面向软件定义晶上系统的安全互连接口架构

李沛杰，沈剑良，郭威，曹志鹏，梅波
（信息工程大学信息技术研究所，河南 郑州 450002）

摘　要：针对软件定义晶上系统中芯粒互连接口缺乏动态性和异构性导致系统易被恶意芯粒攻击的问题，通过最大限度复用功能逻辑，提出一种动态异构冗余的安全互连接口架构。首先基于软件定义互连技术在电路结构、传输协议和报文结构上进行异构性设计，然后增加裁决调度机制实现威胁定位和动态重构，最后对所提架构进行了晶圆级芯粒流片验证。实验表明，所设计的安全互连接口架构在有限资源开销下具有良好的威胁检测、定位与动态防御效果。

关键词：软件定义晶上系统；动态异构冗余；硬件安全；拒绝服务；内生安全
中图分类号：TP309.2
文献标志码：A
DOI: 10.11959/j.issn.1000–436x.2024190

Secure interface architecture for the software defined system on wafer

LI Peijie, SHEN Jianliang, GUO Wei, CAO Zhipeng, MEI Bo
Institute of Information Technology, Information Engineering University, Zhengzhou 450002, China

Abstract: To address the lack of dynamic and heterologous characteristics for interconnect interface in software defined system on wafer, a dynamic heterologous redundancy secure interface (DHR-SI) architecture was proposed to maximize the reuse of functional logic. First, based on software defined interconnect technology, the heterogeneous characteristics were implemented in terms of circuit structure, transmission protocol, and message content. And then an arbitration scheduling mechanism was designed to achieve threat localization and dynamic reconfiguration. Finally, the architecture was validated and tested through a wafer scale chiplet. The experimental analysis shows that the proposed DHR-SI architecture has excellent threat detection, localization, and dynamic defense capabilities with limited overhead.

Keywords: software defined system on wafer, dynamic heterogeneous redundancy, hardware security, denial of service, endogenous safety and security

0　引言

随着人类社会迈入万物智联时代，现有信息系统基础设施中的传感、计算、通信、存储和安全技术都将迎来巨变，软件定义晶上系统（SDSoW, software defined system on wafer）将异构异质芯粒通过高密度集成工艺集成到晶圆基板上实现信息系统高动态的应用部署，是未来信息系统基础设施的“芯”物理底座和新技术物理形态[1-2]。SDSoW 具有复杂的广义功能安全问题[3]，需要构建具备动态异构冗余（DHR, dynamic heterogeneous redundancy）的 SDSoW 内生安全架构[4]。互连接口作为连接异构异质芯粒的关键，其安全性直接影响整个系统，如何构建动态异构冗余的安全互连接口

收稿日期：2024–07–23；**修回日期：**2024–09–28
通信作者：李沛杰，lipeijie@csivo.com
基金项目：国家重点研发计划基金资助项目（No.2022YFB4401401）
Foundation Item：The National Key Research and Development Program of China (No.2022YFB4401401)

（SI, security interface）架构并兼顾由此引入的系统开销成为必须解决的问题。

当前互连接口电路的研究主要集中在实现异构集成系统的高密度互连[5]和高性能通信[6]需求，采用开源静态通信协议[7-8]解决芯粒可靠互连问题缺乏动态性，攻击者可针对接口通信协议发起定制化的网络攻击。互连接口电路中极易植入硬件木马或后门，受到不可信第三方的攻击。因此需基于现有接口协议研究互连接口的安全结构技术。当前以片上系统和2.5D/3D IC中的研究[9-11]最具代表性，这些技术通常通过加密或访问控制保护通信数据的安全，本质上是静态的，难以适应多样化的安全需求。为解决该问题，文献[12-16]通过接口动态性和冗余性应对多样化的安全威胁，证明了动态性、冗余性在异构集成芯片中的有效性。文献[12]提出的动态可配置安全接口，能够防护集成电路（IC）免受信息窃听、信息完整性攻击和拒绝服务（DoS, denial of service）等多种安全威胁。文献[13]设计了一种全面的接口安全管理框架，可动态监测和应对多样化安全威胁。文献[14]提出一种基于混淆微片和历史信息的动态安全防护方法。文献[15]通过在节点出口添加加密标签和入口检测标签，实现了信息窃听攻击的定位，并通过位混淆方法实现窃听攻击动态防护。文献[16]通过复用原始通信协议进行动态数据保护或者安全监测。由于受到IC资源限制，这些安全结构只允许在有限状态内进行动态配置，本质上仍然是静态的，攻击者可通过侧信道等方法分析获得其变化规律，从而继续发起攻击。此外，这些研究仍主要集中在片上系统解决知识产权核（IP）之间网络通信的安全问题，没有涵盖集成系统芯粒互连的安全需求，需要进一步结合SD-SoW的结构特性同时兼顾芯粒间和网络间互连安全特性的一体化安全互连接口架构。

本文主要研究工作如下。

1) 提出一种动态异构冗余安全互连接口（DHR-SI）架构。在兼顾资源开销的前提下设计了一种软件定义互连接口（SDII, software defined interconnect interface）电路，通过增强接口的动态异构冗余特性提升安全性。

2) 提出一种与业务处理相匹配的安全防御方法。通过在现有安全防御机制中增加决策环节，形成检测、捕获、隔离、判决和恢复（DCIDR）机制，不仅提升安全自管理能力，还可有效降低资源消耗。

3) 将所提架构在晶上安全互连芯粒中进行了流片，并基于该芯粒构建了软件定义晶上互连网络系统。对所提架构进行了安全防御测试和性能开销评估，验证DHR-SI的安全性和高效性。

1　接口结构及安全威胁分析

为简化分析且不失一般性，本文以图1(a)所示

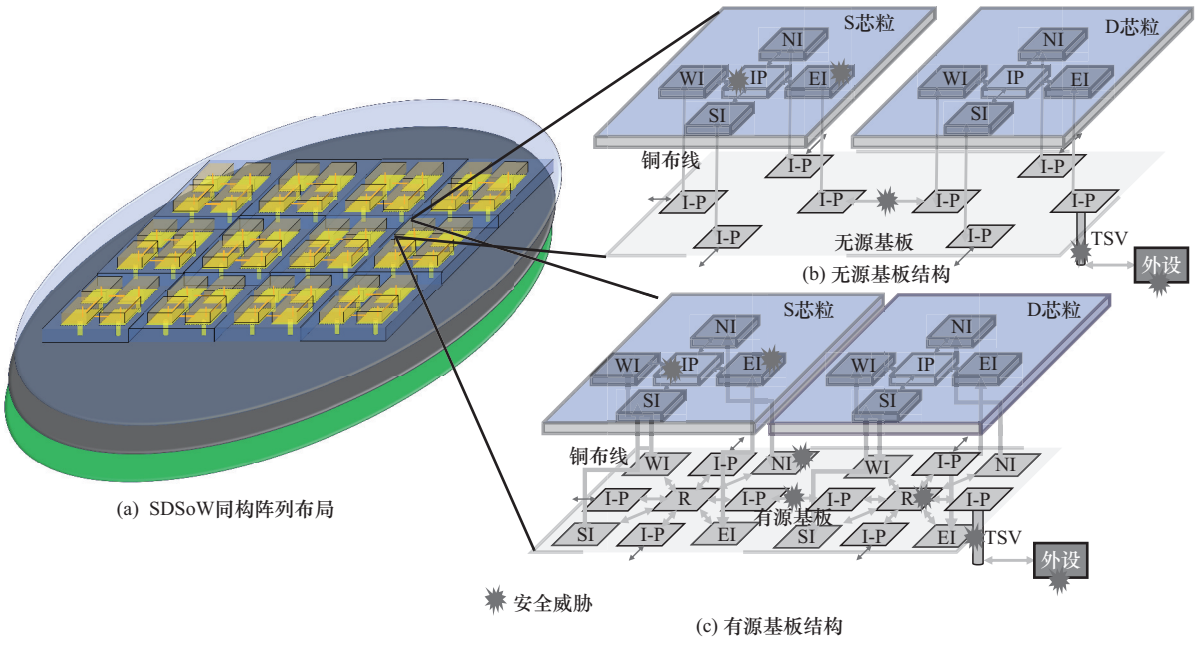


图 1　SDSoW互连结构示意

的同构阵列布局为基础，分析图1(b)所示的无源基板结构和图1(c)所示的有源基板结构，其中，NI、SI、WI和EI分别表示布局在芯粒物理位置四周的互连接口电路[17-18]，I-P表示仅有物理连线的接口电路。互连接口通过路由R连接，兼有片上系统网络接口的网络传输特性和芯粒间互连的端到端传输特性。

