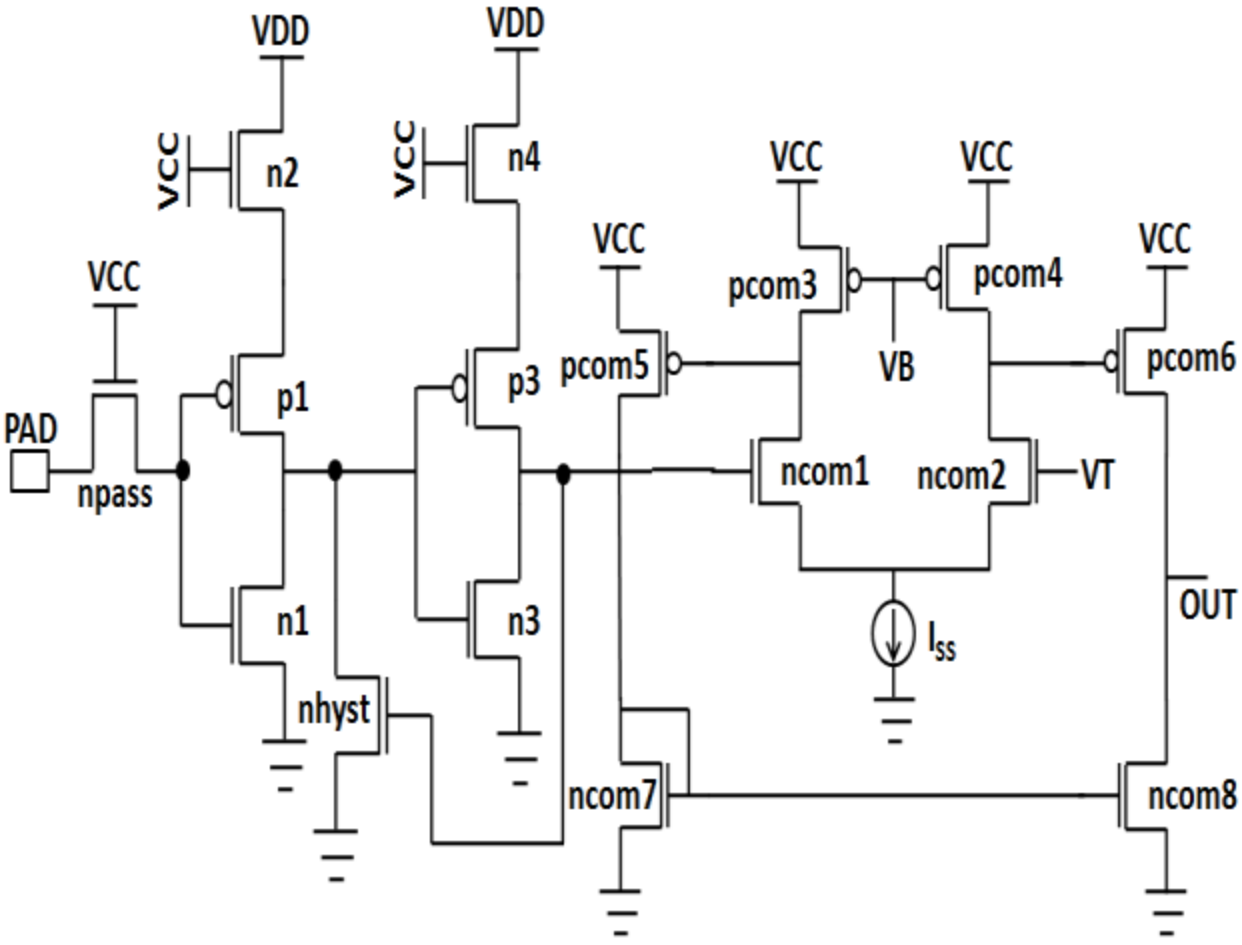
Motivation

- Now-a-days MPSOCs are pervading our day-to-day lives.
- Security issues are emerging as a serious problem.
- Attacks against these systems are becoming more critical and sophisticated.
- Novel solutions have to be proposed in order to defend against these attacks.

