Learning-Based High-Performance, Energy-Efficient, and Secure Interconnection Design Framework

Researchers at the George Washington University have invented a novel network-on-chip framework, named TSA-NoC, which significantly improves on-chip security. The invented framework also minimizes the latency and cost of security techniques for simultaneously improving system-level performance and power.

As the market for parallel computing is growing rapidly, the number and complexity of shared resources (processors, memory, sensors, etc.) is increased. Network-on-chips (NoCs) are playing a critical role in computing systems as the standard interconnect fabric solutions for connecting these shared resources. However, NoCs are vulnerable to attacks that steal sensitive data or damage software/hardware systems. Existing techniques protect NoCs by detecting and isolating the attacker nodes and malicious components. Unfortunately, conventional detection techniques occasionally cause false/miss detection, which leads to penalties in terms of additional power consumption and increased network latency. Moreover, conventional isolation techniques limit the network throughput, forbid communication via certain channels, and detour the packets to avoid infected regions, thus inevitably incur performance degradation.

Our researchers have proposed a machine learning-based secure and efficient on-chip communication framework, called TSA-NoC. Specifically, the proposed framework uses machine learning algorithms, such as an artificial neural network (ANN), for runtime attack detection with higher accuracy. Further, a learning-based attack mitigation method, using deep reinforcement learning, is proposed to isolate the malicious components as well as minimizing network latency and maximizing energy-efficiency.

We believe TSA-NoCs are a powerful innovation and has shown immense promise to support multicore parallel computing and other hot areas, ranging from IoT devices, mobile processors, chip multiprocessors (CMPs), to supercomputers and data centers, with enormous commercial potential in a growing number of environments.

Applications:

· On-chip communication for parallel computing systems (multi-core CPU, GPU, FPGA, TPU, etc.)

Advantages:

- The invented TSA-NoC simultaneously tackles the urgent security challenge along with major limitations of conventional computer architecture designs including performance and energy efficiency.

- Experiment shows the innovation can achieve 97% attack-detection accuracy. Moreover, the proposed attack mitigation method achieves 67% improved energy-efficiency and 28% reduced network latency, compared to state-of-the-art NoC security techniques.

- The key innovations are scalable and can be implemented to nearly any current and future parallel computing world including mobile computing, IoT, multicore processors, embedded systems, servers, cloud computing, data centers, machine learning, etc.

**Inventors**

**Prof. Ahmed Louri**

**Ke Wang**