如图1所示，SDSoW互连接口面临4个部分的安全威胁：继承第三方芯粒的硬件安全威胁，包括芯粒内部恶意IP以及第三方互连接口电路；晶圆级基板的硬件安全威胁，包括设计与制造过程中嵌入的木马和漏洞等；不确定物理失效或硬件木马导致的功能安全威胁，如凸点开裂、铜布线失效、硅通孔（TSV, through silicon via）失效、热应力故障等；来自系统外部外设的安全威胁。这些安全威胁可以独立发生，也可以以复合形式触发一系列安全问题，包括信息窃听、信息完整性攻击和DoS等。

为最大限度复用互连接口功能逻辑，一体化解决SDSoW的安全威胁，SI需在原有互连接口特性基础上新增如下设计要求。

R1 报文检测与处理要求。在芯粒间可靠互连基础上，接收侧和发送侧分别进行报文异常检测。

R2 报文处理要求。在网络可靠互连基础上，接收侧直接转发非本地报文，发送侧检查重复报文；接收侧本地报文通过数据完整性检查后传输至本地IP；本地发送报文数据完整性计算后发送。鉴于互连接口协议的开源特性，攻击者会基于协议漏洞或内嵌木马发起攻击，因此必须在兼容接口协议前提下设计模糊的互连接口结构。

R3 动态性。互连接口内的处理模块应该具备动态特性，允许软件或硬件操作实现结构可变。

R4 异构性。在R2基础上，互连接口内部处理模块的不同组合可实现异构的协议处理模式。

R5 冗余性。同一芯粒不同互连接口互为冗余。

R6 访问控制要求。本地报文的访问控制不在互连接口实现，但非法访问需反馈至互连接口。

R7 系统运行前要求。每个芯粒从3个方向向相邻芯粒发送测试报文，芯粒不检查接收报文的数据完整性，而是对比来自不同互连接口的报文数量及内容。任何不匹配情况都可能指示端口受到攻击，并将被标记停用。

R8 系统运行时要求。每个芯粒定期或在检测到异常时向相邻芯粒发送测试报文，芯粒不检查接收报文数据完整性，而是对比来自不同互连接口的报文数量及内容。任何不匹配的情况都可能指示端口受到异常攻击，该端口将被标记并停用。若无异常，基于相邻侧测试报文进行芯粒间信息协商。

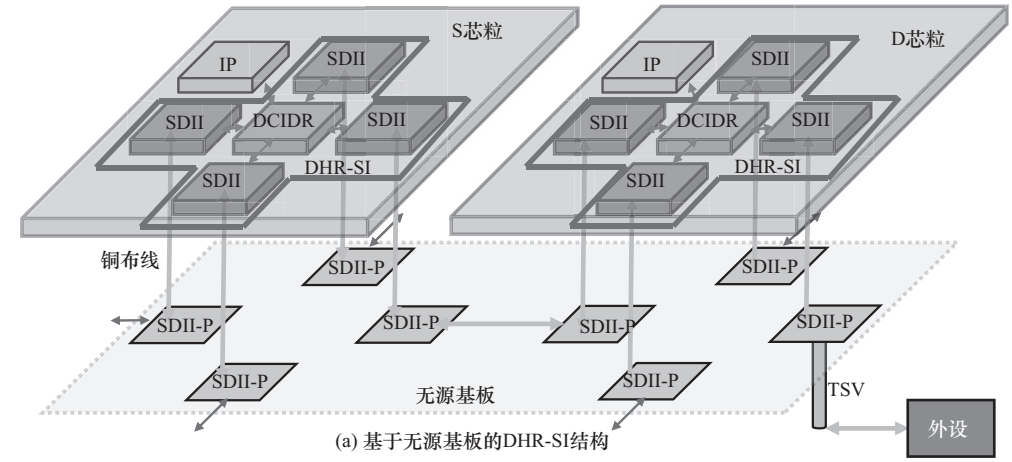
2　DHR-SI结构设计

2.1　总体结构设计

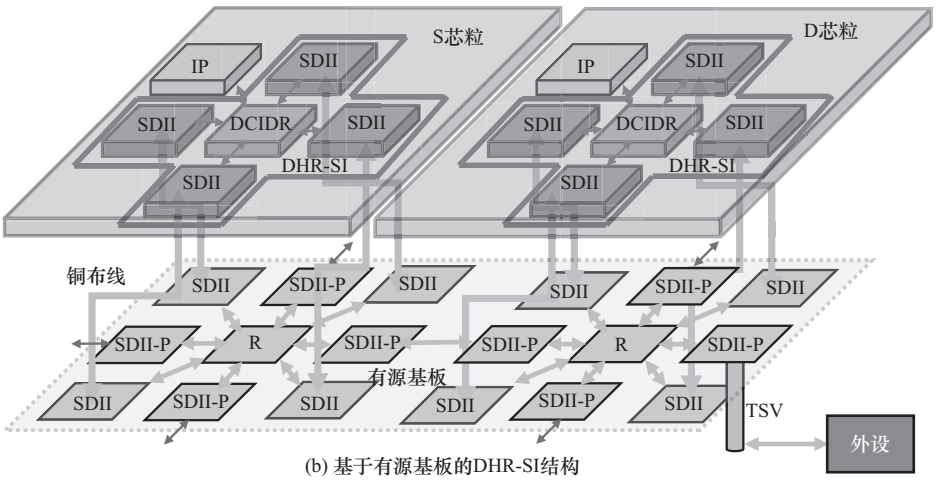
基于上述要求，本文设计如图2所示的DHR-SI总体结构，其中SDII基于开源互连接口协议[7-8]实现各层功能，确保芯粒间互连，满足R1设计要求，并在现有软件定义互连（SDI）技术[19]、异构协议互连互通的接口电路[20]及软件定义协议控制器架构[21]基础上设计满足R3~R5的SDII电路。在无源基板结构中，芯粒的SDII与基板SDII-P（仅有物理连线的SDII）通过TSV连接，基板SDII-P之间通过布线层连接；在有源基板结构中，芯粒SDII与基板SDII通过TSV连接，基板路由R通过SDII-P接口互连。DCIDR模块一体化处理互连接口故障和威胁，满足R2设计要求。DCIDR在不分析本地报文进程号等负载内容的前提下对报文内容进行检测，满足R6~R8设计要求。

为实现芯粒间互连和网络互连，芯粒间传输报文在兼容开源芯粒间互连协议的基础上，同样需具备动态性，使报文核心信息在物理位置上异构。其中主通路报文头信息各字段均可软件定义，头信息中增加源地址和目的地址字段。主通路增加固定格式的定时发送协商测试报文和异常发送检测测试报文，协商测试报文负责与相邻接口交互SDII的混淆结构信息，检测测试报文通过复制捕获到的异常报文信息进行异常检测与定位。

基于DHR-SI的结构及传输报文的特征，图3展示了DHR-SI运行状态转移。SDSoW通过运行前测试标记出异常芯粒和路径，在此基础上，每个SDII首先依次进行自协商，完成出入口协议、SDII内部互连结构、算粒接口及配置等参数的交换和统一，当链路异常或DCIDR决策需进行端口重置时，SDII重新自协商。自协商成功的SDII向相邻芯粒发送速率协商码，进行速率协商，若协商失败，链路根据先验信息设置固定速率进行链路状态测试，测试通过的SDII采用预设置速率通信，否则标记为异常接口。速率协商后，SDII向相邻芯粒发送协



