

面向软件定义晶上系统的安全多维互连网络

李沛杰, 沈剑良, 郭威, 曹志鹏, 梅波
(信息工程大学, 河南 郑州 450001)

摘 要: 针对软件定义晶上系统芯粒间数据篡改和完整性攻击问题, 提出了一种动态异构冗余的安全多维晶上网络架构。实现了一种电路交换和分组交换统一的电路结构, 并引入了一种动态异构冗余多路径传输模型, 可支持同维异构多路径、不同维异构多路径和混合维度异构多路径; 提出一种多路径选择与计算算法, 利用接口状态分布式地构建异构多路径; 设计了一种报文传输与策略裁决机制, 实现首报文复制多径传输、逐报文复制多径传输和全报文复制多径传输, 满足不同场景对安全性和性能的需求。基于 40 nm CMOS 工艺实现了一种同时支持电路交换和分组交换的晶上安全互连芯粒, 并构建了晶上网络系统。测试结果表明, 相比传统多径传输, 所提架构在多路径协同攻击下可提升 35.4%~94.8% 的传输成功率。基于 OMNeT 平台对 16×16 规模的安全多维晶上网络模型进行了性能仿真, 结果表明, 在无安全攻击时, 通过优化传输模式和互连维度, 可实现与传统多径传输相当的延迟。在有安全攻击时, 所提架构能够实现高达 37.37% 的延迟优化。

关键词: 多径传输; 晶上网络; 硬件安全; 数据完整性攻击; 网络安全

中图分类号: TP309.2

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025020

Secure multidimensional interconnection network for the software defined system on wafer

LI Peijie, SHEN Jianliang, GUO Wei, CAO Zhipeng, MEI Bo
Information Engineering University, Zhengzhou 450001, China

Abstract: To address data integrity attacks between dielets in software defined systems on wafer (SDSoW), a secure multidimensional network on wafer (SMNoW) architecture based on dynamic heterogeneous redundancy (DHR) was proposed. A unified circuit switching (CS) and packet switching (PS) structure was implemented, and a DHR-based multipath transmission model was developed. This model supported same dimensional, different dimensional, and mixed dimensional heterogeneous multipath transmission. An algorithm for multipath selection and computation was proposed to construct heterogeneous multipaths based on interface status. To meet varying requirements, multipath transmission methods based on first packet replication, packet-by-packet replication, and all packets replication were achieved through a packet transmission and policy arbitration mechanism. The proposed

收稿日期: 2024-09-12; 修回日期: 2025-01-03

通信作者: 李沛杰, lipeijie@csivo.com

基金项目: 国家重点研发计划 (2023YFB4404202, 2022YFB4401401)

Foundation Item: The National Key R&D Program of China(2023YFB4404202,2022YFB4401401)

引用格式: 李沛杰, 沈剑良, 郭威, 等. 面向软件定义晶上系统的安全多维互连网络[J]. 网络与信息安全学报, 2025, 11(2): 102-114.

Citation Format: LI P J, SHEN J L, GUO W, et al. Secure multidimensional interconnection network for the software defined system on wafer[J]. Chinese Journal of Network and Information Security, 2025, 11(2): 102-114.

SMNoW was tested in a network on wafer system based on the unified CS and PS structure. Experimental analysis shows that the proposed architecture increases transmission success rates from 35.4% to 94.8% compared to typical multipath arbitration feedback transmission methods under multipath collaborative attacks. The performance of a 16×16 multidimensional network on wafer was evaluated using the OMNeT platform. Results indicate that by selecting appropriate transmission modes and interconnection dimensions, the proposed architecture could achieve delay characteristics comparable to traditional multipath (MP) transmission. Furthermore, under security attacks, the proposed architecture achieves up to 37.37% transmission delay optimization compared to MP.

Keywords: multipath transmission, network on wafer, hardware security, data integrity attack, network security

0 引言

软件定义晶上系统 (software defined system on wafer, SDSoW) 通过高密度集成技术, 将异构功能芯粒在晶圆级硅基板互连, 实现高动态的应用部署, 是未来信息系统基础设施的新技术形态^[1]。晶上网络 (network on wafer, NoW) 作为 SDSoW 上芯粒互连的通道, 是数据高性能和高可信传输的关键, 但面临着系统故障、软硬件木马等攻击的安全问题, 存在复杂的广义功能安全威胁。如何构造安全可靠的 NoW 架构, 保障芯粒间端到端数据的安全传输成为必须解决的问题。

目前业界对 NoW 安全性的研究较少, 但现有的先进集成芯片网络安全和 NoW 可靠性传输技术研究对 NoW 安全性的研究具有参考意义。在网络安全研究上, 文献[2]通过可重配置互连网络混淆芯粒连接, 以防止外部窥探。文献[3]利用有源转接板构建物理隔离互连结构实时检测数据。文献[4]通过在片上 3D NoC 的路由节点部署检测电路来规避硬件木马攻击。但这些研究在 NoW 中是不成立的, 攻击者可利用网络节点、操作系统或应用软件中的漏洞和后门, 或嵌入在系统硬件中的木马发起网络攻击。在可靠性传输技术方面, 文献[5]基于 2.5D 互连实现面向不同应用网络拓扑的动态重构。文献[6]在业务通道上通过设计分离通道来支持动态可变的数据传输。文献[7]利用动态路由解决晶上系统的可靠传输问题。文献[8]基于软件可配置网络和预先存储的多冗余模式适应不同的数据负载。文献[5-8]利用 NoW 的动态性或冗余性提升数据传输的性能或可靠性。实际上, 基于网络的动态性和冗余性可构建多路径传输, 文献[9]在 SD-WAN 中提出多跳多路径传输机制, 通过软件定义切换备选路径应对网络攻击和链路故障。这些研究都利用了网

络的动态性和冗余性, 增加了嗅探和数据篡改的难度, 但由于传输业务及路径缺乏异构性, 难以应对多路径的协同攻击。鉴于此, 内生安全技术被引入互连网络, 利用动态异构冗余 (dynamic heterogeneous redundancy, DHR) 架构和多模裁决机制将广义功能安全问题转化为可控的概率问题。NoW 天然具有 DHR 特性, 可构建 DHR 架构的多径传输, 保障芯粒间端到端数据的安全传输。

本文主要贡献如下。

1) 提出一种安全多维晶上网络 (secure multi-dimensional NoW, SMNoW) 架构: 基于电路交换 (circuit switching, CS) 和分组交换 (packet switching, PS) 统一的电路结构构建多维异构多路径。

2) 提出一种基于 DHR 架构的多路径传输 (DHR-based multipath transmission, DHR-MT) 模型: 基于多路径选择与计算算法构建同维度、不同维度和混合维度的异构多路径。

3) 提出一种报文传输与策略裁决机制: 支持多种多径传输模式并进行策略裁决。

4) 在 40 nm 工艺节点上实现了晶上安全互连芯粒并构建 NoW 系统。测试结果表明, SMNoW 可有效防御多类型安全攻击, 并在保障安全性的同时达到与传统多径传输相匹配的传输性能。

