Выявление угроз и проектирование безопасной архитектуры сети на кристалле

Загартдинов Булат

руководитель отдела исследований, НТЦ «Вулкан»

аспирант, НИУ «МЭИ»

История возникновения

1980-е

Общая шина

Единая системная шина (ISA) обслуживала и транзакции памяти, и медленные устройства ввода-вывода

1990-е

Разделение шин по назначению

Единая системная шина стала бутылочным горлышком и была разделена на несколько шин по назначение и скоростям (Back/Front Side Bus, Advanced System/Peripheral Bus)

2000-е

Матричная коммутация

Разделяемая шина сменились высоко-производительными интерфейсами на базе матричных коммутаторов и соединений точка-точка (crossbar, peer-to-peer)

2010-е

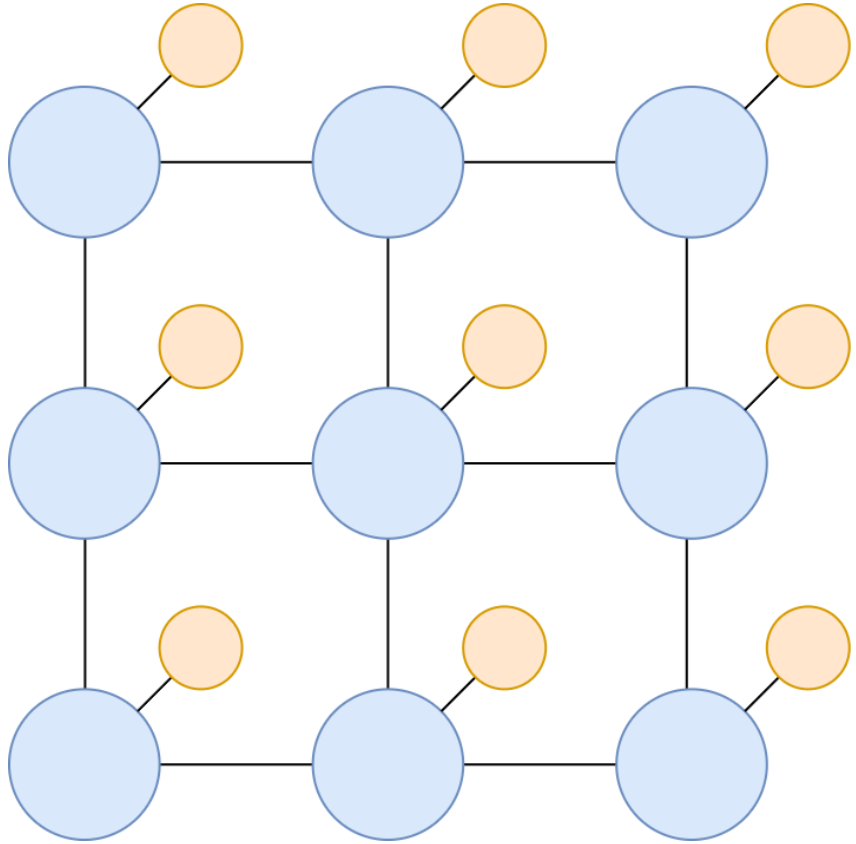
Сети на кристалле

Матричные коммутаторы стали занимать слишком большую площадь кристалла и потреблять избыточную энергию

Архитектура

Основные компоненты:

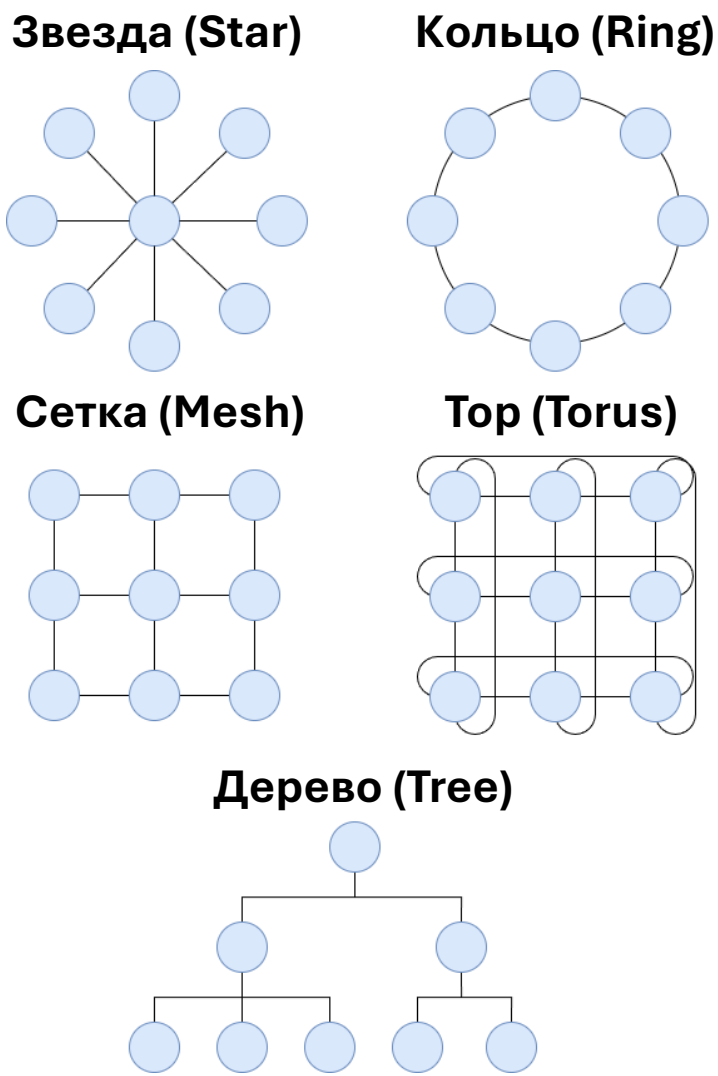
- Сетевые интерфейсы (Network Interface, NI)
- Маршрутизаторы (Routers)
- Каналы связи (Links)
- Конечные точки (Endpoint)