(a) 基于无源基板的DHR-SI结构



(b) 基于有源基板的DHR-SI结构

图 2　DHR-SI 总体结构

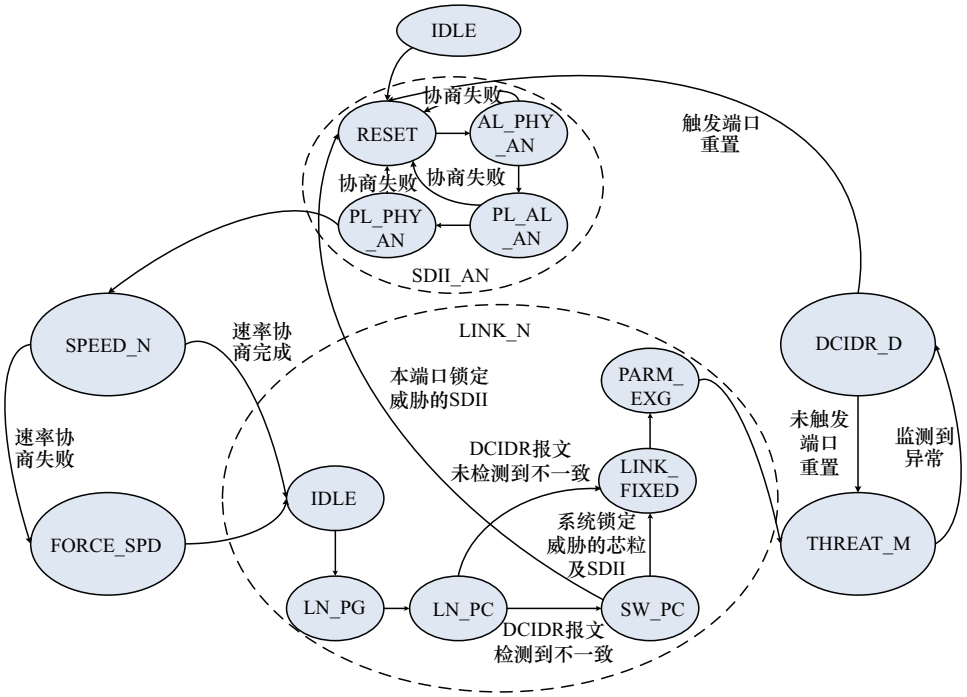


图 3　DHR-SI 运行状态转移

商测试报文，相邻芯粒比较接收到的测试报文信息，若检测异常，首先标记路径不可信，然后向上游依次执行异常检测，直至定位异常接口，此时DCIDR重置异常SDII并重新自协商。若检测无异常，测试报文的最小传输路径将被作为芯粒间主通路数据传输的路径，并根据协商报文交换链路双方参数。链路初始化完成后，不同芯粒间可进行数据交互，DHR-SI持续监测交互数据，并由DCIDR进行策略裁决。

2.2　SDII结构设计

为实现接口结构的动态性和异构性，本文将原有刚性互连接口电路算粒化和软件定义化，引入SDI算粒连接所有功能算粒，然后根据业务驱动[21]，动态构建与业务匹配的电路结构。如图4所示，SDII由软件定义协议层（SDPL, software defined protocol layer）、软件定义适配层（SDAL, software defined adapter layer）和软件定义物理层（SDPHY, software defined physical layer）构成。SDI内部由多个SDI_8组成，每个SDI_8由4路Mux电路和D触发器组成，其接口可基于业务软件定义信号含义。基于SDI构建的SDII在接口和功能算粒的互连上均呈现高动态特性，内部结构对外设和IP均不可见，外设和IP难以发起注入式攻击。SDII在完成自协商后在SDPHY中通过博弈论模型[22]完成速率和通信协议协商，在SDAL中，链路训练（Link Training）模块和控制序列生成与检测（CTL）模块完成链路参数交换，并在替换和重排序（Replace & Reorder）模块中存储协商的参数信息。

安全威胁的触发通常通过匹配特定组合[14]实现，SDII在SDPHY中增加可灵活配置的码流混淆电路B_Ob和B_DeOb，分别在码流级和报文级实现报文模糊，一旦触发SDII重置，码流混淆和重排序电路就会动态切换，原有触发威胁的组合将失效。

为实现安全威胁的检测和定位，SDAL在接收侧设计循环冗余校验（CRC, cyclic redundancy check）模块CRC Chk，当CRC异常时，SDPL的TX Retry进行包重传并记录重传次数，超过最大重传限制时，发送侧丢弃该报文，DCIDR触发SDII重新协

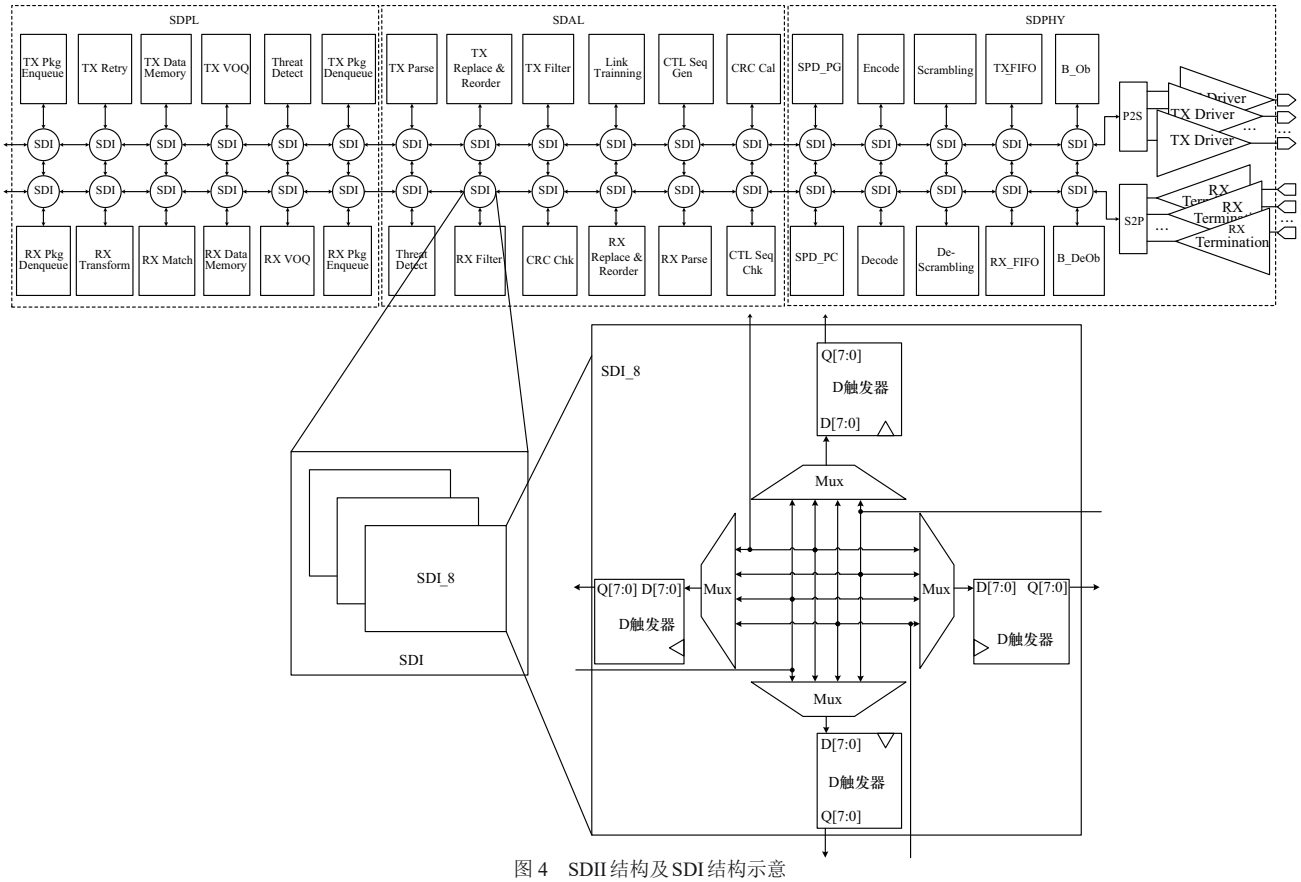


图 4　SDII结构及SDI结构示意

商，TX Filter 过滤发送报文，Replace & Reorder 动态切换重组规则。由于 CRC 具有漏检率，为应对即时信息窃听攻击，TX Parse 解析待发送的临近报文，对除 CRC 和目的地址字段外的数据进行 XOR 校验和对比，校验值相同但目的地址不同的报文被认为存在信息窃听（多播和广播除外），此时 SDII 重新协商，Replace & Reorder 动态切换重组规则。