1 NoW 的结构及安全威胁分析

1.1 问题描述

NoW 作为 SDSoW 的网络支撑, 其结构如图 1 所示, 其中布局在芯粒物理四周的互连接口 (NI、SI、WI 和 EI) 对内通过决策和路由 (decision and routing, D&R) 实现数据交叉互通, 对外通过接口凸点 (IO) 和铜布线与晶圆基板上的互连结构相连。芯粒互连和基板互连共同构成 NoW。互连结构按照是否存在有源逻辑 (路由 R 和互连接口) 分为有源基板互连和无源基板互连两类。

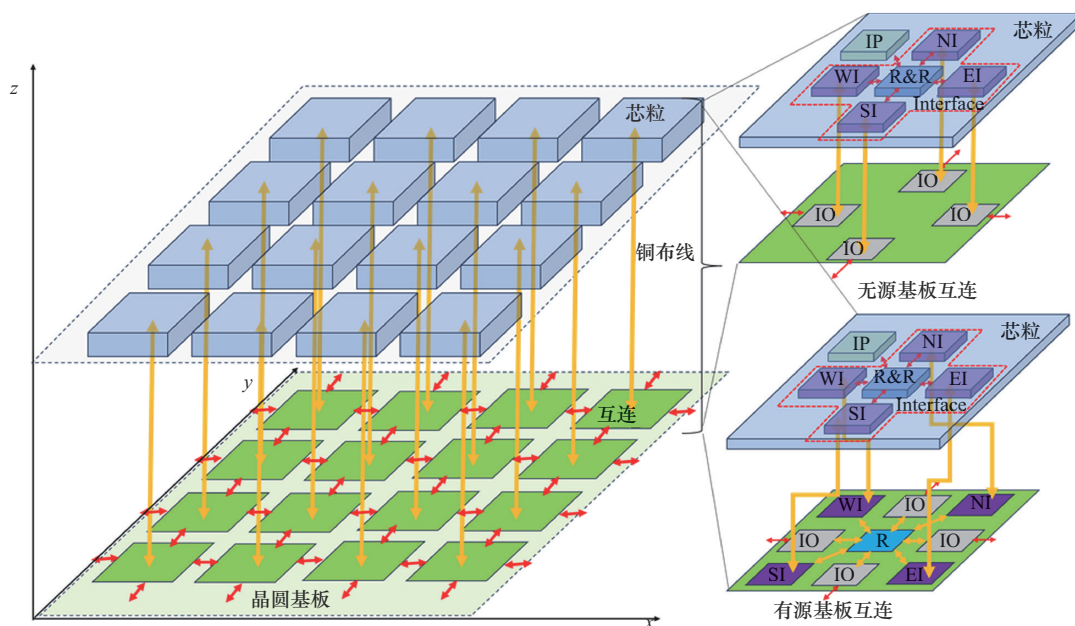


图 1 NoW 的结构示意

Figure 1 NoW structure schematic

NoW 中的安全威胁如图 2 所示, SDSoW 中的报文可由源芯粒 S 的本地 IP 经多条传输路径到达目的芯粒 D 。由于不可信第三方的设计与制造, NoW 中芯粒、芯粒与基板的铜互连、基板互连单元等网络元素存在不确定物理失效, 以及大量已知或未知的硬件木马、漏洞和后门, 攻击者可通过 3 类场景威胁数据传输安全: ① 信息完整性攻击导致端口间频繁重传, 消耗信

道带宽 (攻击隐藏在不确定物理失效中); ② 信息完整性攻击导致系统重路由并经过恶意节点, 造成信息泄露 (图 2 虚线); ③ 基于信息完整性漏检漏洞, 信息完整性逃逸性检查致使篡改数据被目的芯粒接收。

1.2 解决方案

攻击者可将安全攻击伪装在不确定物理失效中, 因此单路径传输难以保障敏感数据的可靠性

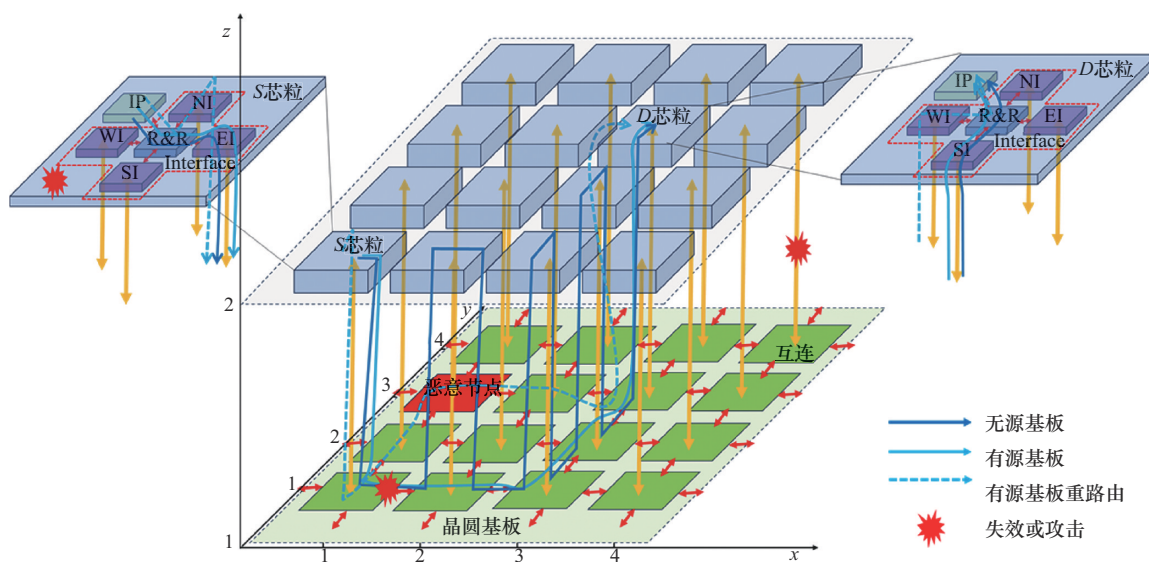


图 2 NoW 中的安全威胁

Figure 2 Security threats in NoW

和可信度。为满足 NoW 拓扑的灵活性和长距离低延迟传输需求, NoW 的互连接口及路由需支持多种转发模式^[6,8]和更大传输带宽。NoW 天然的冗余特性使得构建多路径传输成为可能。本文创新性地提出一种 SMNoW 架构, 其中互连接口和路由节点采用 CS 和 PS 共存的电路结构。基于该网络, 本文构建了 DHR 的多路径传输模型, 包括同维异构多路径 (same dimensional heterogeneous multipath, SDHM)、不同维异构多路径 (different dimensional heterogeneous multipath,

DDHM) 和混合维度异构多路径 (mixed dimensional heterogeneous multipath, MDHM) 3 种。

2 DHR-MT 模型

基于 SMNoW 的基本结构, 本文提出 DHR-MT 模型, 支持 SDHM、DDHM 和 MDHM 共 3 种异构多路径传输模式。DHR-MT 模型的整体架构如图 3 所示, DHR-MT 模型通过芯粒的 D&R 实现多路径数据的比较与裁决。D&R 根据接收报文的一致性检测结果, 动态清洗异常路径并触发