Сеть на кристалле с топологией сетка (mesh)

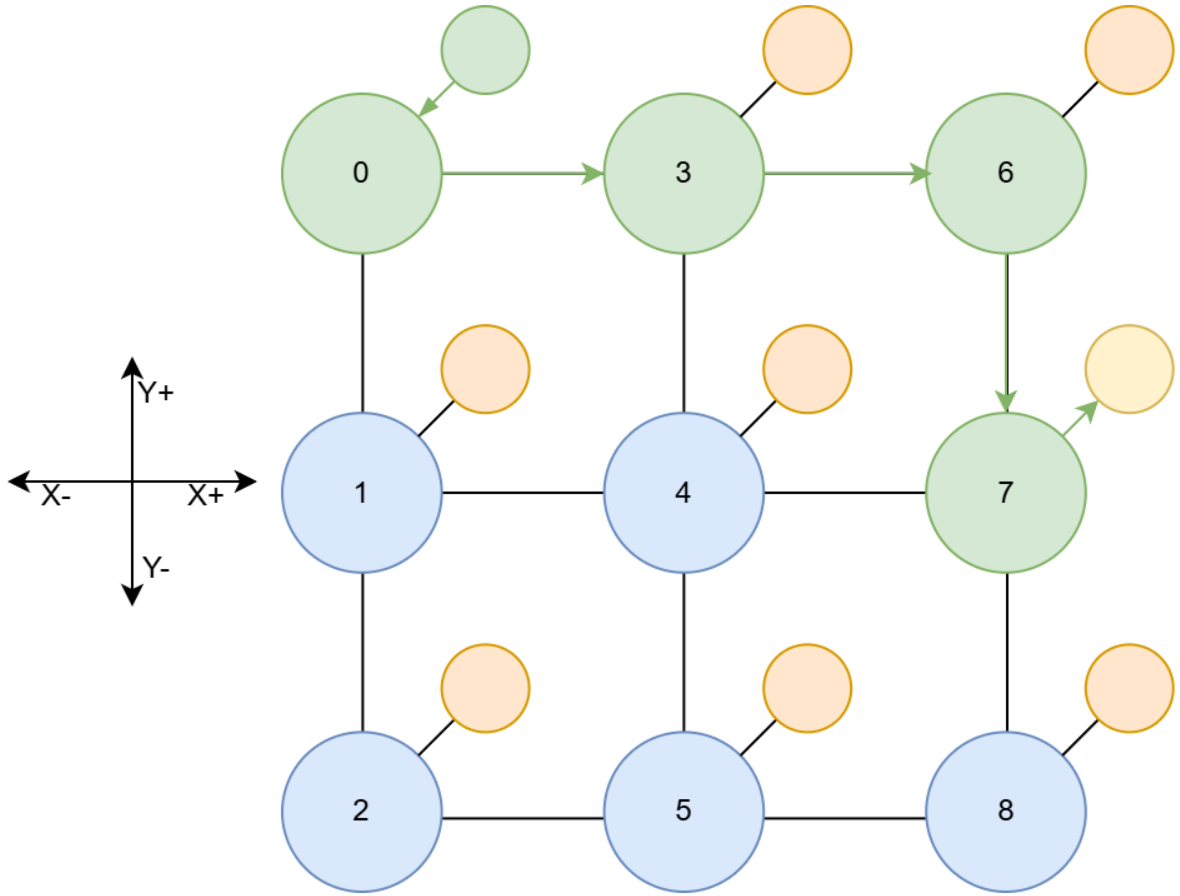
Топология

- Сетка (Mesh) – узлы соединены в прямоугольную решетку
- Top (Torus) – сетка, где крайние узлы соединены друг с другом (закольцованы)
- Кольцо (Ring) – простая последовательная цепочка
- Дерево (Tree) или звезда (Star) – иерархическая структура