SDPL 在收发侧的虚拟队列对入队报文均设置最大存活时间（TTL, time to live），可基于 TTL 机制检测 DoS 攻击。如图 5 所示，DoS 攻击存在 3 种基本的攻击场景：①攻击链路上只有一个攻击节点，且没有其他节点与被攻击节点 V 有通信业务；②攻击链路上有多个攻击节点；③攻击链路上只有一个攻击节点，但还有其他节点与被攻击节点 V 有通信业务。为精确定位 DoS 攻击，本文主要基于 TTL 机制在 DCIDR 中实现一种实时检测与定位算法，以应对拥塞、致瘫、DoS 等的威胁，具体如 3.3 节所述。

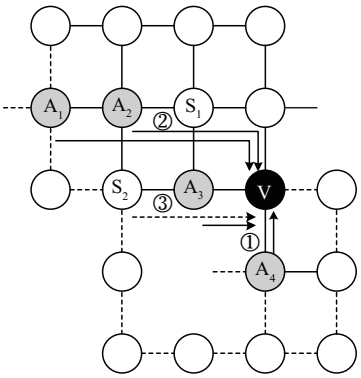


图 5　SDSoW 中典型的 DoS 攻击场景

2.3　DCIDR 结构设计

如图 6 所示，DCIDR 由检测、捕获、隔离、决策和恢复模块组成，可对 SDII 在链路上检测到的异常和威胁进行统计，进而执行对应威胁的隔离、决策和恢复机制。为减少不必要的开销，DCIDR 为 SDPHY、SDAL 和 SDPL 分别设置专用捕获空间，捕获异常字符或异常报文头信息，任何检测到的威胁都会触发中断并告知软件系统，或形成记录

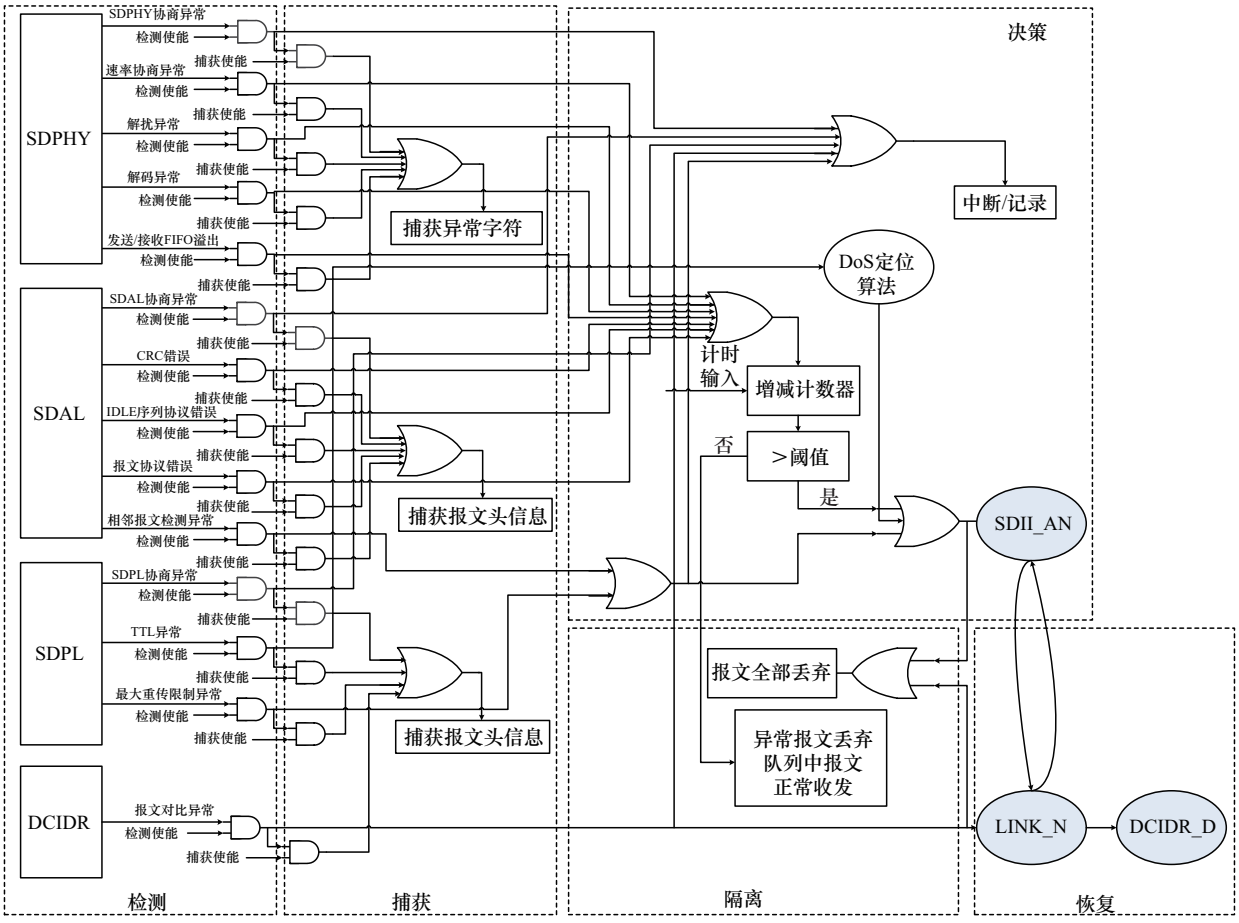


图 6　DCIDR 结构

文件便于查看历史信息。

按照安全威胁导致功能异常的严重性，DCIDR将异常分为如表1所示的3个级别，不同级别异常触发的决策、隔离与恢复机制不同。

频繁决策可能导致误判并影响性能，因此DCIDR设计了一个随时间递减和随威胁检测递增的增减计数器。当计数超过阈值时，表明短时间内检测到大量异常，端口可能受到了安全攻击或不确定物理失效，此时DCIDR动态重置端口。特别地，当端口检测到相邻报文检测异常、最大重传异常和报文对比异常时，DCIDR直接重置异常端口。当检测到TTL异常时，DCIDR执行如算法1和算法2所述的DoS攻击实时检测和定位算法。当端口动态重置时，所有报文全部丢弃，DHR-SI将重新协商。对于未触发重置的威胁，为避免过保护，端口将实行隔离操作，仅丢弃异常报文。

算法1　DoS攻击实时检测算法

DHR-SI(i)的SDII在t时刻入队数据包pkg

1) TTL计时器启动
2) SDII(i).TTL_event = 0
3) if pkg出队 then
4)　TTL计时器清零
5) else if TTL超时 then
6)　SDII(i).TTL_event = 1
7) else
8)　TTL计时
9) end if

算法2　DoS攻击实时定位算法

所有SDII(i).TX_TTL_event = 1的节点组成集合$R=\{\text{DHR-SI}(i), \text{DHR-SI}(i).\text{TX_TTL_event}=1\}$；所有被移除$R$的节点组成疑似攻击集合$\text{SR}=\{\text{DHR-SI}(j), \text{DHR-SI}(j).\text{DoS_Attacker}=1\}$；所有确定的攻击节点组成确定攻击集合$\text{CR}=\{\text{DHR-SI}(m), \text{DHR-SI}(m).\text{DoS_Attacker}=2\}$；