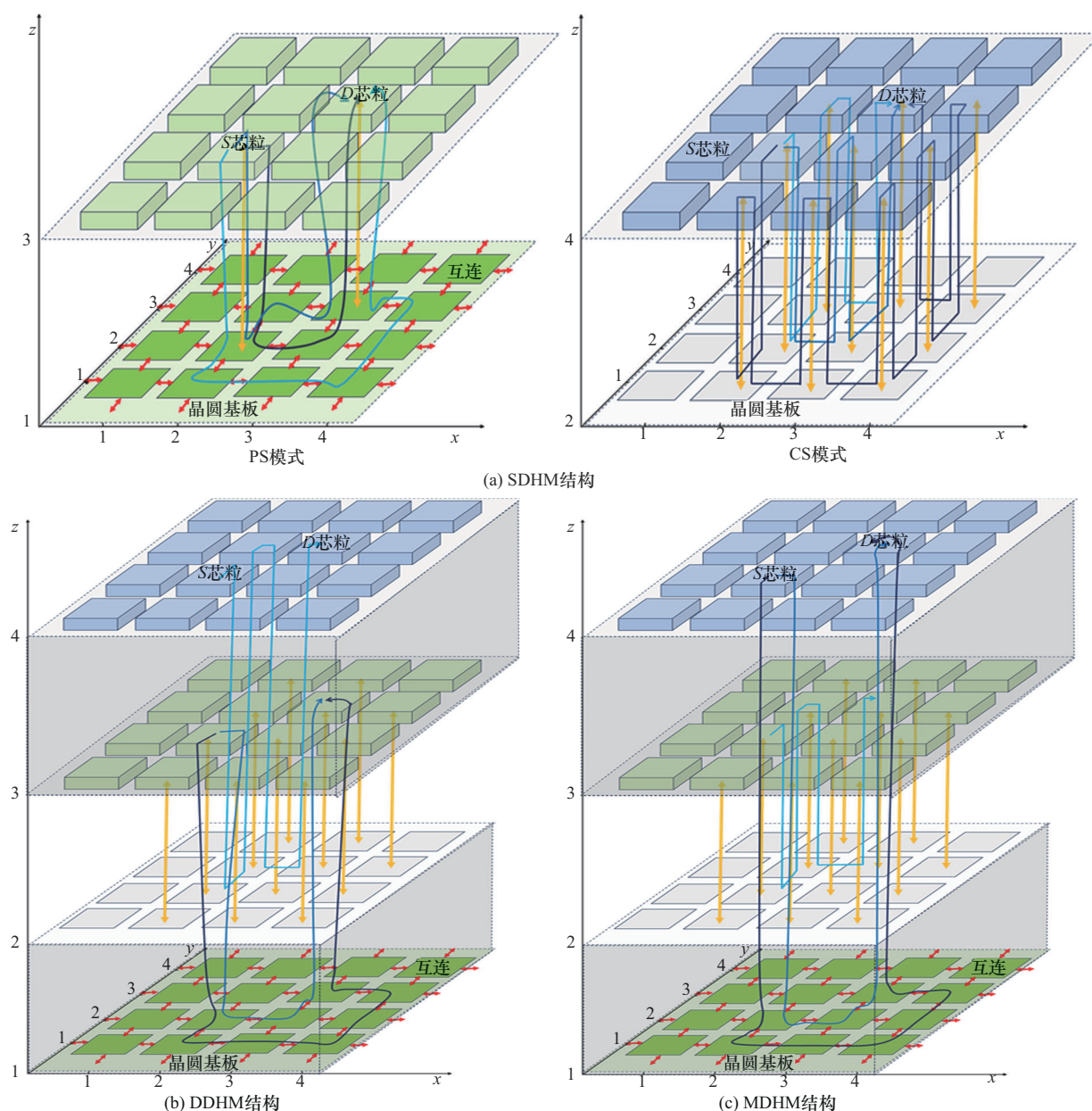


图3 DHR-MT模型的整体架构

Figure3 Overall architecture of DHR-MT model

重构。SMNoW 的多维互连结构（多维互连接口（multidimensional interconnect interface, MII）和多维转发（multidimensional forwarding, MF））为异构路径提供物理支撑，其中 MF 通过 CS 与 PS 混合架构实现细粒度路径控制。

3 SMNoW 关键结构设计

3.1 MII 结构设计

MI I 结构如图4所示，MI I 主要基于 DHR 特性

结构设计^[10-11]，并在此基础上增加多维互连结构。在 MI I 结构中，互连接口分布在芯粒物理四周，支持动态协议切换与报文结构重组，其核心功能如下。

- 1) 接口状态检测：实时监控链路异常（如物理失效或攻击），触发动态重构。
- 2) 多路径选择与计算：根据接口状态和网络拓扑，生成异构路径集合。
- 3) 报文比较与策略裁决：对多路径报文进行