Маршрутизация

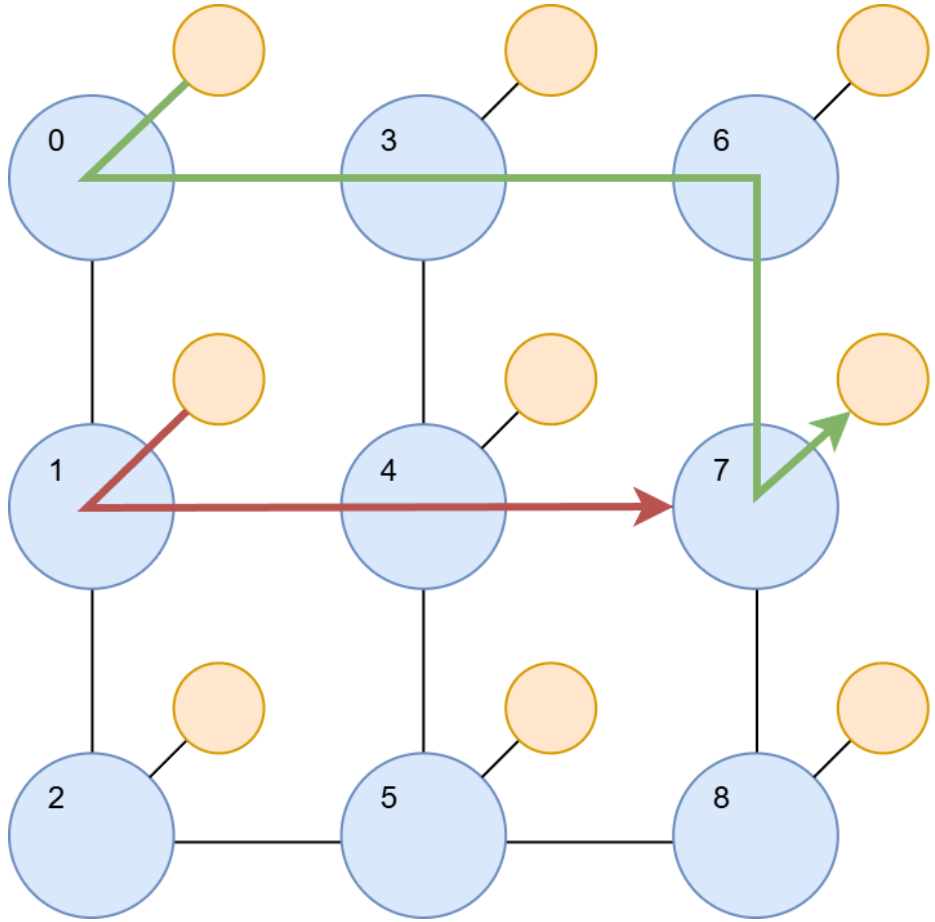
- Детерминированная (Deterministic) – путь между узлами неизменен
- Адаптивная (Adaptive) – путь зависит от состояния соседних маршрутизаторов
- Статическая (Source routing) – путь прописывает узел-отправитель



XY маршрутизация

Коммутация

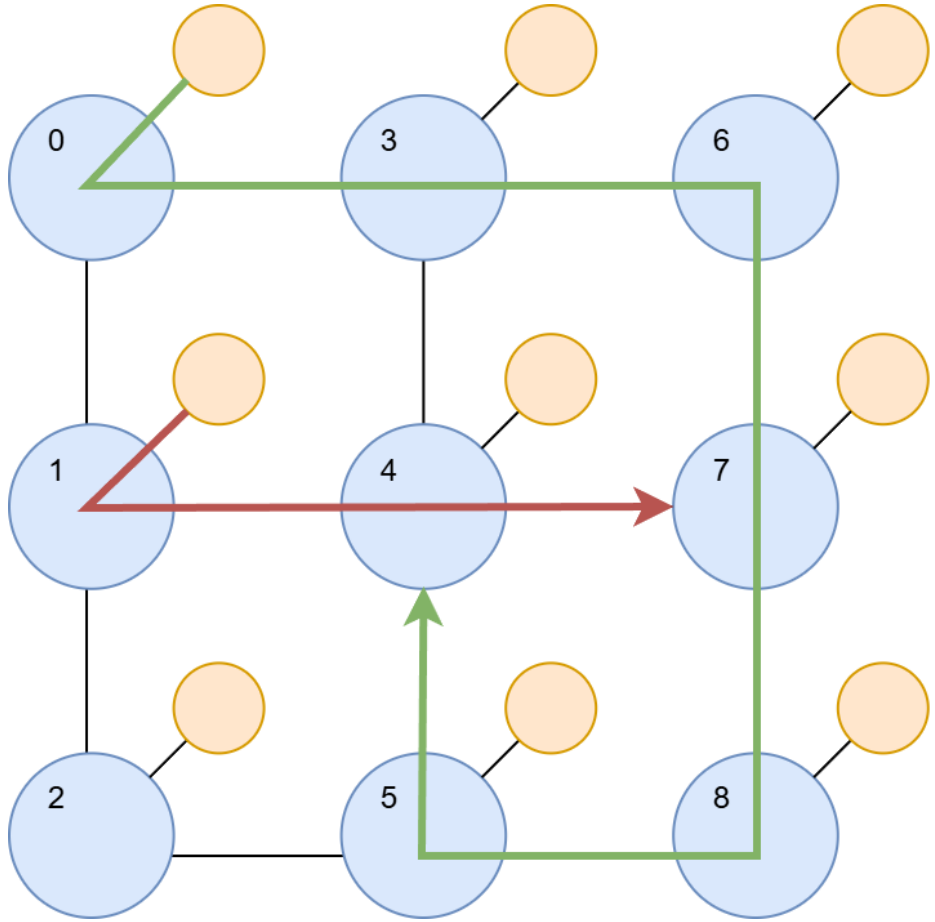
- Хранение и пересылка (Store-and-Forward)
- Сквозная коммутация (Virtual Cut-Through)
- Коммутация по принципу червоточины (Wormhole)



Wormhole коммутация

Проблемы

- Взаимная блокировка (Deadlock)
- Живая блокировка (Livelock)
- Потеря пакетов (Packet Loss)
- Когерентность кэшей (Cache Coherence) для многоядерных и гетерогенных систем