1) $\forall i, \text{DHR-SI}(i) \in R$
2) if $R = \varnothing$ then
3) 将SR中所有DHR-SI(j)移入CR，DHR-SI(j).DoS_Attacker=2；
4) else
5)　if DHR-SI(i)的所有其他SDII的接收TTL均未超时 then
6)　　if SR = ∅ then
7)　　DHR-SI(i).DoS_Attacker=1

表1　不同级别异常的隔离决策与恢复机制

异常级别	异常名称	决策	隔离与恢复
1	临近报文检测异常	SDII重置	丢弃所有报文，上游SDII重置
	TTL异常	DoS定位	丢弃所有报文，定位到的DHR-SI禁用
	最大重传限制异常	SDII重置	丢弃所有报文，上游SDII重置
	报文对比异常	定位异常SDII	异常SDII丢弃所有报文，异常SDII重置
2	速率协商异常	增减计数器统计	重新协商
	解扰异常	增减计数器统计	复位PHY
	解码异常	增减计数器统计	复位PHY
	发送/接收FIFO溢出	增减计数器统计	复位PHY
	CRC错误	增减计数器统计	异常报文丢弃
	控制序列协议错误	增减计数器统计	异常序列丢弃
	报文协议错误	增减计数器统计	异常报文丢弃
3	SDPHY协商异常	增减计数器统计	重新协商
	SDAL协商异常	增减计数器统计	重新协商
	SDPL协商异常	增减计数器统计	重新协商

8) 将DHR-SI(i)移入SR
9) 置位DHR-SI(i).enable=false
10) 重新执行算法1
11) 更新R，跳到步骤2)
12) else
13) if DHR-SI(i)与SR中的DHR-SI(j)有重叠路径 then
14) 置位DHR-SI(i).enable=true
15) 更新路径与DHR-SI(i)不重合，重新执行算法1
16) 更新R
17) if DHR-SI(j)$\in R$ then
18) 将DHR-SI(j)移入CR，DHR-SI(j).DoS_Attacker=2
19) 置位DHR-SI(j).enable=false
20) 更新CR和R，跳到2)
21) else
22) 将DHR-SI(j)移除SR
23) 更新SR，跳到步骤2)
24) end if
25) else
26) 将DHR-SI(j)移入CR，DHR-SI(j).DoS_Attacker = 2
27) 置位DHR-SI(j).enable=false
28) 更新CR，跳到步骤2)
29) end if
30) end if
31) else
32) 重新执行算法1
33) end if
34) end if

算法1中，步骤1)~步骤4)执行收发侧入队报文的TTL计时，步骤5)~步骤6)执行收发侧TTL异常检测。算法2中，每个节点初始R、SR和CR均为空，步骤2)~步骤4)执行定位算法的开始和结束，当节点检测到发送侧TTL超时，R将不为空（图5中$R=\{A_1,A_2,S_1,S_2,A_3,A_4\}$），此时开始执行DoS攻击定位直至$R$重新为空。步骤5)~步骤12)执行疑似攻击点的定位，对于所有检测到发送侧TTL超时的SDII，DCIDR检测其余3个SDII的接收侧TTL是否超时，若未超时，表明该节点是与V之间有业务通信的末端节点，当SR为空时，将其放入SR并标记禁用，重新执行算法1，并更新R，此时$R=\{A_2,S_1,A_3\}$，SR$=\{A_1,S_2,A_4\}$。步骤13)~步骤30)执行疑似节点的确认或排除，在R和SR均不为空时，检测R中的节点是否与SR中节点有重叠路径（如图5所示，A_1与A_2及S_1均有重叠路径，S_2与A_3有重叠路径），若有，则将SR中的对应节点移出并重新使能，同时将其传输路径更新到与原路径不重叠，重新执行算法1。由于S_2并不是攻击节点，在路径变更后，将不会触发TTL异常，因此被移出SR（步骤21)~步骤22)），但由于A_1是攻击节点，即使路径变更，仍会触发TTL异常，因此被直接移入CR并标记禁用（步骤17)~步骤20)），此时$R=\{A_2,S_1,A_3,A_4\}$，SR$=\{A_4\}$，CR$=\{A_1\}$。对于SR中与R中节点无重叠路径的节点，一定是攻击节点，直接移入CR（步骤25)~步骤28)），此时，$R=\{A_2,S_1,A_3,A_4\}$，SR$=\varnothing$，CR$=\{A_1,A_4\}$。重新执行算法1，直到R为空，此时若SR中仍有节点，则一定是攻击节点，将其移入CR，A_2被确认为攻击节点后，S_1将被排除，算法结束。

3 测试与仿真分析

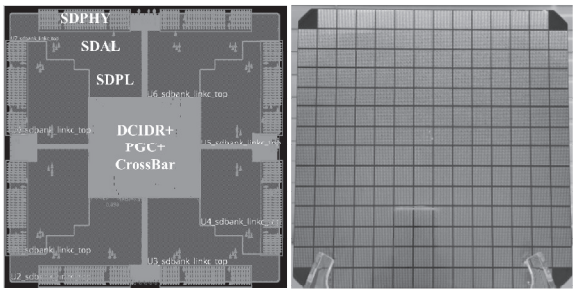
3.1 安全性分析

本文在电路结构和报文结构上设计了多层次的动态异构冗余。在电路结构上，DHR-SI与芯粒内部IP物理隔离，芯粒间的互连接口彼此异构，互连接口物理冗余，可有效规避恶意芯粒发起的嗅探和窃听攻击。在报文结构上，由于可定义的数据报文结构，核心信息隐藏在报文中且动态可变，攻击者很难按照位置和信息匹配发起攻击。在威胁处理上，由于SDII对转发报文不重新计算CRC，因此任何针对数据报文的无差别攻击都会在下游SDII接收侧被检测到；发送侧基于TTL的DoS防御机制能够有效定位任意场景下的分布式DoS攻击，任何突发性的大流量都会被截留在本端口处理，避免了大量合法数据包攻击进入下级。DCIDR基于3个异常级别触发的安全防御机制，既可以基于端口的动态重置保障接口免受真正安全攻击，也可避免过保护导致性能折损。

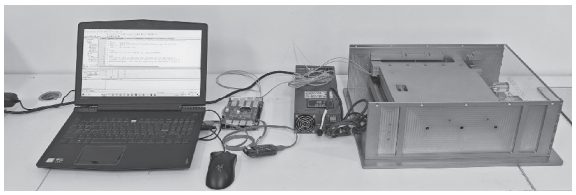
3.2 安全防御测试

本文在40 nm CMOS工艺上将DHR-SI电路在晶上安全互连芯粒进行了设计并流片，其版图如

图 7(a)所示，全芯粒 8 个 SDII 共享中心区域的 DCIDR、核心交换 Crossbar 及内嵌的包生成与检测（PGC, packet generate and check）模块，192 个芯粒键合到无源基板上形成如图 7(a)所示的晶圆级互连网络芯片。基于键合后的芯片与供电、散热、微组装、机箱等分部件组装形成如图 7(b)所示的软件定义晶上互连网络系统测试环境。



(a) 晶上安全互连芯粒版图及贴装后的芯片实物



(b) 软件定义晶上互连网络系统测试环境

图 7　晶上安全互连芯粒及软件定义晶上互连网络系统测试环境

测试时，通过上位机后门控制芯粒的 PGC 生成报文的不同信息模拟不同安全威胁。初始设置系统中所有芯粒的 PGC 均使能，生成 40% 吞吐量的随机报文。按照表 2 模拟恶意芯粒行为，分别对信息完整性、信息窃听和 DoS 等的攻击检测效率（ADT, attack detection time）和安全防御效率（DSR, defense success rate）进行测试。

ADT 是恶意芯粒发起攻击到 DHR-SI 检测到攻击之间的时间。芯粒发起攻击以软件对 PGC 后门配置时刻计算，检测到攻击以中断触发时刻计算。

DSR 是攻击被检测到且执行安全防御策略后，对相同攻击的防御成功率。一般用攻击定位率（ALR, attack location rate）和攻击防御率（ADR, attack defense rate）的乘积表示。