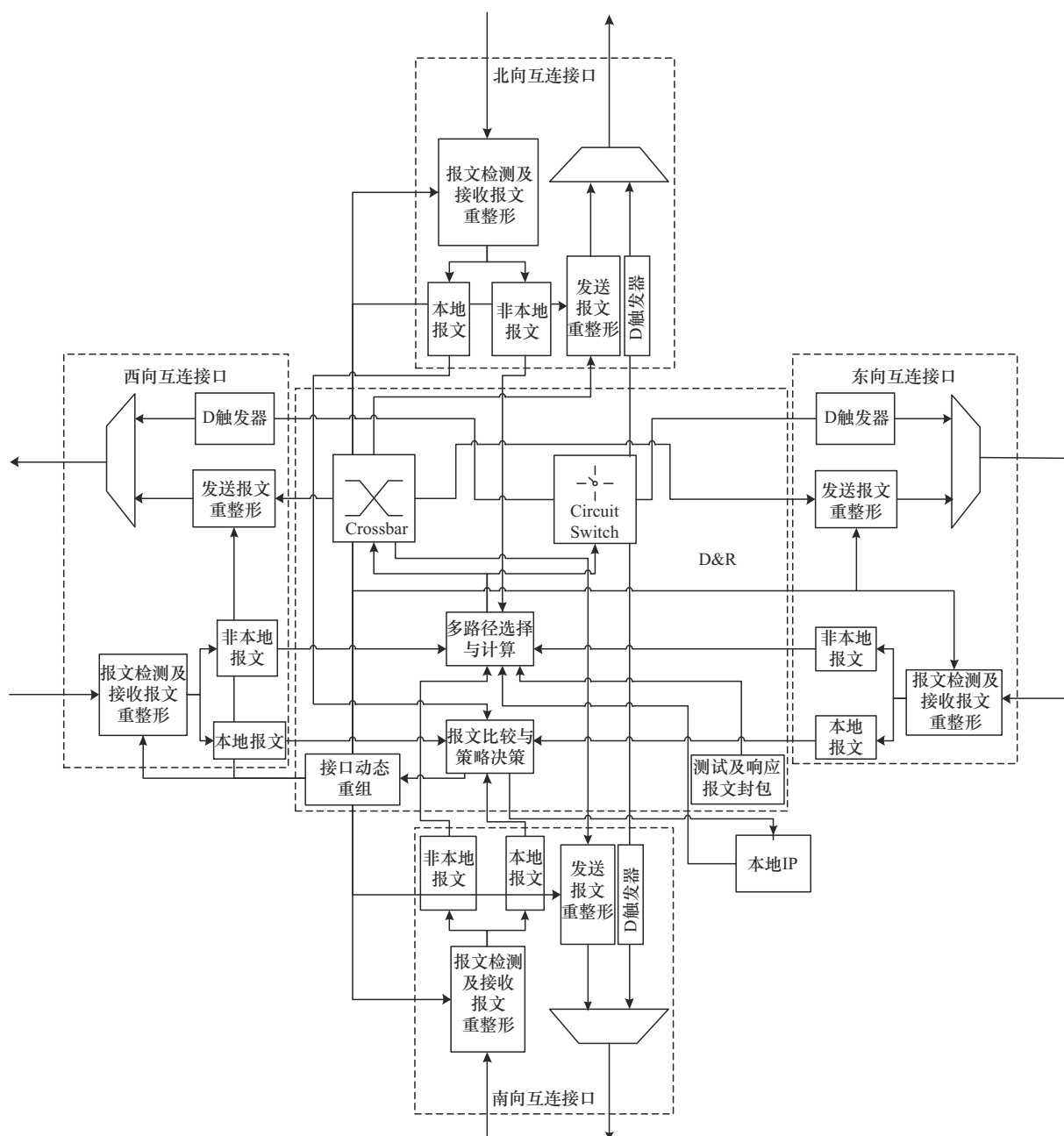


图 4 MII 结构示意

Figure4 MII structure schematic

哈希对比, 若不一致, 则反馈异常路径信息, 触发清洗与重构。

3.2 MF结构设计

MF由CS和PS两部分组成, 其结构如图5示, 本文采用文献[12]所述的多协议交换互连架构, 其中, Crossbar采用不带交叉节点缓存的互连网络, 在CS模式下, 根据多路径选择与计算的结果, 交叉节点可动态定义为不同电路连接, 直至连接释放并重新建立新的连接。Crossbar的IB、OB及交叉节点阵列可分别定义, 以实现细粒度的混合维度。

3.3 多路径选择与计算算法

本算法的目标是基于网络拓扑与接口状态, 生成满足异构性、时延与安全约束的多路径集合。以Mesh结构为例, 对于 $m \times n$ 的NoW, 算法相关参数如表1所示。

如式(1)所示, NoW中的所有芯粒采用三维描述, 其中 k 从1~4分别表示逻辑结构上的基板PS层、基板CS层、芯粒PS层和芯粒CS层。

$$N = \{C_{i,j,k}, 1 \leq i \leq m, 1 \leq j \leq n, 1 \leq k \leq 4\} \quad (1)$$

源芯粒和目的芯粒如式(2)和式(3)所示。

$$C_{src} = C_{i_s, j_s, k_s} \in N \quad (2)$$

$$C_{dest} = C_{i_d, j_d, k_d} \in N \quad (3)$$

NoW的网络构成不一定是全阵列型的, 考虑晶圆边缘的芯粒, 通过虚拟芯粒补齐阵列, 但通过芯粒接口状态区分, 具体如式(4)所示。

$$st_l = \begin{cases} 0, & \text{链路断开} \\ 1, & \text{链路连接} \\ 2, & \text{链路丢失} \end{cases} \quad (4)$$