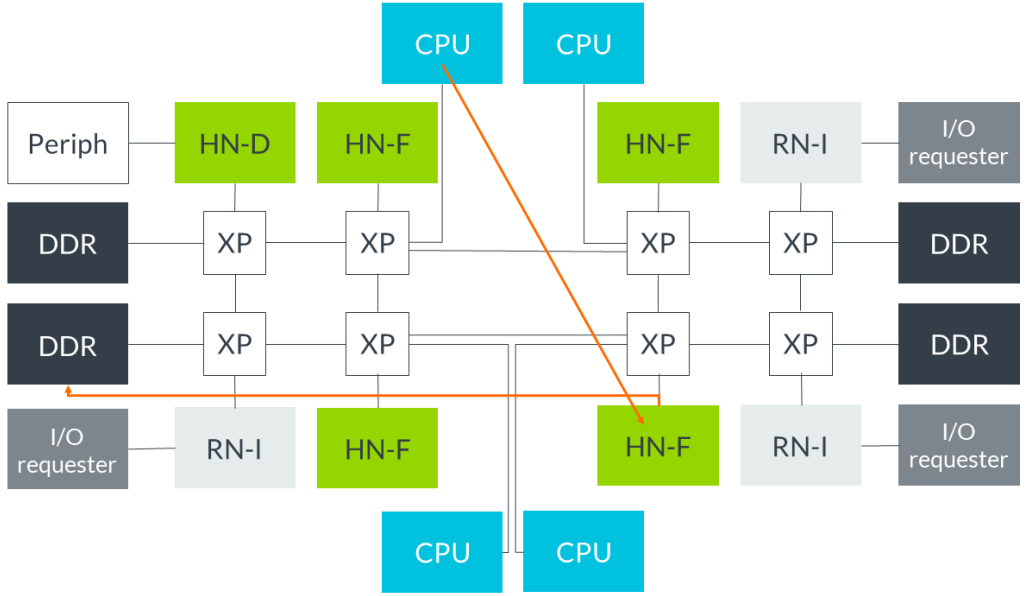
Взаимная блокировка

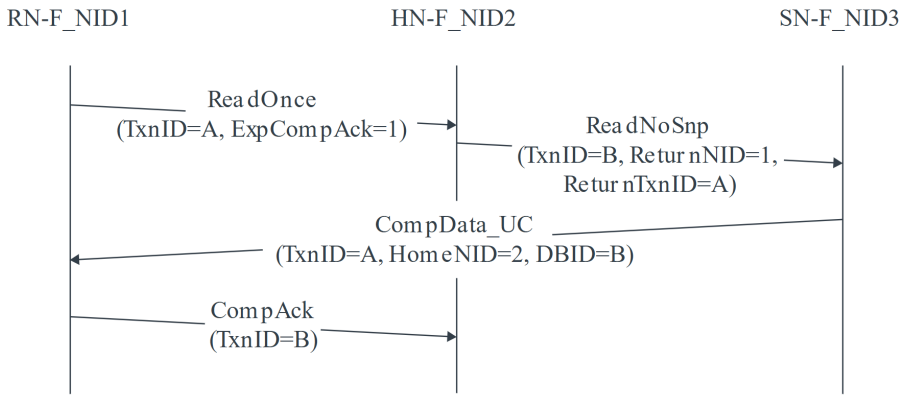
ARM Coherent Hub Interface

- Спецификация протокола обмена данными в сети на кристалле обеспечивающего когерентность кэш-памяти
- Однозначно не определяет используемые топологию, протоколы маршрутизации и коммутации, однако предъявляет к ним определенные требования:
  - Поддержка кредитного управления потоком (Credit-based Flow Control) на канальном уровне
  - Минимизация задержек и поддержка виртуальных каналов (Virtual Channels) маршрутизаторами
  - Соблюдение приоритетов (QoS) и порядка пакетов
  - Уникальная адресация в рамках одного кристалла (NodeID и SAM)

ARM Coherent Hub Interface

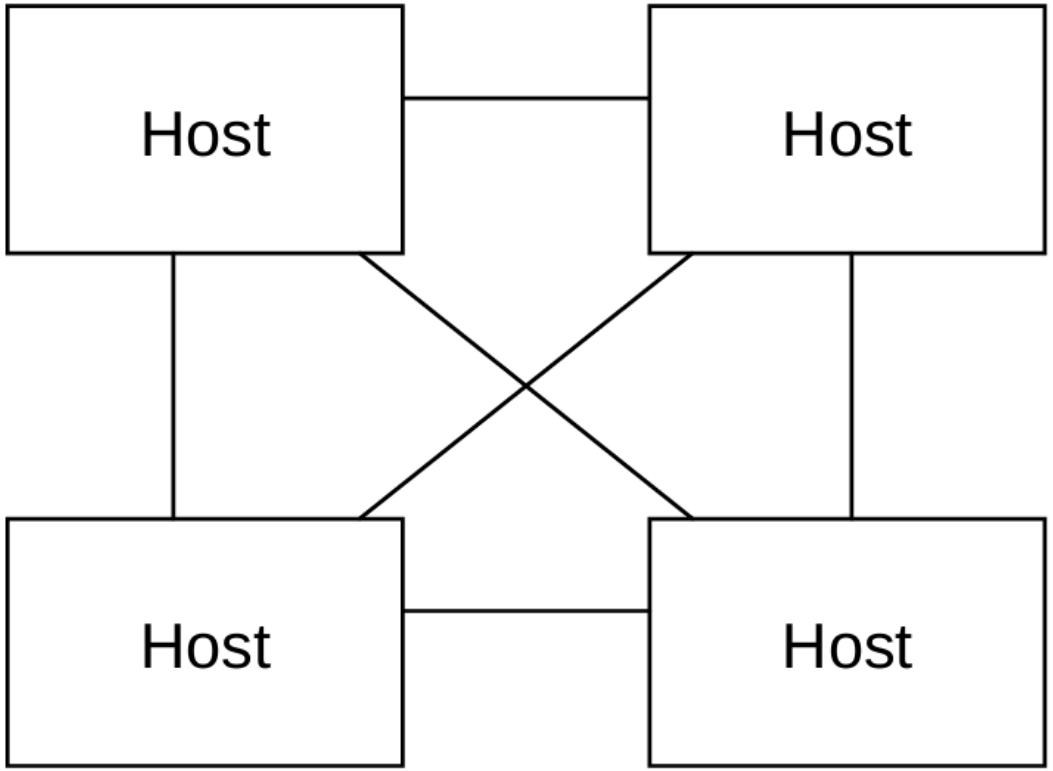
- Конечные точки разбиты на типы
  - HN – точка синхронизации кэш-памяти
  - MN – маршрутизаторы
  - RN – инициатор запроса
  - SN – контроллеры памяти и периферии
- и классы
  - HN-I – ввод/вывод
  - HN-F – полная когерентность
  - HN-D – синхронизация TLB кэшей