3.2.1　信息完整性攻击测试

如图 8(a)所示，信息完整性攻击的 ADT 和报文长度及最大重传限制次数紧密相关，这主要是由于 CRC 要在报文接收结束时完成，因此报文越长，最大重传次数越大，报文发送到对端的时间、对端触发 CRC 错误异常的时间及触发最大重传限制异常的时间就越长。由于 DHR-SI 分布式的异常检测机制，信息完整性攻击不会蔓延至整个网络，具有更优的攻击防御效率。

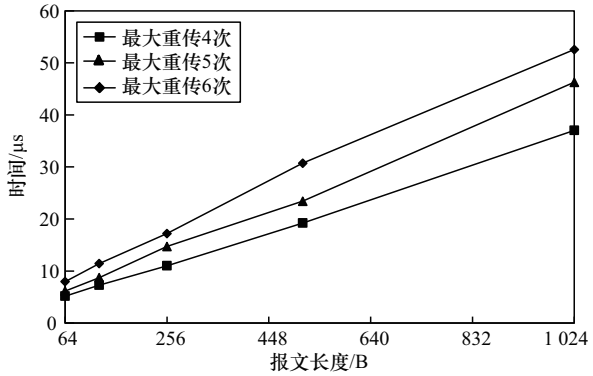
如图 8(b)所示，Crypt[23]和 P-sec[24]等 e2e 加密算法具有极高的 ALR，但由于源端加密方式难以定位威胁且加密算法固定，无法有效防御相同的安全攻击。Key+ob[15]和 L-ob[14]等 s2s 安全防御算法需要通过每节点密钥检查定位威胁，由于算法具有漏检率，ALR 较低；但由于混淆设计可动态防御相同威胁再次攻击，因此具有极高的 ADR。DHR-SI 在检测到威胁后，会触发端口重置并混淆报文结构，有效防御相同威胁的再次攻击，与 s2s 算法一样，DHR-SI 的 CRC 具有漏检率，其 ALR 较低，因此在 SDII 设计中，可以通过增加类似哈希校验的方式实现更高的 DSR。

3.2.2　信息窃听攻击测试

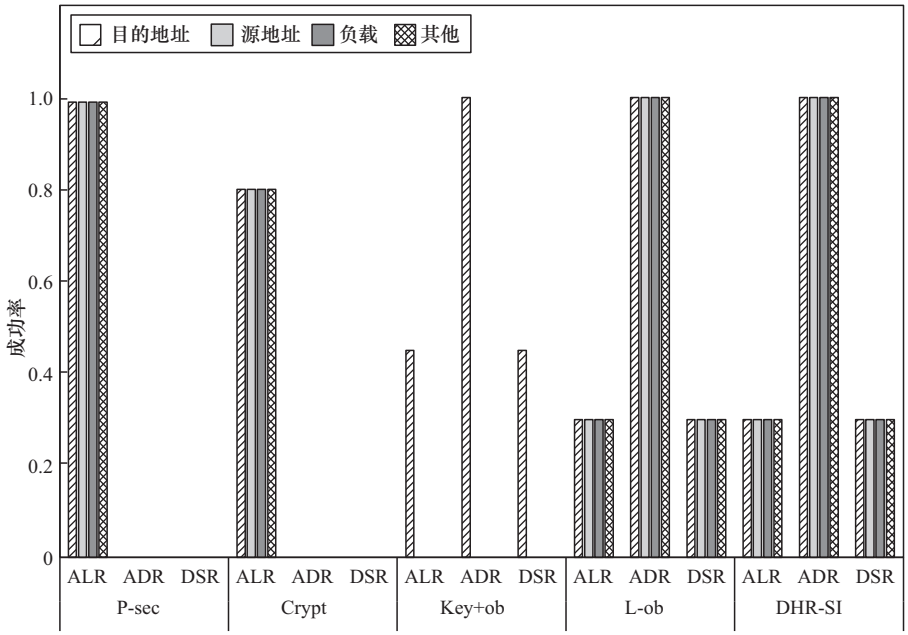
图 9 给出了不触发 CRC 错误的信息窃听攻击的 ADT 和 DSR 测试结果。相比于 SIM[25]，SDII 具有更大的异常检测范围，有效检测间隔内的窃听攻击 DHR-SI 都可以准确检测和定位，但超过队列最大间隔的窃听报文将漏检。与信息完整性攻击一样，Crypt[23]等的加密防御由于头信息一般不加密，因此难以在检测到异常后定位攻击。不同于 Key+ob[15]及 L-ob[14]存在漏检率的情况，DHR-SI 通过增加极小的 XOR 电路逻辑，实现与发送队列深度匹配的信息窃听攻击检测范围，具有极高的 ALR，并通过重构电路结构、通信协议和报文结构，使原有的信息窃听失效，实现极高的 DSR。

表 2　测试环境

后门配置项	报文长度/B	报文密度	报文内容	攻击节点/个	最大重传次数/次
信息完整性攻击	(64,128,256,512,1024)	单包多次触发	随机转发报文，CRC 错误	1	4~6
信息窃听攻击	(64,128,256,512,1024)	单包多次触发，间隔 0~7	目的地址不一致，CRC 正确	1	—
DoS 攻击	64	(20%,40%,60%,80%,100%) 吞吐量	最高优先级，目的地址一致，CRC 正确	1~5	—



(a) ADT测试结果



(b) DSR测试结果

图 8　信息完整攻击的ADT和DSR测试结果

3.2.3　DoS攻击测试

基于TTL的DoS攻击更关心实时定位情况，如图10(a)所示，ADT与恶意节点的数量及分布关系极大，场景①由于不存在重叠攻击路径，实时定位算法仅需执行一次，因此ADT与恶意节点数量无关。但对于场景②和场景③，由于需要确认疑似攻击节点或排除正常节点，因此ADT和重叠路径上攻击节点的数量或需要排除的合法节点数量呈线性递增关系。由于DoS攻击更容易隐藏在合法的攻击节点中，因此场景③所需的定位时间比场景②更长。图10(b)给出了DoS攻击DSR测试结果，可以看出，系统在定位到DoS攻击后均会禁用该节点，DSR就是ALR，与DoSTier[12]和ML-DoS[26]检测方法相比，基于TTL的DoS定位算法能够实现与片内一样的ALR。

3.3　性能与开销评估

3.3.1　功耗和面积评估

DHR-SI主要基于开源互连接口进行了算粒的软件定义化设计，并新增了SDI算粒、XOR检测、源目的地址解析与封装、威胁决策、DoS定位算法及码流混淆电路等功能。与文献[21]一样，软件定义化的接口电路设计不会带来大的面积和功耗开销，而码流混淆电路是在接口冗余功能基础上对重映射机制的调整，几乎不引入额外开销。本文基于晶上安全互连芯粒的物理实现结果，对其开销进行了统计分析，如表3所示，相比于同样支持多种安全威胁检测、定位与防御的可重构多层次安全机制[12]及具有码流混淆和动态重构安全防御机制的设计，DHR-SI可以以1.96%的面积开销和5.45%的功耗开销实现接口的动态异构冗余。