多路径选择与计算算法描述如算法1所示。

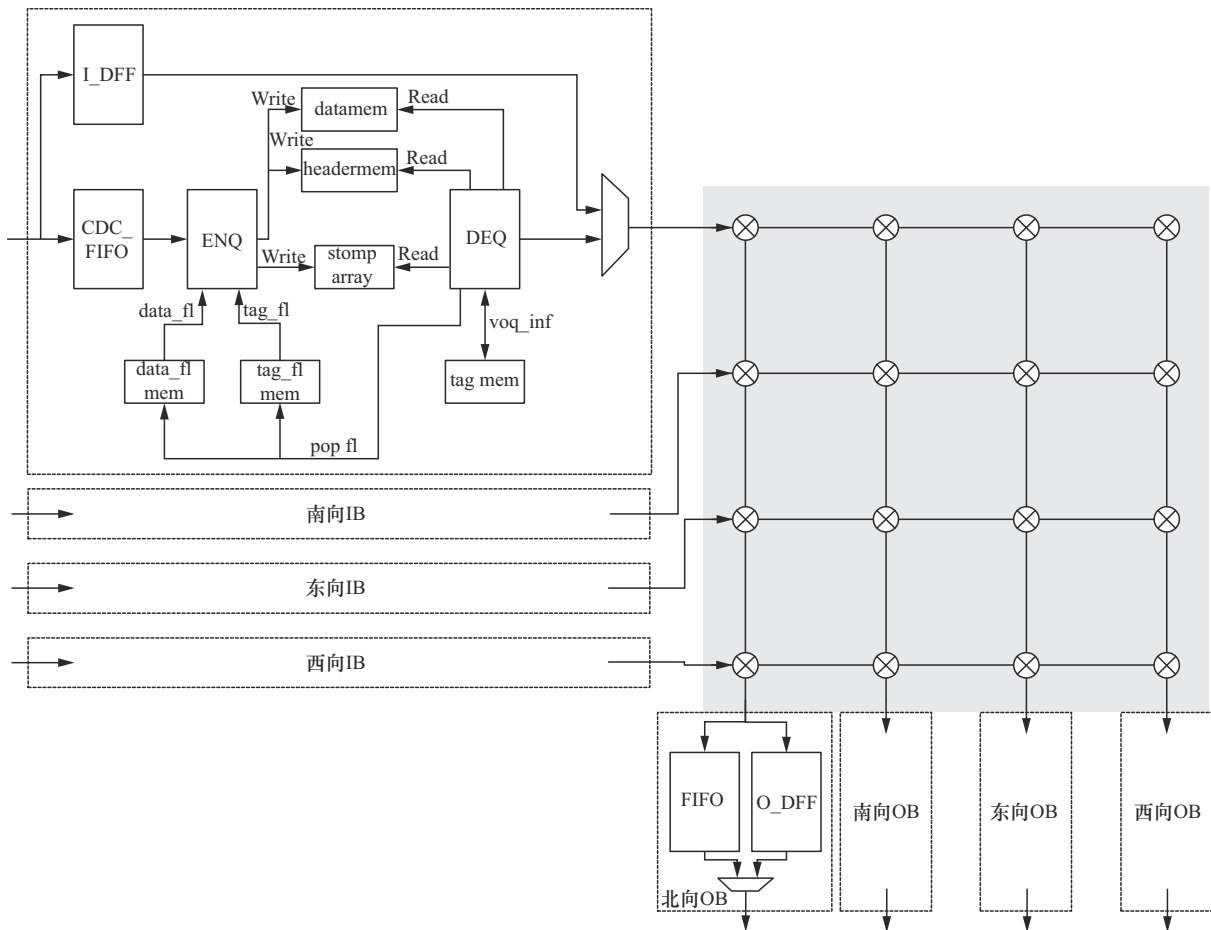


图5 MF结构示意图

Figure5 MF structure schematic

表 1 算法相关参数

Table 1 Algorithm correlation parameter

符号	含义
N	互连节点集合
C_{src}	源芯粒
C_{dest}	目的芯粒
st_l	节点物理接口状态
$l \in \{N, S, W, E\}$	互连接口物理位置
$ST_{i,j,k}$	节点接口状态集合
$p_{C_a \rightarrow C_b}(r)$	C_a 到 C_b 的第 r 条路径
$p_{C_a \xrightarrow{C_c} C_b}(r)$	C_a 到 C_b 经过 C_c 的第 r 条路径
$S(r)$	第 r 条路径上的芯粒集合
L	C_{src} 到 C_{dest} 的异构路径数量
P_{sdhm_ps}	基于 PS 的 SDHM 路径集合
P_{sdhm_cs}	基于 CS 的 SDHM 路径集合
P_{ddhm}	DDHM 路径集合
P_{mdhm}	MDHM 路径集合
M	最大重构次数
cnt	重构次数计数器
data_mem _{i}	路径 i 的报文存储空间
hash_mem _{i}	路径 i 的哈希值存储空间
key_inf _{ij}	路径 i 的第 j 个报文的关键信息, 包括源地址、目的地址、流 ID、优先级和序列号
hash _{ij}	路径 i 的第 j 个报文的哈希值
CNT	报文一致的数量

算法 1 多路径选择与计算算法输入 $N, C_{src}, C_{dest}, ST_{i,j,k}$ 输出 $P_{sdhm_ps}, P_{sdhm_cs}, P_{ddhm}, P_{mdhm}$

- 1) while $i \neq i_d \&\& j \neq j_d$ do
- 2) 计算 $p_{C_{src} \rightarrow C_{dest}}(r) = XY_YX_path(C_{src}, C_{dest})$
- 3) 计算 $S(r) = node(p_{C_{src} \rightarrow C_{dest}}(r))$
- 4) $i = i_s, j = j_s$
- 5) if $i_s \leq i_d \&\& ST_{i,j,k}(3) \neq 1 \parallel i_s \geq i_d \&\& ST_{i,j,k}(2) \neq 1$ or $j_s \leq j_d \&\& ST_{i,j,k}(0) \neq 1 \parallel j_s \geq j_d \&\& ST_{i,j,k}(1) \neq 1$
- 6) 更新 $p_{C_{src} \rightarrow C_{dest}}(r) = path_turn(C_{src}, C_{dest})$
- 7) 更新 $S(r)$
- 8) return
- 9) else

10) 更新 i, j, k

11) end if

12) end while

13) if $r < 1$

14) 到 1)

15) else

16) $I = find_i(S(r)), J = find_j(S(r))$ 17) $i_{max} = maximum(I), j_{max} = maximum(J)$ 18) $i_{min} = minimum(I), j_{min} = minimum(J)$ 19) if $i_s \leq i_d \&\& j_s \leq j_d$ 20) $i_{mid} = i_{min} - 1, j_{mid} = j_{min} - 1$ 21) if $ST_{i_s, j_s, k}(1) = 1 \&\& j_{mid} \geq 0$

22) 计算 $P_{C_{src} \xrightarrow{C_{i_s, j_{mid}, k}} C_{dest}}(r) = XY_YX_path(C_{src}, C_{dest})$

23) 计算 $S(r) = node\left(P_{C_{src} \xrightarrow{C_{i_s, j_{mid}, k}} C_{dest}}(r)\right)$

24) 重新执行 6)~8)

25) $P_{sdhm_ps} = \{p_{C_{src} \rightarrow C_{dest}}(0), p_{C_{src} \rightarrow C_{dest}}(1),$

$$p_{C_{src} \xrightarrow{C_{i_s, j_{mid}, 1}} C_{dest}}(2)\}$$
26) $P_{sdhm_cs} = \{p_{C_{src} \rightarrow C_{dest}}(0), p_{C_{src} \rightarrow C_{dest}}(1),$

$$p_{C_{src} \xrightarrow{C_{i_s, j_{mid}, 1}} C_{dest}}(2)\}$$
27) 更新 r 28) else if $ST_{i_s, j_s, k}(2) = 1 \&\& i_{mid} \geq 0$

29) 计算 $P_{C_{src} \xrightarrow{C_{i_{mid}, j_s, k}} C_{dest}}(r) = XY_YX_path(C_{src}, C_{dest})$

30) 计算 $S(r) = node\left(P_{C_{src} \xrightarrow{C_{i_{mid}, j_s, k}} C_{dest}}(r)\right)$

31) 重新执行 6)~8)

32) $P_{sdhm_ps} = \{p_{C_{src} \rightarrow C_{dest}}(0), p_{C_{src} \rightarrow C_{dest}}(1),$

$$p_{C_{src} \xrightarrow{C_{i_{mid}, j_s, 1}} C_{dest}}(2)\}$$
33) $P_{sdhm_cs} = \{p_{C_{src} \rightarrow C_{dest}}(0), p_{C_{src} \rightarrow C_{dest}}(1),$

$$p_{C_{src} \xrightarrow{C_{i_{mid}, j_s, 2}} C_{dest}}(2)\}$$
34) 更新 r

```

35) else
36)  $C_{i_{next}, j_{next}, k} = \text{find\_first}(S(r))$ 
37) 计算  $P_{C_{src} \xrightarrow{C_{i_{mid}, j_{next}, k}} C_{dest}}(r) = XY\_YX\_path$ 
    ( $C_{src}, C_{dest}$ )
38) end if
39) else if  $i_s \leq i_d \&\& j_s > j_d$ 
40)  $i_{mid} = i_{min} - 1, j_{mid} = j_{max} + 1$ 
41) if  $ST_{i_s, j_s, k}(0) = 1 \&\& j_{mid} \leq n$ 
42) 执行 22)~38)
43) else if  $i_s > i_d \&\& j_s \leq j_d$ 
44)  $i_{mid} = i_{max} + 1, j_{mid} = j_{min} - 1$ 
45) 执行 22)~27)
46) if  $ST_{i_s, j_s, k}(3) = 1 \&\& i_{mid} \leq m$ 
47) 执行 29)~38)
48) else
49)  $i_{mid} = i_{max} + 1, j_{mid} = j_{max} + 1$ 
50) 执行 41)~42), 46)~47)
51) end if

```

算法1的含义如下：源芯粒首先基于XY和YX路由方式构建同维异构路径（步骤1)~3)）。若原始路径发现节点多维互连全部故障，则绕行（步骤4)~8)）或在故障节点处切换互连维度（步骤9)~10)），在确定至多两条路径后，计算路径边界（步骤16)~18)），并根据源芯粒和目的芯粒的位置关系，从边界向外构建新路径（步骤19)~50)）。以目的芯粒在源芯粒东北方向为例（步骤19)~38)），若源芯粒在西向（步骤21)~27)）或南向