ARM CHI Chip-to-Chip (C2C)

- Поддерживает передачу через межкристальный транспорт (например UCIe или CXL для микросхем)
- Использует шлюз для подключения к другим кристаллам (NodeID Remapping)



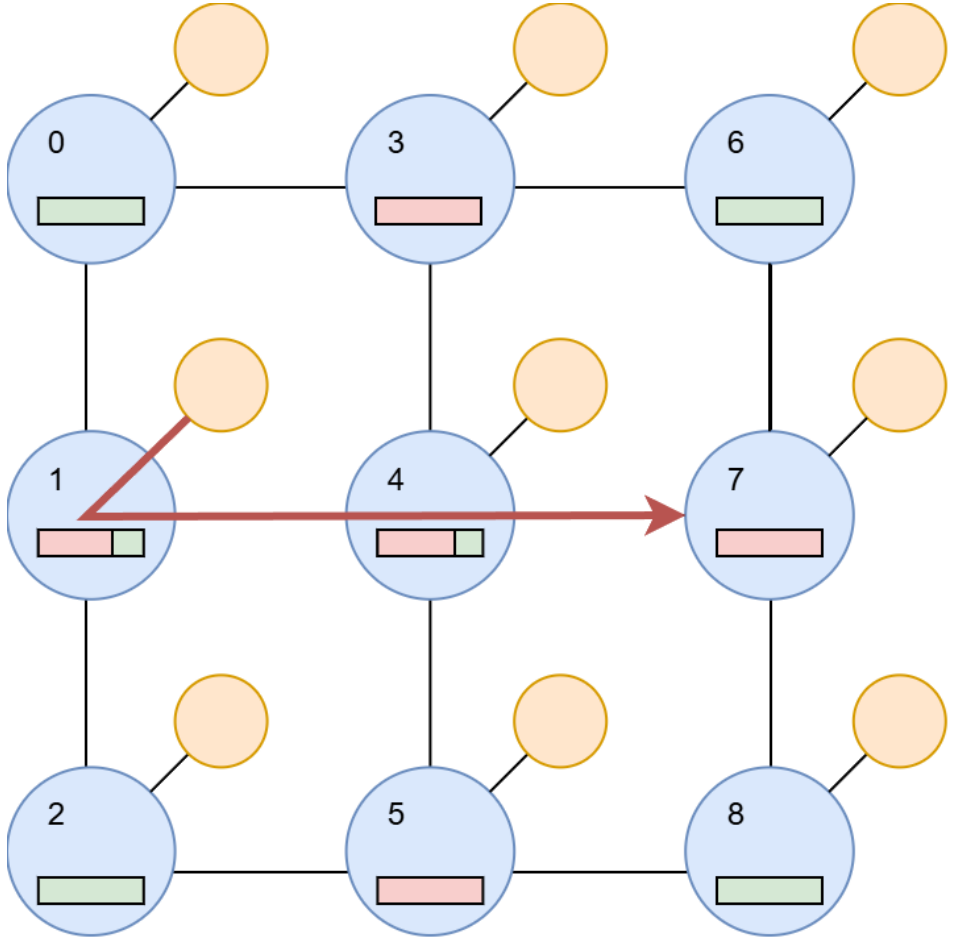
Example of four chips in a fully connected topology

Угрозы для сетей на кристалле

- Атака отказ в обслуживании на элементы или всю сеть на кристалле
- Подмена и перехват данных
- Атаки по сторонним каналам