Proposed solutions

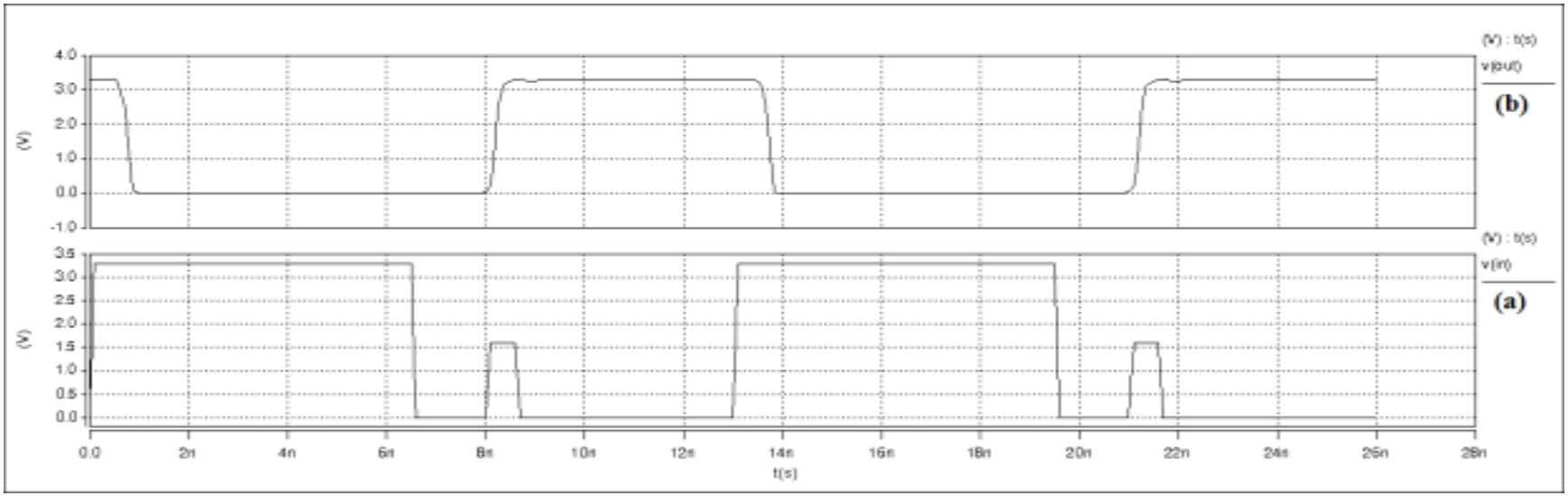
- We have designed and implemented different hardware based solutions to ensure security of an MPSoC.
- Security assisting modules can be implemented at different abstraction levels of an MPSoC design.
- We have proposed solutions both at circuit level and system level of abstractions.

