Problems and Challenges of Emerging Technology

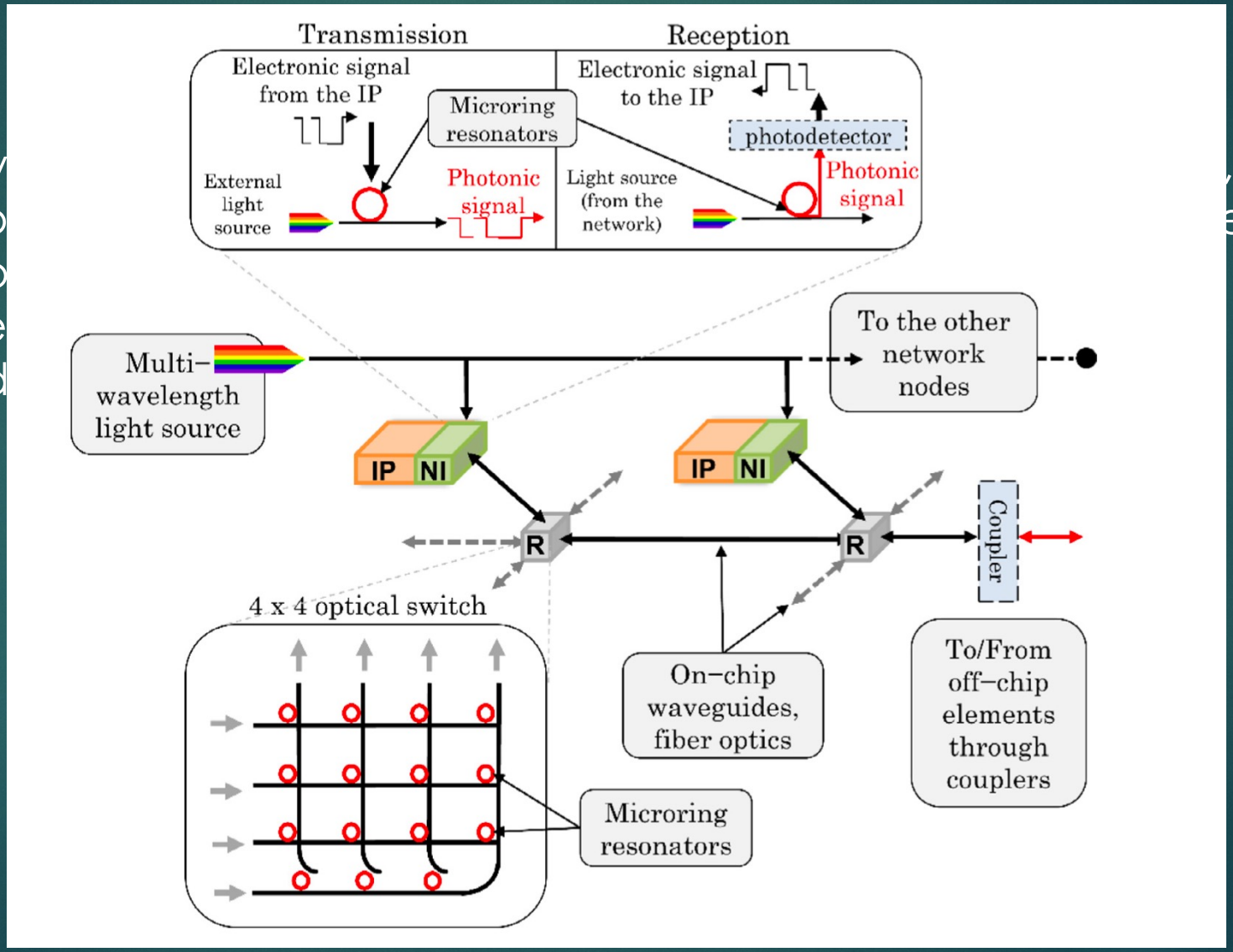
YAO XIAO, 2019180015

Networks–on–Chip

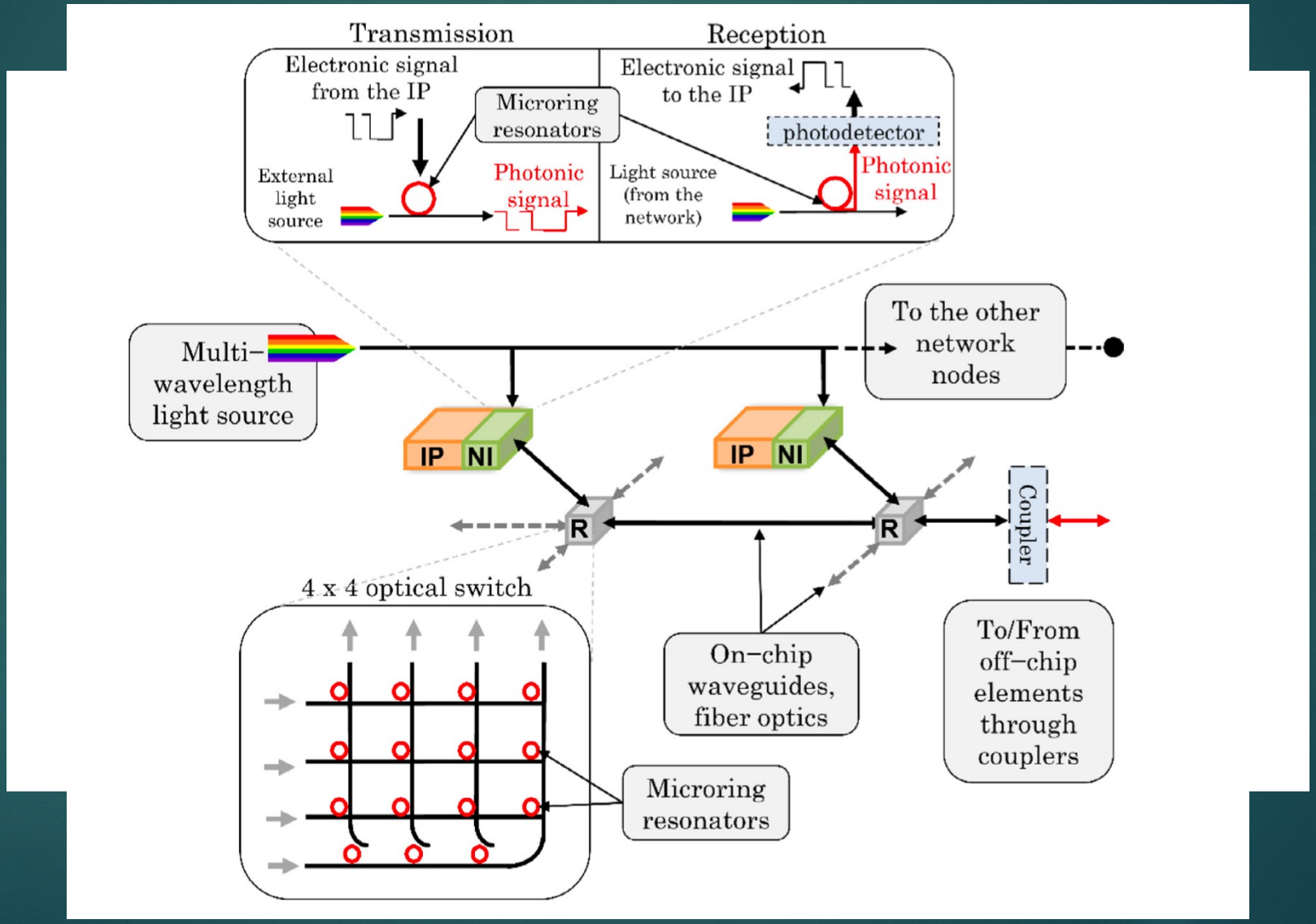
- The advancement of technology makes it possible to stack many different cores with the same or different processing elements, memory, intellectual property (IP), etc. in a multi-layer single chip. bottleneck. In fact, conventional buses cannot keep up with the bandwidth and complexity of recent multiprocessors or multiprocessor chips.
- The essence of the network-on-chip (NoC) paradigm is that when extended to this heterogeneity and/or the dimensionality of the core, the concept of on-chip interconnection has changed from a traditional bus to a complex network. Part of the potential of the NoC concept lies in the complete separation of computing and data transmission

Networks-on-Chip

- When sw
  many co
  technolo
  response
  bandwid



Networks–on–Chip



Networks-on-Chip
Challenges: High throughput capability

- The pursuit of high-efficiency NoC with high throughput is the main reason for the exploration of emerging technology NoC. From this perspective, the hybrid approach is a viable solution. For example, the combination of conventional NoC and optical NoC is very interesting. Conventional NoC can handle local and repeated transactions, while ONoC can handle remote transactions or transactions with higher throughput. The same method can be applied to WiNoC. WiNoC can be used to connect multiple islands of PE locally connected with traditional NoC. In addition, the new substrate material can provide higher yields while having a reasonable cost of power consumption.

Networks-on-Chip
Challenges: Security

- For the NoC paradigm, many aspects must be reconsidered, and the future SoC is most likely to use NoC as an interconnection infrastructure. As a first attempt, Fiorin et al. [1] discussed NoC security challenges through existing work. The first is how to use NoC to protect SoC, and the second is how to authenticate the SoC security mechanism based on secure NoC.