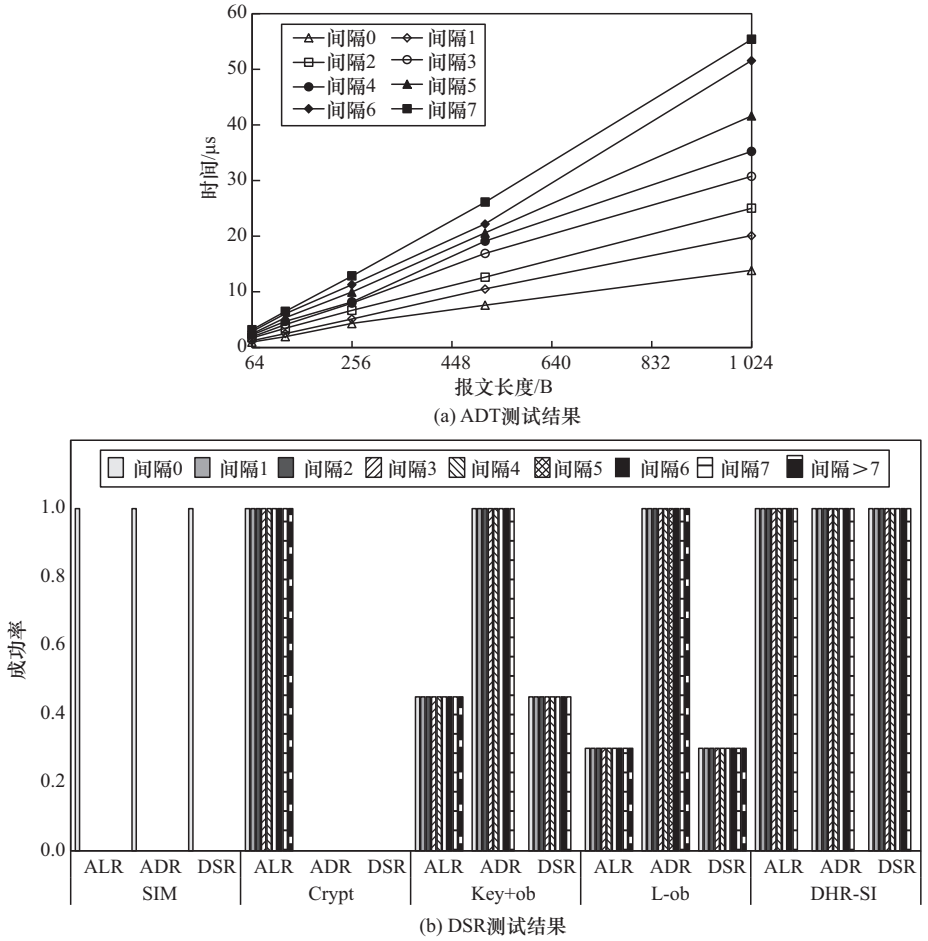


图 9　信息窃听攻击的ADT和DSR测试结果

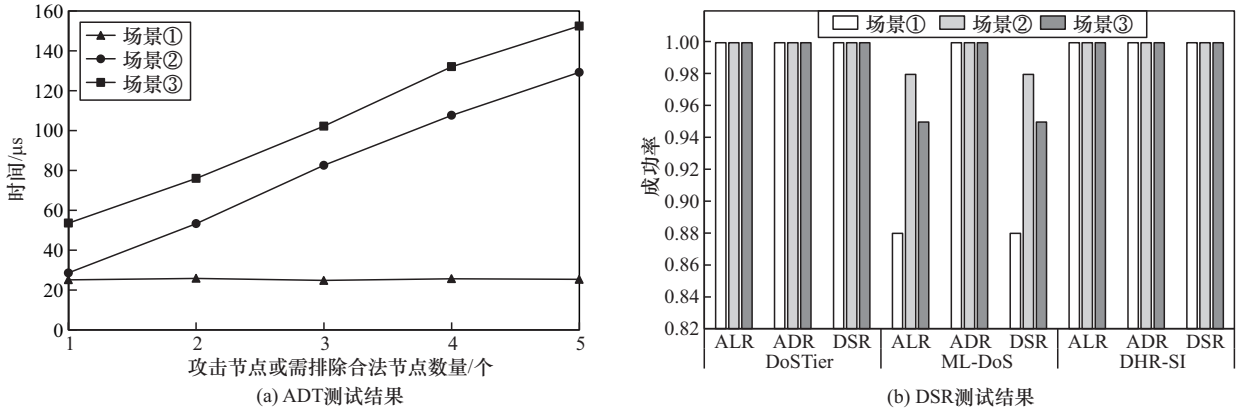


图 10　DoS攻击的ADT测试结果

3.3.2　时延评估

受限于实际测试环境，本文基于OMNeT环境对16×16个节点的网络模型进行仿真，评估引入DHR-SI对系统时延的影响。在仿真环境中，节点以不同报文密度发送64 B报文，攻击节点在每端口以25%吞吐量发送恶意报文，分别分析对比信息完整性攻击、信息窃听攻击和DoS攻击在无恶意攻击有安全策略（NAWS, no attack with secure）、有恶意攻击无安全策略（WANS, with attack no secure）和有恶意攻击但执行安全策略（WAWS, with attack with secure）3种情况下系统的平均时延。

为分析稳定业务处理系统中，攻击节点变化对系统时延的影响，设定节点发送数据吞吐量固定为40%。如图11所示，对于信息完整性攻击和

信息窃听攻击，攻击节点密度对系统时延影响不大（平均时延分别增加7.5%和7.8%），这使得恶意节点能够更好地躲避系统检测，但由于DHR-SI分布式的异常检测与防御，因此能够更好地定位此类攻击。但对于DoS攻击，攻击节点密度越大，系统所展现出被攻击的特征越明显，DoS攻击更容易暴露，实时检测与定位时间越长，从而导致了系统平均时延的增大（平均增加32.7%，最大61.1%）。

表3　　DHR-SI的功耗和面积开销

开销内容	面积/um^2	面积比例	功耗/mW	功耗比例
SDII+DCIDR	37 887 924	—	1 568	—
算粒软件定义化	193 228	0.51%	31.36	2%
SDI算粒	492 543	1.30%	47.04	3%
XOR及存储	18 943	0.05%	1.25	0.08%
地址解析与封装	11 366	0.03%	1.57	0.1%
决策及DoS定位	26 142	0.069%	4.23	0.27%
总体增加比例	7 422 226	1.96%	85.45	5.45%
文献[12]	—	5.70%	—	7.90%
文献[15]	—	2%	—	8.60%

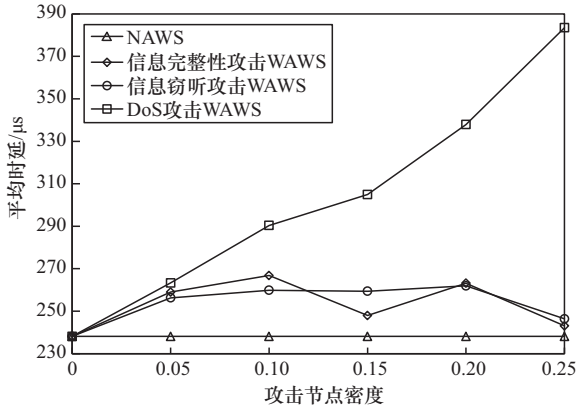


图11　稳定业务下恶意节点密度对系统平均时延影响

为进一步验证攻击对系统的影响，图12模拟了稳定物理结构（攻击节点密度固定）下不同报文密度对系统时延的影响，设定攻击节点密度为20%。从图12可以看出，当系统遭到信息完整性攻击或DoS攻击时，WANS下平均时延显著提高，这主要是由于CRC错误导致节点间不断重传或大量合法报文注入，造成了系统拥塞。信息窃听攻击中单个报文复制对系统时延带来的影响有限，因此WANS下平均时延变化不大（平均73%），这也说明信息窃听攻击更难被发现。系统在3种攻击下执行安全策略后的系统平均时延与基准NAWS相比分别增加4.2%、7.6%和83.5%，其中DoS攻击WAWS下的平均时延增加主要消耗在定位算法执行上，随着恶意节点的定位和禁用，拥塞数据逐渐被丢弃，系统将恢复正常通信。