Proposed Input Receiver



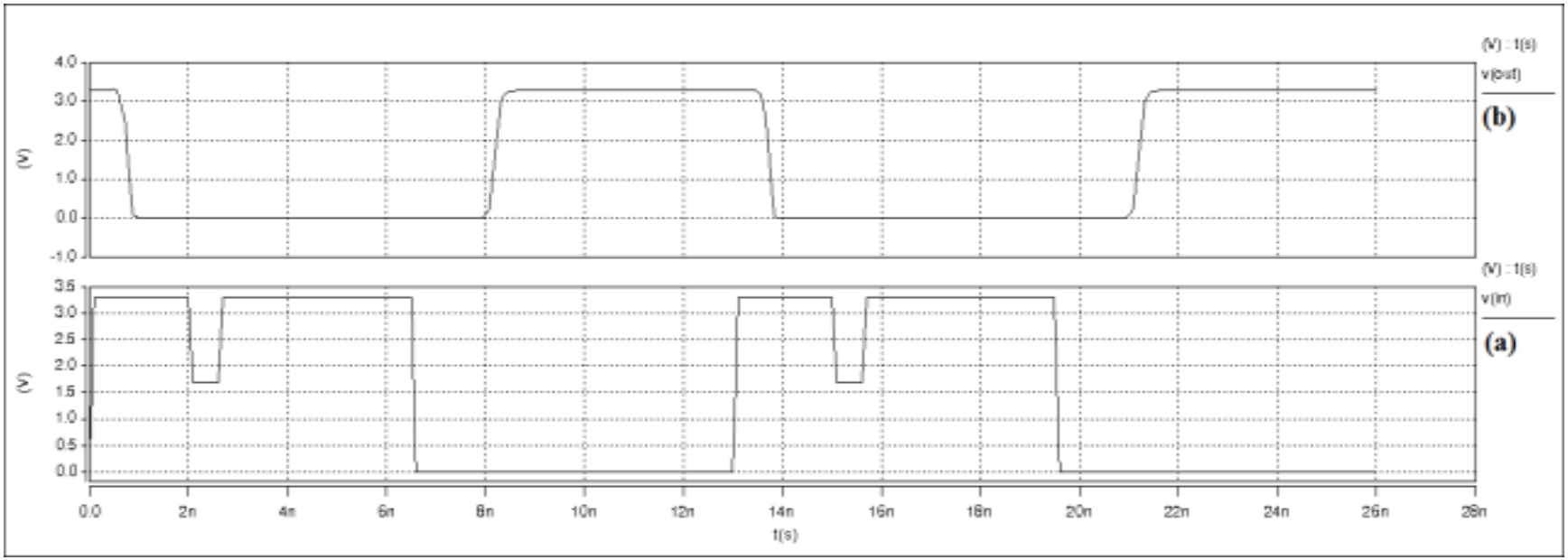
Arnab k. Biswas, “Wide Voltage Input Receiver with Hysteresis Characteristic to Reduce Input Signal Noise Effect,” *ETRI Journal. Vol. 35, No. 5, pp. 797-807, 2013.*