（步骤28)~34)）状态正常，则通过边界外最近中间节点构建路径；否则，从原有路径中选择最近节点作为中间节点构建路径（步骤35)~38)），并通过更改交叉节点的互连维度实现异构。最终可构建同维异构路径 P_{sdhm_ps} 和 P_{sdhm_cs} ，从SDHM路径可构建不同维异构路径 P_{ddhm} 、 P_{mdhm} 。则基于存在交叉节点的路径构建。源芯粒可根据性能需求从 P_{sdhm_ps} 、 P_{sdhm_cs} 、 P_{ddhm} 和 P_{mdhm} 选择异构路径。

3.4 报文传输与策略裁决机制

报文多路径传输及策略决策流程如图6所示，源芯粒在选定异构路径后，按流ID分包并复制报文，通过多条异构路径发送至目的芯粒。根据表2所示的传输延迟和安全性需求，选择首报文复制多径传输（multipath transmission based on first packet replication, MT-FPR）、逐报文复制多径传输（multipath transmission based on packet by packet replication, MT-PPR）或全报文复制多径传输（multipath transmission based on all packet replication, MT-APR）。

表2 报文传输模式

Table 2 Packet transmission mode

传输延迟需求	安全性需求	异构路径选择	报文传输模式
低	高	P_{sdhm_ps}	MT-PPR
高	高	P_{sdhm_cs}	MT-APR
低	低	P_{sdhm_ps}	MT-FPR
高	低	P_{sdhm_cs}	MT-FPR

目的芯粒接收到报文后，按照策略裁决算法进行裁决，具体描述如算法2所示。

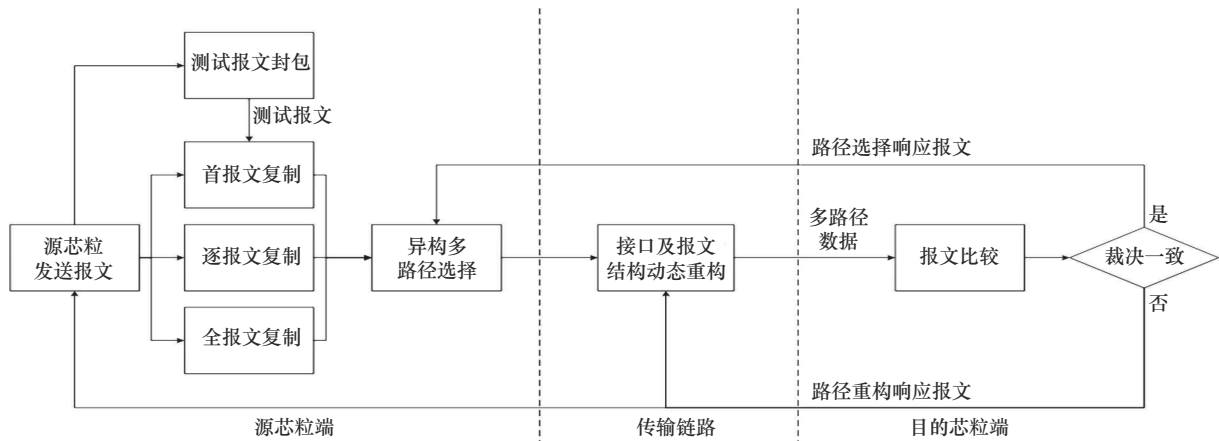


图6 报文多路径传输及策略决策流程

Figure6 Process of packet multipath transmission and policy arbitration

算法2 策略裁决算法**输入** 路径 i 接收的第 j 个报文 pkg_{ij} , $i \in P_{\text{sdhm_ps}} // P_{\text{sdhm_cs}} // P_{\text{ddhm}} // P_{\text{mdhm}}$ **输出** 最终决策报文 pkg_dec

```

1) if  $\text{data\_mem}_i \neq \emptyset$  begin
2)   $\text{hash}_{ij} = \text{hash\_cal}(\text{pkg}_{ij}(\text{key\_inf}_{ij}))$ 
3)   $\text{hash\_mem}_i = \{\text{hash}_{ij}\}$ 
4)  if  $\text{hash\_mem}_i \neq \emptyset$  then
5)    查找相同哈希值  $\text{hash} = \text{find\_same}(\text{hash}_{ij})$ 
6)    根据哈希值分别读取报文存储空间
 $\text{data}_i = \text{read\_mem}_i(\text{hash})$ 
7)    比较  $\text{data}_i$  和  $\text{data}_k$ ,  $i \neq k$ 
8)    if  $\text{data}_i = \text{data}_k$  then
9)       $\text{CNT} = \text{CNT} + 1$ , 更新  $k$ 
10)   else
11)     更新  $i, k$ 
12)   end if
13)   if  $\text{CNT} = L$  begin
14)      $\text{pkg\_dec} = \text{data}_i$ , 更新  $j$ 
15)     反馈维持响应报文到所有路径
16)      $\text{cnt} = 0$ 
17)   else if 存在  $\text{CNT} \geq \frac{L+1}{2}$ 
18)      $\text{pkg\_dec} = \text{data}_i$ , 更新  $j$ 
19)     反馈重构响应报文到异常路径
20)      $\text{cnt} = 0$ 
21)   else
22)     反馈重构响应报文到所有路径
23)      $\text{cnt} = \text{cnt} + 1$ 
24)     等待测试报文并重复执行 7)~18)
25)     if  $\text{cnt} = M + 1$  begin
26)       更新路径, 重新执行 1)~19)
27)     else
28)       重新执行 17)~19)
29)     end if
30)   end if
31) end if
32) end if

```

算法2的含义如下: 目的芯粒的D&R首先计算不同路径上报文的哈希值(步骤1)~3)), 然

后检查相同哈希值的报文内容(步骤4)~7))。若报文内容一致, 递增计数器直到比较结束(步骤8)~12))。若裁决通过且结果一致, 向源芯粒发送维持响应报文, 并基于该路径集进行数据传输(步骤13)~16))。若裁决通过但存在异常路径, 向异常路径上的芯粒发送重构响应报文, 指示动态重组互连接口和报文结构(步骤17)~20))。若裁决不通过, 向所有路径上的芯粒发送重构响应报文, 进行动态重组(步骤22)~23))。同时告知源芯粒异常信息, 源芯粒封装测试报文并发送, 目的芯粒接收后重新裁决(步骤24))。若超过最大重构次数限制或裁决通过, 则结束; 否则, 选择新的传输路径, 并标记异常路径标识为不可用(步骤24)~26))。

4 测试与仿真分析**4.1 安全性分析**

SMNoW利用多维互连结构, 支持SDHM、DDHM和MDHM等多种异构冗余路径, 且异构性随维度的增加而增强。互连接口和传输报文的动态结构, 使得多路径在互连、报文和传输模式上高度异构, 攻击者难以协同攻击; 当目的芯粒裁决不通过时, 可快速重构并清洗异常路径。这种典型的DHR结构, 可有效避免单条传输路径中硬件木马、漏洞或后门触发的数据完整性攻击。并且, 由于最大限度的异构性, 攻击者对异构路径上传输数据发起的协同攻击很难造成逃逸。