- Work in this area is focused on using NoC to protect the system. However, newer methods assume that in the case of a NoC purchased by a third party, the NoC itself may be the source of the threat.

Cyberattack

- Safe operation in cyberspace is a global information flow network associated with the Internet, which is vital to the continued operation of the international economy and many other areas. The Internet is an extraordinary tool for many purposes. It is also vulnerable to attacks by hostile intruders, whether it is to spread misinformation, damage important infrastructure or steal valuable data. Most of these malicious activities are carried out by individuals or groups of people who try to enrich themselves or influence public opinion. However, it is becoming more and more obvious that government agencies that often cooperate with some of them are using cyber weapons to weaken the enemy by sowing mistrust or undermining key institutions, or to enhance their defense capabilities by stealing military-related technical knowledge.

Cyberattack Challenges

- It is not difficult to imagine violent skirmishes erupting in cyberspace, for example, if a cyber attack causes the collapse of critical infrastructure.

Cyberattack Challenges

- Cyberspace is only regarded as an area of its own. Although the introduction of cyber weapons instead of nuclear or conventional ammunition is fertile ground for the implementation of regulatory measures, it can be said that these measures are similar to arms control. This is not a new challenge, but a challenge that has become more and more urgent with the development of technology. For example, when will such a digital attack paralyze the critical information systems of other countries?