Circuit Performance in the Presence of Noise



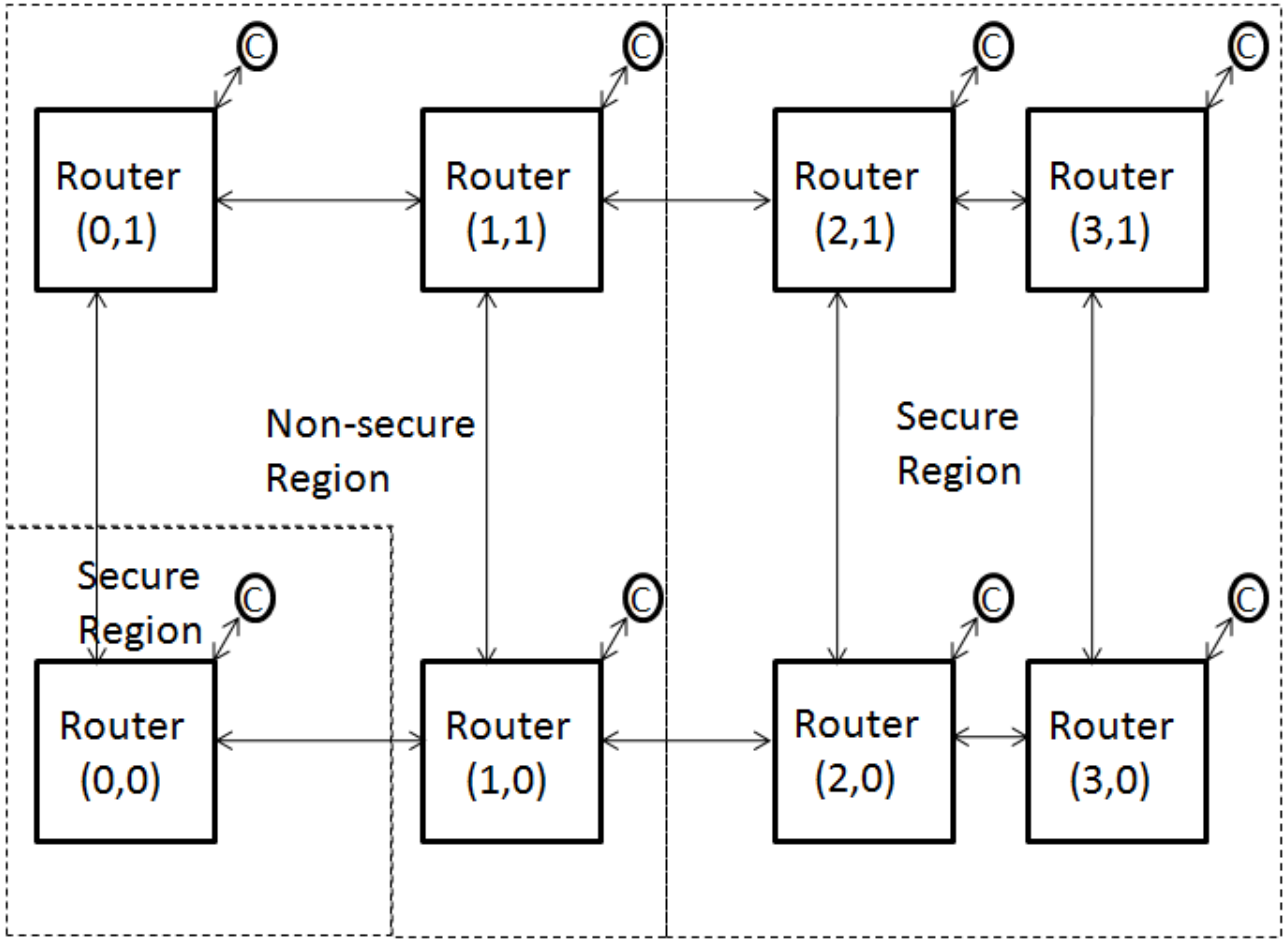
(a) Input voltage with noise pulse at logic zero, (b) Output voltage without any false peak