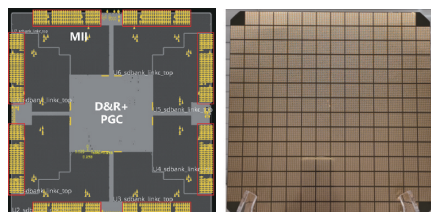
4.2 安全性测试

本文在40 nm CMOS工艺上设计并流片了CS和PS结构共存的晶上安全互连芯粒, 将192个芯粒集成到无源硅基板上, 构成如图7(a)所示的NoW系统。芯粒版图如图7(b)所示, 全芯粒8个MII共享中心区域的D&R及内嵌的包生成与检测(packet generate and check, PGC)模块, PGC可定义和检查报文的任何信息, 芯粒未设计加密等复杂的安全机制, 仅检查数据CRC。

按照表3所示测试环境, 分别对单路径传输(single path, SP)、多路径传输(multipath, MP)、MRR^[13]、MT-PPR、MT-FPR和MT-APR等模式, 在单路径攻击、多路径非协同攻击和多路径协同攻击下的安全防护效果进行测试。基于节点CRC检测逃逸机制, 对数据正确传输的成功率进行评估。



(a) 软件定义晶上网络系统测试环境



(b) 晶上安全互连芯粒版图及贴装后的芯片实物

图7 集成多维互连结构的安全互连芯粒版图及NoW系统
Figure7 The layout of secure chiplet with multidimensional interconnect structure and NoW system

表3 测试环境

Table 3 Test environment

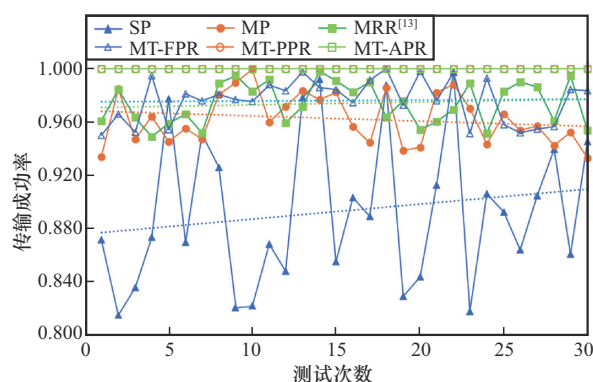
后门配置项	异常 报文路径	异常 报文生成	节点及报 文结构	传输 路径数
单路径攻击	1	随机报文	固定	3
多路径非 协同攻击	2	随机报文	固定 或动态	3
多路径协同 攻击	2	首报文/随机报 文/单一报文	固定 或动态	3

4.2.1 单路径攻击测试

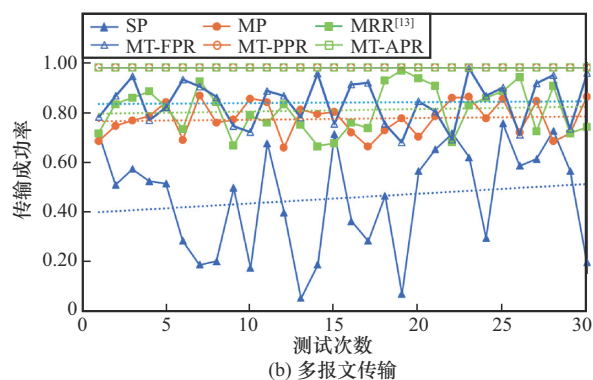
单路径攻击测试结果如图8所示，攻击者绕过CRC检测篡改数据报文，导致SP和MP模式下目的芯粒无法检测篡改。MP将报文分散到不同路径传输，因此对单路径攻击有一定效果。MRR和MT-FPR通过比较从多路径接收的首报文应对篡改攻击，但无法处理非首报文篡改，尤其在多报文传输中，传输成功率较单包传输降低15%左右。而MT-PPR和MT-APR对所有报文都复制并多径传输，目的芯粒通过比较不同路径的相同数据进行大数裁决，非攻击异构路径的传输使得大数裁决一定通过，确保了数据的正确接收。

4.2.2 多路径非协同攻击

多路径非协同攻击测试结果如图9所示，目的芯粒的一致性比较和裁决反馈机制使非协同攻击下的多路径传输报文因内容不一致而裁决不通过，从而触发裁决反馈，并清洗路径、重新传输。这使得MRR、MT-FPR、MT-PPR和MT-APR的传输成功率高于无裁决反馈的MP（多报文传输下分别提升5.1%、10.7%、66.4%、66.4%）。



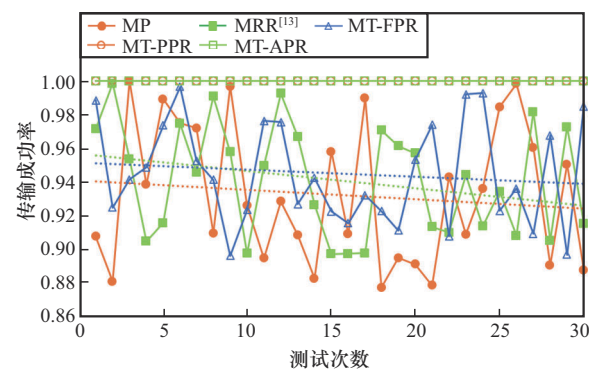
(a) 单报文传输



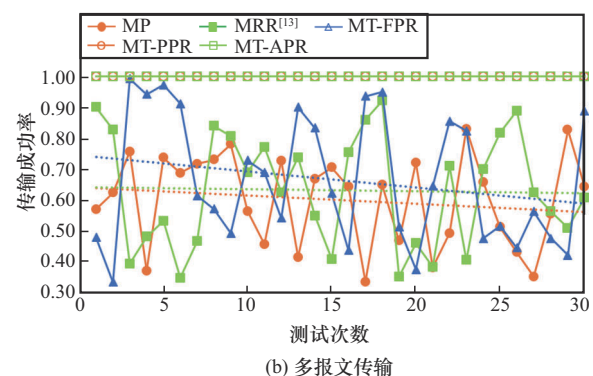
(b) 多报文传输

图8 单路径攻击测试结果

Figure8 Test result under single-path attack



(a) 单报文传输



(b) 多报文传输

图9 多路径非协同攻击测试结果

Figure9 Test result of multipath non-cooperative attack

常传输，显著降低传输时延。如图 11(b)所示，相比 MP，MT-FPR、MT-PPR 和 MT-APR 在 CS 模式下的延迟变化分别是 29.53%、4.23% 和 -13.9%，在 PS 模式下的延迟变化分别是 0.97%、-29.97% 和 -37.73%。MT-FPR 延迟增加主要由首包复制、报文比较、策略裁决、路径重构及首包重传导致。MT-PPR 和 MT-APR 相比 MP 具有延迟优化，尤其在 PS 模式下，策略裁决机制显著降低数据重传次数，从而优化延迟。