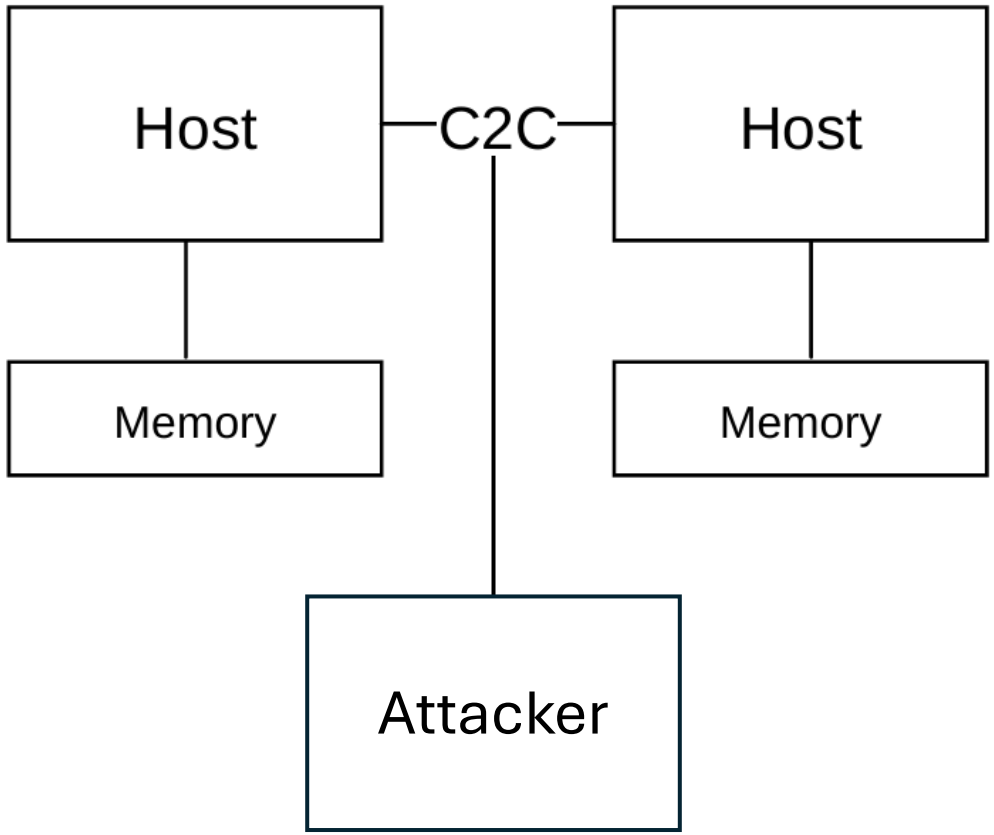
Атака отказ в обслуживании

- Переполнение буферов маршрутизаторов и конечных точек мусорными пакетами
- Блокировка трафика на уровне протокола
- Эксплуатация недостатков маршрутизации для создания петель в трафике



Подмена и перехват данных

- Через внесенные элементы (например через атаку на цепочку поставок)
  - Вредоносный маршрутизатор и/или функциональные блоки
  - Контактное подключение
- Через активное воздействие путем
  - Изменения в таблице маршрутизации
  - Манипуляции в протоколе когерентности



Атаки по сторонним каналам

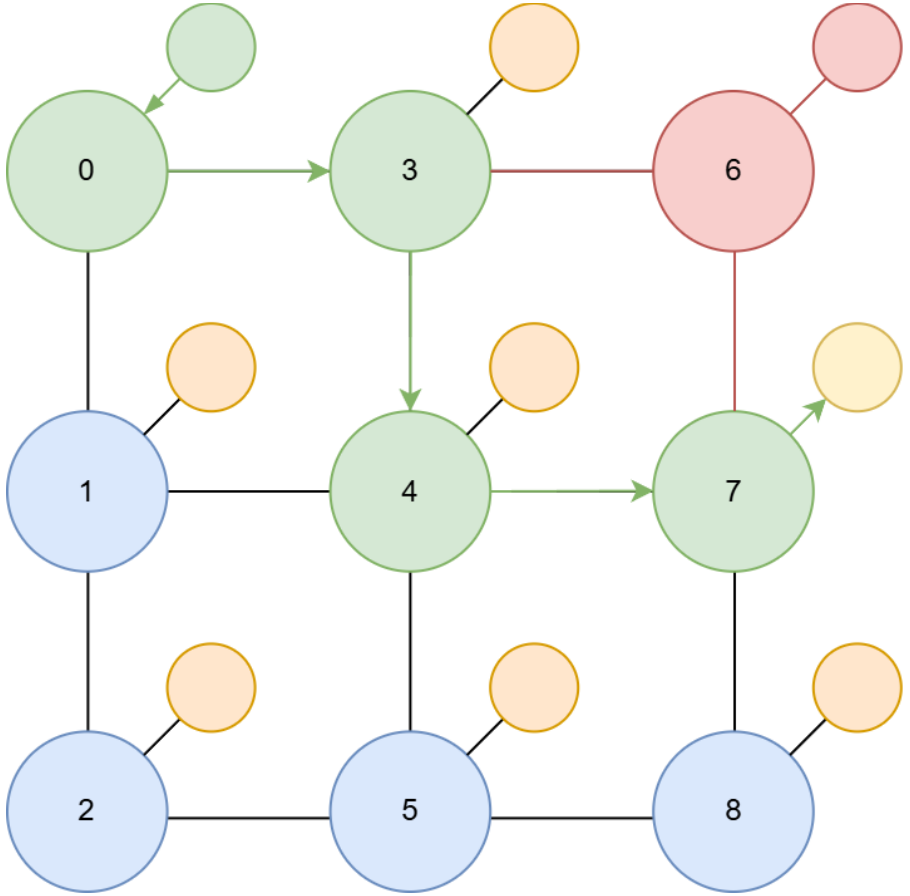
- Атаки с оценкой временных задержек
  - На основе конфликта за разделяемые аппаратные ресурсы (кэш-память, каналы связи)
  - На основе неоднородного доступа к памяти (необходимо иметь возможность прямого измерения времени выполнения операций целевого функционального блока)
- Физические атаки
  - Атаки на основе электромагнитного излучения
  - Анализ энергопотребления

Механизмы защиты

- Изоляция неисправных узлов
- Разделение трафика на домены безопасности
- Унифицированный доступ к памяти
- Зашумление трафика
- Разделение и мониторинг ресурсов памяти системы
- Схемы аттестации
- Шифрование канала