Circuit Performance in the Presence of Noise



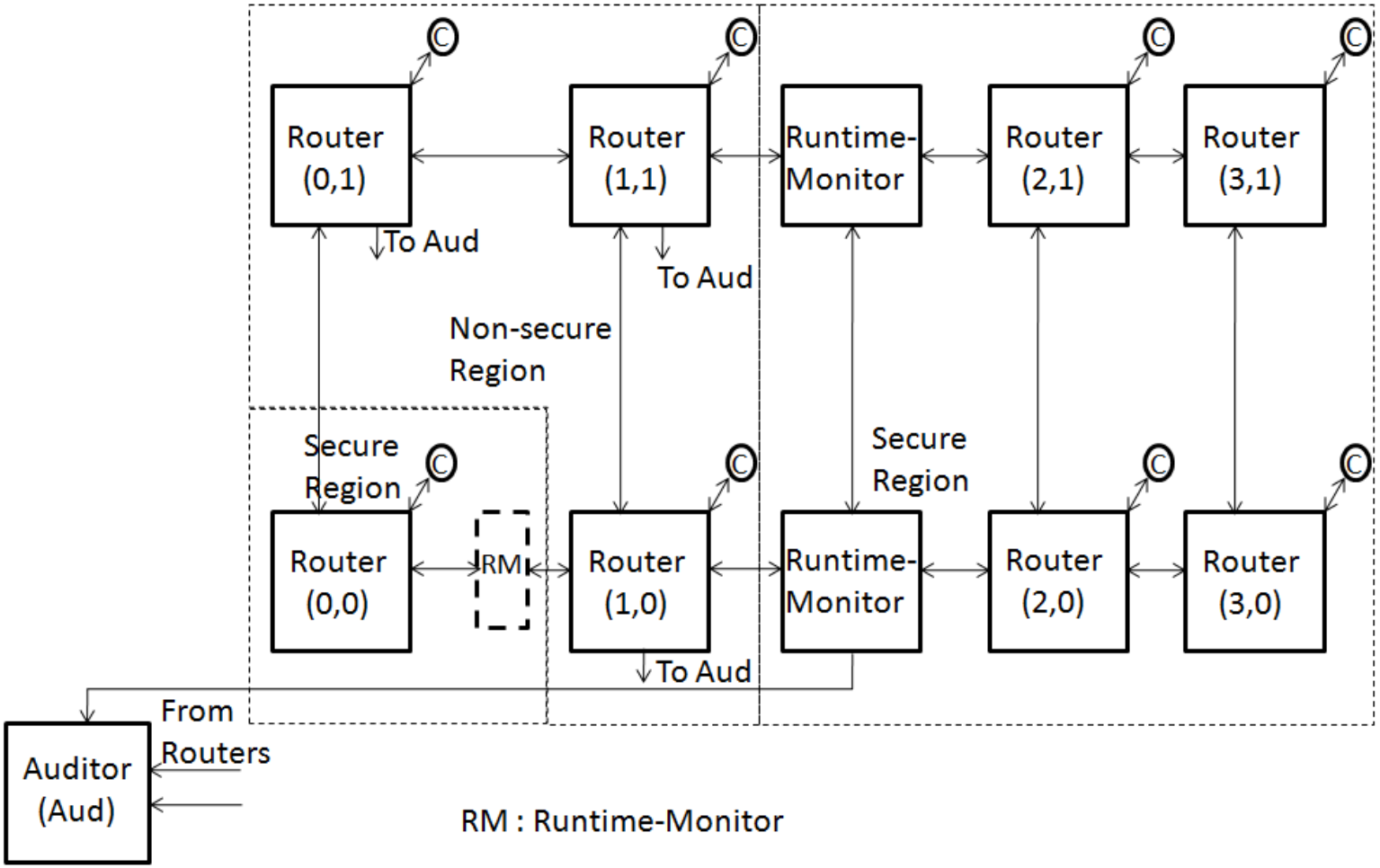
(a) Input voltage with noise pulse at logic one, (b) Output voltage without any false peak