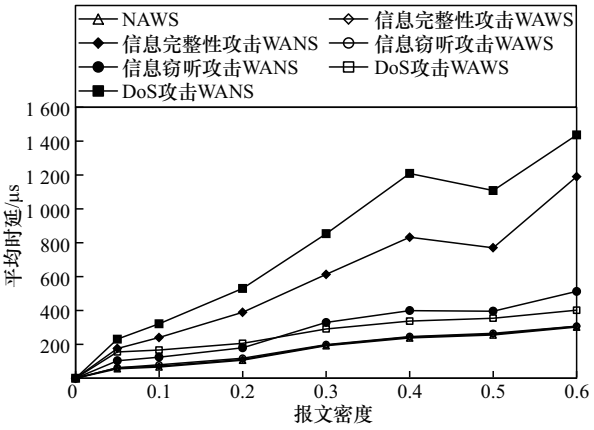


图12　稳定物理结构业务流量对系统平均时延影响

4　结束语

本文对软件定义晶上系统的互连接口安全问题进行了研究。考虑开源协议的不可靠及安全策略的资源开销约束，基于软件定义互连技术实现了一种DHR-SI架构。利用一体化的DCIDR机制实现威胁检测与定位，并通过SDII的动态异构冗余结构特性，实现接口电路结构、接口物理位置和传输报文等多层次的异构，从而提升接口安全特性。基于DHR-SI，实现了一种晶上安全互连芯粒，并基于该芯粒构建的软件定义晶上互连网络系统开展了安全防御测试，测试和仿真结果表明，所设计的安全互连接口电路能够以最小的资源开销实现最优的安全防御。后续还将结合SDNoW的灵活特性，构建安全互连网络架构，连同DHR-SI构建多维DHR内生安全架构，进一步增强SD-SoW的系统安全。

参考文献：

[1] 吴林晟, 毛军发. 从集成电路到集成系统[J]. 中国科学: 信息科学, 2023, 53(10): 1843-1857.
WU L S, MAO J F. From integrated circuits to integrated systems[J].

Scientia Sinica (Informationis), 2023, 53(10): 1843-1857.

[2] 邬江兴, 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 X, LIU Q R, SHEN J L, et al. From SoC to SDSoW: a new paradigm for microelectronics development[J]. Scientia Sinica (Informationis), 2024, 54(6): 1350-1368.

[3] 邬江兴. 工业控制网络广义功能安全问题与解决之道[J]. 信息安全研究, 2022, 8(6): 524-527.
WU J X. Generalized functional safety problems and solutions in industry control network[J]. Journal of Information Security Research, 2022, 8(6): 524-527.

[4] 邬江兴. 网络空间内生安全—拟态防御与广义鲁棒控制[M]. 北京: 科学出版社, 2020.
WU J X. Principle of cyberspace mimic defense-generalized robust control and endogenous security[M]. Beijing: Science Press, 2020.

[5] 李沛杰, 刘勤让, 陈艇, 等. 异构集成互连接口研究综述[J]. 集成电路与嵌入式系统, 2024, 24(2): 31-40.
LI P J, LIU Q R, CHEN T, et al. Research on the heterogeneous integrated interconnect interface[J]. Integrated Circuits and Embedded Systems, 2024, 24(2): 31-40.

[6] JANGAM S, PAL S, BAJWA A, et al. Latency, bandwidth and power benefits of the SuperCHIPS integration scheme[C]//Proceedings of the 2017 IEEE 67th Electronic Components and Technology Conference (ECTC). Piscataway: IEEE Press, 2017: 86-94.

[7] SHARMA D D, PASDAST G, QIAN Z G, et al. Universal chiplet interconnect express (UCIe): an open industry standard for innovations with chiplets at package level[J]. IEEE Transactions on Components, Packaging and Manufacturing Technology, 2022, 12(9): 1423-1431.

[8] ARDALAN S, CIRIT H, FARJAD R, et al. Bunch of wires: an open die-to-die interface[C]//Proceedings of the 2020 IEEE Symposium on High-Performance Interconnects (HOTI). Piscataway: IEEE Press, 2020: 9-16.

[9] CHARLES S, MISHRA P. A survey of network-on-chip security attacks and countermeasures[J]. ACM Computing Surveys, 2022, 54(5): 1-36.

[10] DOFE J, GU P, STOW D, et al. Security threats and countermeasures in three-dimensional integrated circuits[C]//Proceedings of the Great Lakes Symposium on VLSI 2017. New York: ACM Press, 2017: 321-326.

[11] 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.

[12] CHARLES S, MISHRA P. Reconfigurable network-on-chip security architecture[J]. ACM Transactions on Design Automation of Electronic Systems, 2020, 25(6): 1-25.

[13] FACCENDA R F, COMARÚ G, CAIMI L L, et al. A comprehensive framework for systemic security management in NoC-based many-cores[J]. IEEE Access, 2023, 11: 131836-131847.

[14] BORATEN T, KODI A K. Mitigation of denial of service attack with hardware trojans in NoC architectures[C]//Proceedings of the 2016 IEEE International Parallel and Distributed Processing Symposium (IPDPS). Piscataway: IEEE Press, 2016: 1091-1100.

[15] THEJASWINI P, VIVEKANANDA G, ANU H, et al. Hardware Trojan detection and mitigation in noc using key authentication and obfuscation techniques[J]. EMITTER International Journal of Engineering Technology, 2022: 370-388.

[16] FIORIN L, PALERMO G, SILVANO C. A configurable monitoring infrastructure for NoC-based architectures[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2014, 22(11): 2438-2442.

[17] SUNDARAM J, GOPAL S, THOMAS T P, et al. A reconfigurable asynchronous SERDES for heterogenous chiplet interconnects[C]//Proceedings of the 2021 22nd International Symposium on Quality Electronic Design (ISQED). Piscataway: IEEE Press, 2021: 542-546.

[18] PAL S, LIU J Y, ALAM I, et al. Designing a 2048-chiplet, 14336-core waferscale processor[C]//Proceedings of the 2021 58th ACM/IEEE Design Automation Conference (DAC). Piscataway: IEEE Press, 2021: 1183-1188.

[19] 吕平, 刘勤让, 邬江兴, 等. 新一代软件定义体系结构[J]. 中国科学: 信息科学, 2018, 48(3): 315-328.
LYU P, LIU Q R, WU J X, et al. New generation software-defined architecture[J]. Scientia Sinica (Informationis), 2018, 48(3): 315-328.

[20] 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 X, et al. A multi-protocol SerDes circuit for the applications in software defined interconnection system[J]. Acta Electronica Sinica, 2021, 49(4): 817-823.

[21] LI P J, SHEN J L, 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.

[22] 李晓东, 沈剑良, 李沛杰. 基于博弈论模型的物理层协议自协商机制[J]. 现代电子技术, 2023, 46(8): 84-90.
LI X D, SHEN J L, LI P J. Physical layer protocol auto-negotiation mechanism based on game theoretical model[J]. Modern Electronics Technique, 2023, 46(8): 84-90.

[23] CHARLES S, MISHRA P. Securing network-on-chip using incremental cryptography[C]//Proceedings of the 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). Piscataway: IEEE Press, 2020: 168-175.

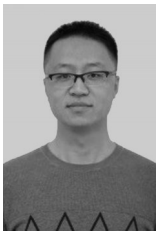
[24] BORATEN T, KARANTH KODI A. Packet security with path sensitization for NoCs[C]//Proceedings of the 2016 Design, Automation & Test in Europe Conference & Exhibition (DATE). Singapore: Research Publishing Services, 2016: 1136-1139.

[25] RAPARTI V Y, PASRICHA S. Lightweight mitigation of hardware Trojan attacks in NoC-based manycore computing[C]//Proceedings of the 2019 56th ACM/IEEE Design Automation Conference (DAC). Piscat-

away: IEEE Press, 2019: 1-6.

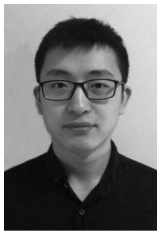
[26] SUDUSINGHE C, CHARLES S, MISHRA P. Denial-of-service attack detection using machine learning in network-on-chip architectures[C]// Proceedings of the 15th IEEE/ACM International Symposium on Networks-on-Chip. New York: ACM Press, 2021: 35-40.

[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、博士生，主要研究方向为软件定义晶上系统、软件定义互连、硬件安全等。

沈剑良（1982– ），男，浙江德清人，博士，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、可重构计算等。



郭威（1990– ），男，北京人，博士，信息工程大学副研究员，主要研究方向为网络空间主动防御、计算机体系结构、人工智能与大数据、内生安全等。

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、互连网络等。

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、硬件木马防御等。