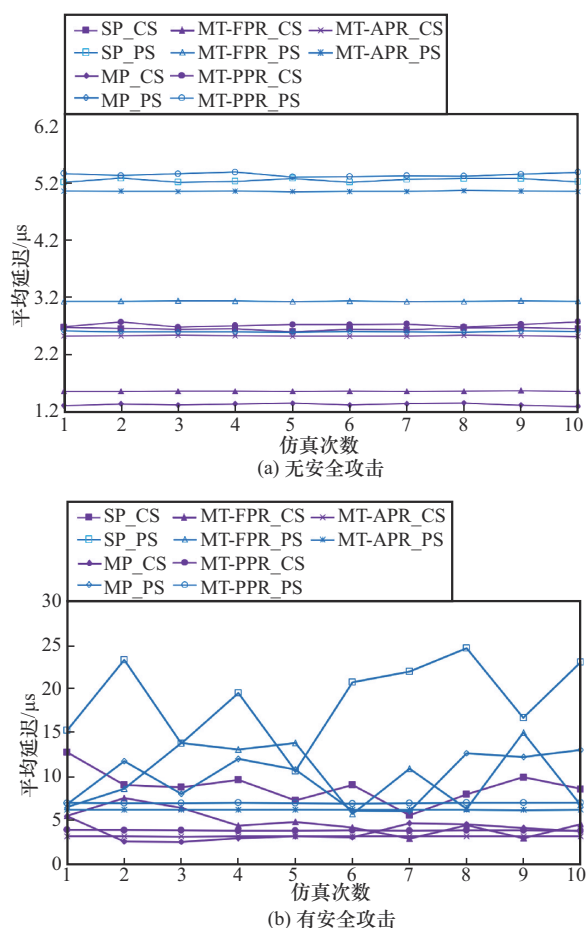


图 11 不同传输模式下报文传输延迟仿真结果

Figure 11 Simulation results of packet transmission delay in different transmission modes

5 结束语

本文主要研究了软件定义晶上系统中芯粒间数据篡改和完整性攻击问题，基于晶上网络的动态性和冗余性，引入多径传输和软件定义互连技术，构建了 DHR 的安全多维晶上网络架构，并提出 DHR 的多路径传输模型；实现了电

路交换和分组交换共存的多维互连接口和转发电路结构，通过多路径选择与计算算法构建多维异构路径；提供了 3 种多路径传输模式，满足不同性能和安全需求，基于芯粒决策模块实现策略裁决和路径反馈，结合动态性清洗异常路径，确保多径数据安全传输。测试和仿真结果表明，SMNoW 在多路径协同攻击下的安全性明显提升。在安全攻击下，可通过选择传输模式和互连维度有效降低传输延迟。后续将结合 SDSoW 的分布式 DHR 架构，研究统一业务下的协同调度问题。

参考文献：

- [1] 郭江兴, 刘勤让, 沈剑良, 等. 从 SoC 到 SDSoW: 微电子发展的新范式[J]. 中国科学: 信息科学, 2024, 54(6): 1350-1368.
WU J L, LIU Q R, SHEN J L, et al. From SoC to SDSoW: a new paradigm for microelectronics development [J]. Sci Sin Inform, 2024, 54(6): 1350-1368.
- [2] TALUKDAR J, CHAUDHURI A, KIM J, et al. Securing heterogeneous 2.5D ICs against IP theft through dynamic interposer obfuscation[C]// Proceedings of 2023 Design, Automation & Test in Europe Conference & Exhibition (DATE). Piscataway: IEEE Press, 2023: 1-2.
- [3] NABEEL M, ASHRAF M, PATNAIK S, et al. 2.5D root of trust: secure system-level integration of untrusted chiplets[J]. IEEE Transactions on Computers, 2020, 69(11): 1611-1625.
- [4] ZHANG Z, YU Q. Invariance checking based trojan detection method for three-dimensional integrated circuits[C]// Proceedings of 2020 IEEE International Symposium on Circuits and Systems (ISCAS). Piscataway: IEEE Press, 2020: 1-5.
- [5] VAISBAND B, IYER S S. Communication considerations for silicon interconnect fabric[C]// Proceedings of 2019 ACM/IEEE International Workshop on System Level Interconnect Prediction (SLIP). Piscataway: IEEE Press, 2019: 1-6.
- [6] CHEN S L, PAL S, KUMAR R. Waferscale network switches [C]// Proceedings of the 51th Annual International Symposium on Computer Architecture. Piscataway: IEEE Press, 2024: 1-17.
- [7] WAN Z, CAO Z, LI S, et al. Modeling and analysis of waferscale switching network with multiple system faults[C]// Proceedings of 2024 IEEE International Symposium on Circuits and Systems (ISCAS). Piscataway: IEEE Press, 2024: 1-5.
- [8] BUTERA W. A dynamically configurable network for software defined hardware[C]// Proceedings of 2020 IEEE High Performance Extreme Computing Conference (HPEC). Piscataway: IEEE Press,

2020: 1-7.

- [9] AN H, NA Y, LEE H, et al. Resilience evaluation of multipath routing against network attacks and failures[J]. Electronics, 2021, 10 (11): 1240.

- [10] 李沛杰, 沈剑良, 苑红晓, 等. 一种应用于软件定义互连系统的多协议 SerDes 电路[J]. 电子学报, 2021, 49(4): 817-823.

LI P J, SHEN J L, YUAN H S, et al. A multi-protocol serdes circuit for the applications in software defined interconnection system[J]. Journal of Electronics, 2021, 49(4): 817-823.

- [11] LI P, SHEN J, LYU P, et al. Architecture design of protocol controller based on traffic-driven software defined interconnection[J]. Chinese Journal of Electronics, 2024, 33(2): 362-370.

- [12] 董春雷, 沈剑良, 李沛杰, 等. 面向软件定义互连系统的多协议交换电路[J]. 通信学报, 2024, 45(5): 44-53.

DONG C L, SHEN J L, LI P J, et al. Multi-protocol switching circuit for software defined interconnection system[J]. Journal on Communications, 2024, 45(5): 44-53.

- [13] REN Q, HU T, WU J, et al. Multipath resilient routing for endogenous secure software defined networks[J]. Computer Networks, 2021, 194: 108-134.

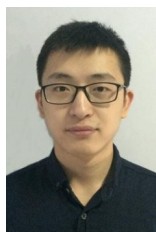
[作者简介]



李沛杰 (1990-), 男, 山西襄汾人, 信息工程大学助理研究员, 主要研究方向为软件定义晶上系统、硬件安全、软件定义互连。



沈剑良 (1982-), 男, 浙江德清人, 信息工程大学研究员、博士生导师, 主要研究方向为片上系统芯片、软件定义晶上系统。



郭威 (1990-), 男, 北京人, 信息工程大学副教授, 主要研究方向为计算机体系结构、人工智能与大数据、内生安全。



曹志鹏 (1996-), 男, 陕西西安人, 信息工程大学博士生, 主要研究方向为软件定义晶上系统、计算机体系结构、互连网络。



梅波 (1998-), 男, 安徽宣城人, 信息工程大学博士生, 主要研究方向为内生安全、硬件木马防御。