Изоляция неисправных узлов

- Анализ ошибок узлов
- Выключение из сети в случае накапливания предельного уровня ошибок
- Пример: Link Health Monitoring в UCIe

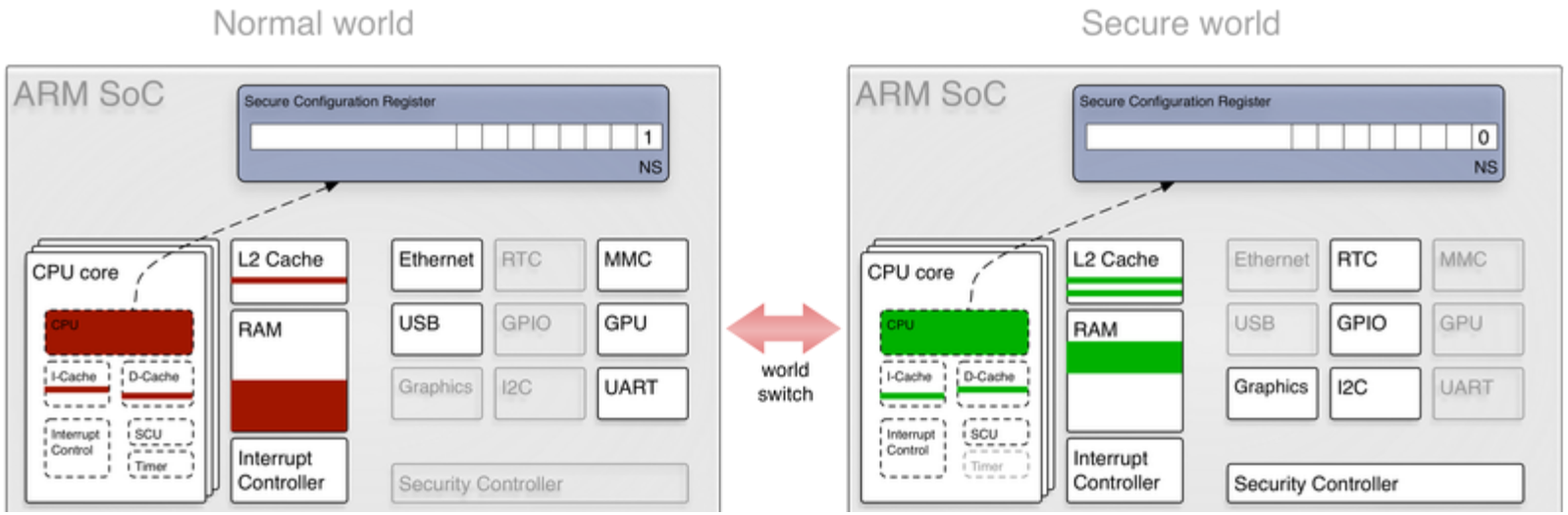


Защита от атак по сторонним каналам

- Унифицированный доступ к памяти
  - Время доступа к ресурсам сводится к единому за счет искусственных задержек в выполнении операций
  - Приводит к серьезной деградации по производительности
  - Программная реализация эффективна только относительно других функциональных блоков
- Зашумление трафика
- Разделение и мониторинг ресурсов памяти
  - Например программное управление ресурсами памяти в memory system resource partitioning and monitoring (MPAM)