Problem at system level



Arnab k. Biswas; S. k. Nandy; Ranjani Narayan, “Router attacks and their prevention in SoCs with multiple Trusted Execution Environments,” Work-in-progress, *DAC 2014, Design Automation Conference, San Francisco, USA, June 1-5, 2014.*

Runtime Monitor

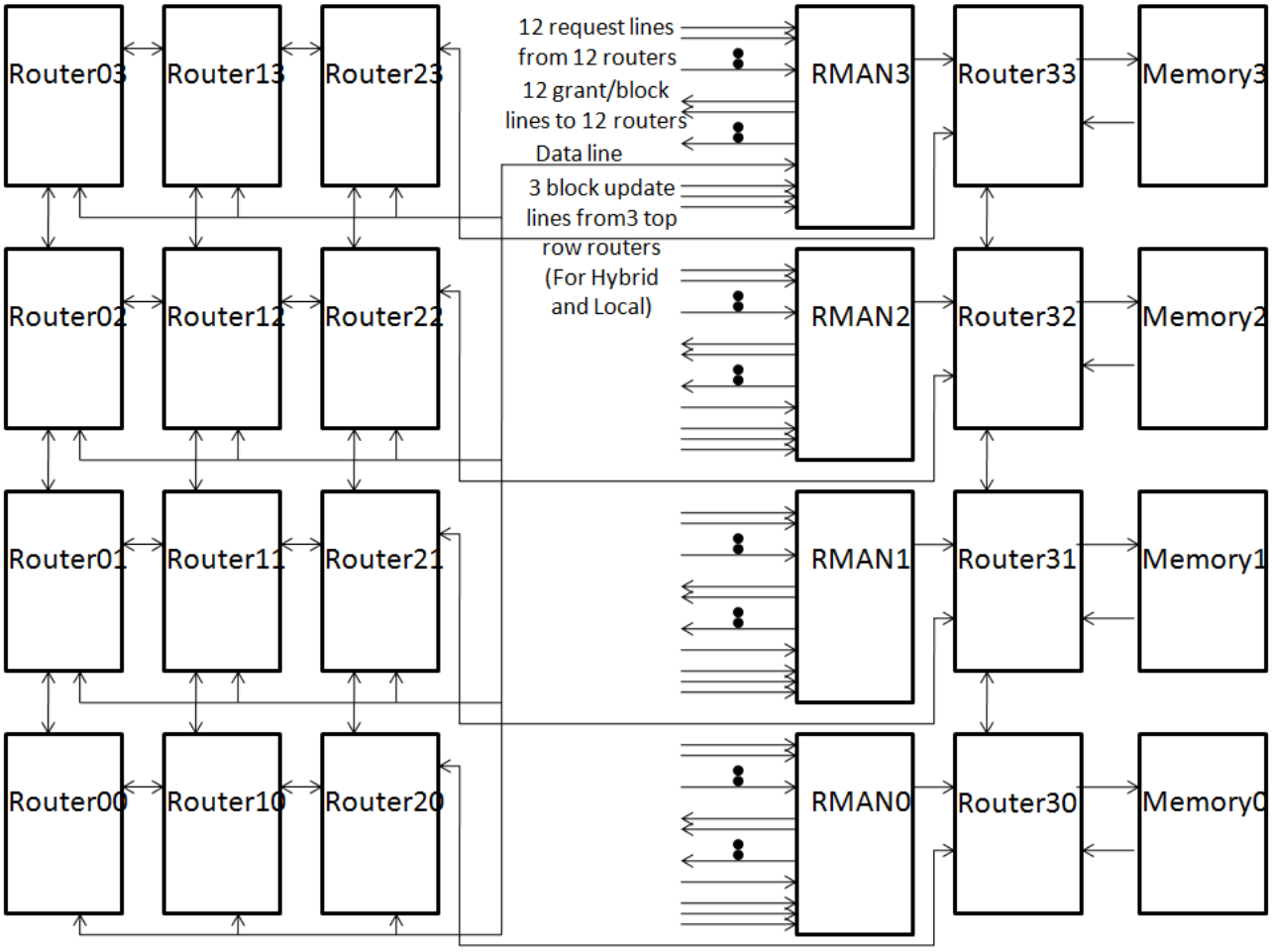


Problem at the application level

- 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.

Arnab k. Biswas; S. k. Nandy, “Role Based Shared Memory Access Control mechanisms in NoC based MP-SoC,” Nano Communication Networks, March 2016, Volume 7, pp. 46-64.

Central, Hybrid, and Local access control



Conclusions

- Different attacks targeted toward an MPSoC are considered and different security mechanisms are proposed to secure the MPSoC.
- A new input receiver with hysteresis characteristic that can operate at input voltage levels between 0.9 V and 5 V is proposed. The circuit can protect the MPSoC from false logic reception and glitch/transient attack.
- We have identified new attack scenarios (unauthorized access attack and mis-routing attack) in NoC routers. We have also proposed different countermeasures to protect from various ill effects of the routing table based attack.
- We have proposed four access control mechanisms based on the Role Based Access Control (RBAC) model. The proposed access control mechanisms prevent a number of software attacks.

References

[1] Arnab k. Biswas; S. k. Nandy, “Role Based Shared Memory Access Control mechanisms in NoC based MP-SoC,” Nano Communication Networks, March 2016, Volume 7, pp. 46-64. http://dx.doi.org/10.1016/j.nancom.2015.11.002.

[2] Arnab k. Biswas; S. k. Nandy; Ranjani Narayan, “Network-on-Chip Router attacks and their prevention in MP-SoCs with multiple Trusted Execution Environments,” *IEEE CONECCT 2015, IEEE International Conference on Electronics, Computing and Communication Technologies, Bangalore, India, July 10-11, 2015*.

[3] Arnab k. Biswas, S. Nandy, and R. Narayan, “Router attack toward noc-enabled mpsoc and monitoring countermeasures against such threat,” Circuits, Systems, and Signal Processing, October 2015, Volume 34, Issue 10, pp. 3241–3290. [Online] Available: http://dx.doi.org/10.1007/s00034-015-9980-0.

[4] Arnab k. Biswas; S. k. Nandy; Ranjani Narayan, “Router attacks and their prevention in SoCs with multiple Trusted Execution Environments,” Work-in-progress category, *DAC 2014, Design Automation Conference, San Francisco, USA, June 1-5, 2014*.

[5] Arnab k. Biswas, “Wide Voltage Input Receiver with Hysteresis Characteristic to Reduce Input Signal Noise Effect,” *ETRI Journal.* Vol. 35, No. 5, pp. 797-807, 2013.

Thank you