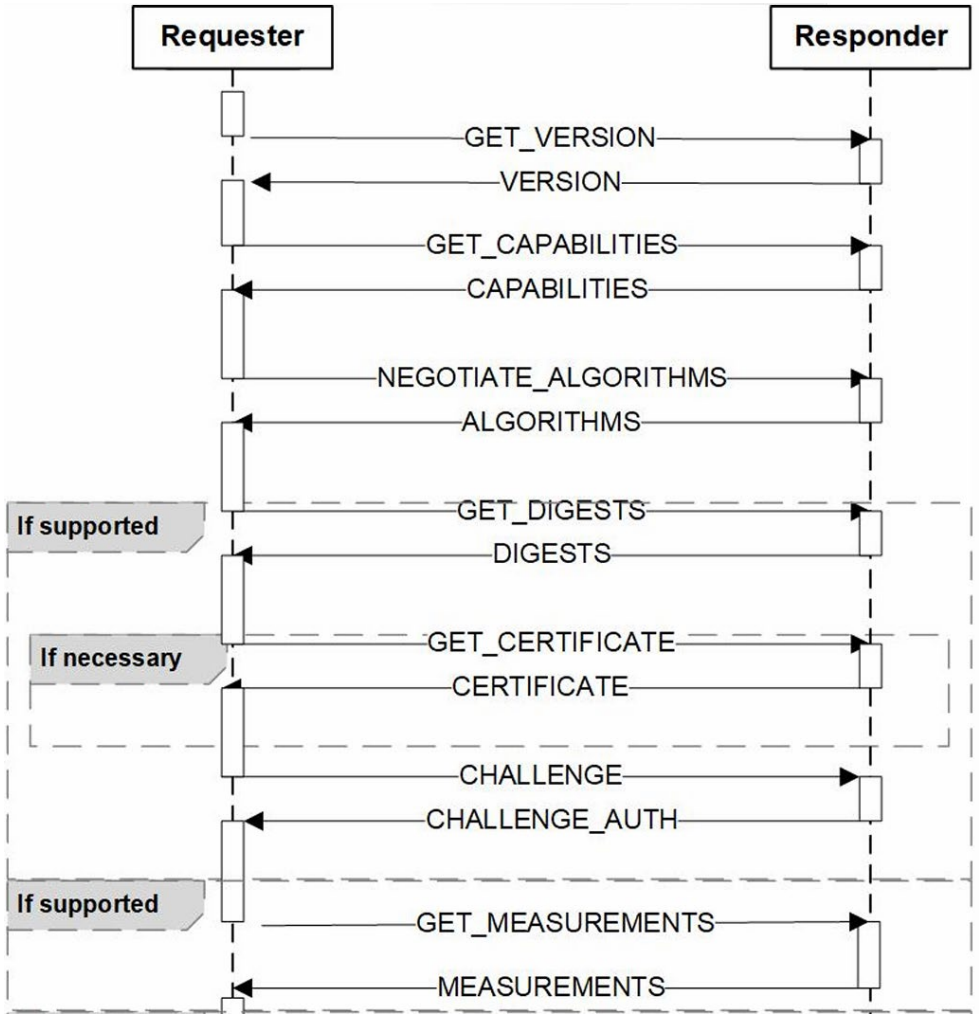
Разделение трафика на домены

- Изоляция контекста функциональных блоков доменами безопасности
  - Такой принцип используется для технологии ARM TrustZone
  - Может привести к усилению атак по сторонним каналам на основе конфликтов за каналы связи



Схемы аттестации и шифрование канала

- Метод основан на использовании схем аттестации и алгоритмов обмена ключами
- Подробно описан в открытой спецификации DMTF Security Protocol and Data Model
- Пример: Component Measurement and Authentication и Integrity and Data Encryption в UCIe

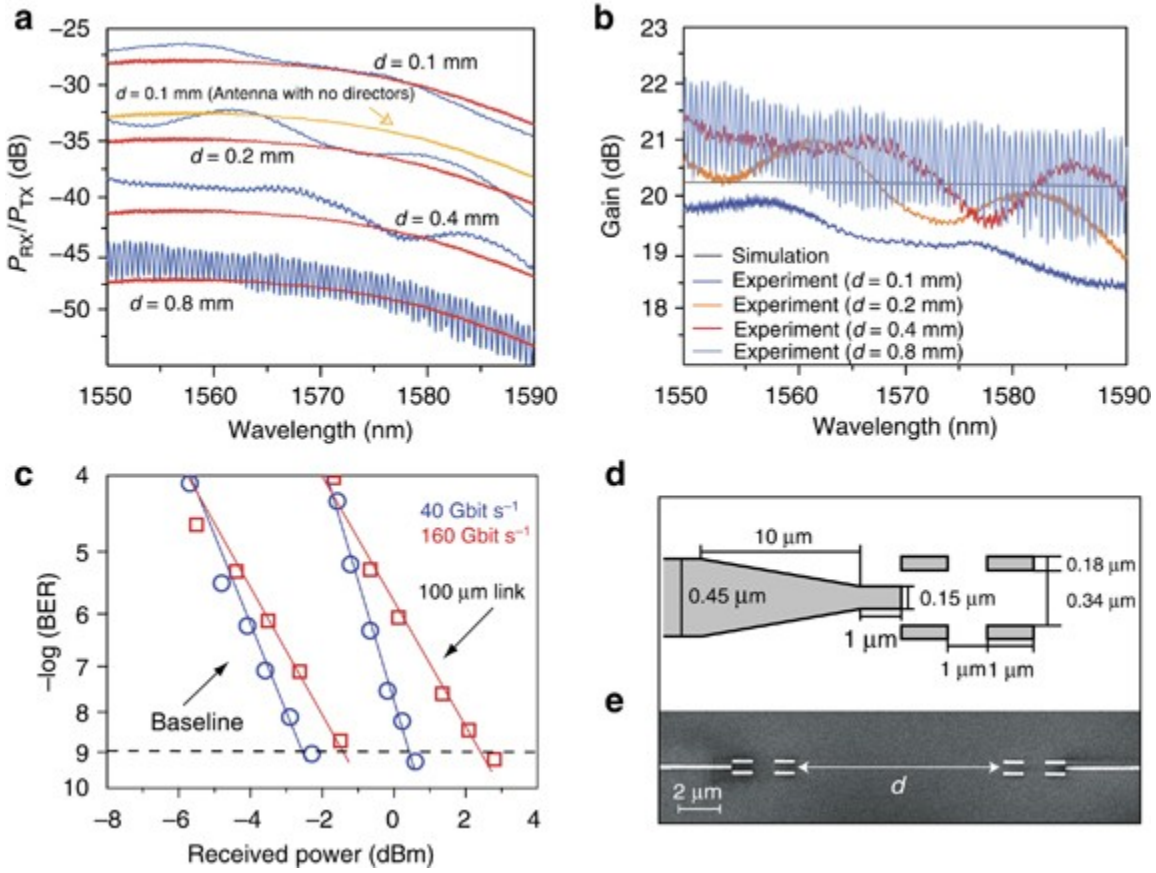


Новые горизонты

Внутренние интерфейсы микросхем прошли путь от единой системной шины к распределённым сетям на кристалле с пакетной маршрутизацией

Медные соединения столкнулись с ограничениями открывая путь оптическим и беспроводным архитектурам

Эти инновации порождают новые угрозы безопасности требующие дальнейших исследований



*On-chip wireless silicon photonics: from reconfigurable interconnects to lab-on-chip devices | Light: Science & Applications

Спасибо за внимание!
Вопросы?

Загартдинов Булат

me@vaire.lt