

基于虚拟通道非均匀分布的路由算法

郭林林 李光顺 吴俊华

(曲阜师范大学计算机科学学院 日照 276826)

摘 要 随着片上系统(systems on chip, SoC)集成度的提高, IP核之间的通信成为 SoC 急需解决的问题。近年来提出的片上网络(network on chip, NoC)是解决 SoC 通信问题的一种有效方法。虚拟通道和路由算法是 NoC 设计中的关键技术, 对 NoC 的延时、吞吐量等性能有重要的影响。根据 NoC 负载分布特点, 提出一种新的虚拟通道非均匀分布技术 VCND。该技术在 Mesh 内部使用虚拟通道, 在边界上使用非虚拟通道, 从而减少缓冲单元的数量。同时提出一种改进的无死锁路由算法 CXY(combination XY)。仿真结果表明, 与 XY 路由算法和 XY-YX 路由算法相比, CXY 路由算法提高了网络吞吐量, 并降低了网络平均延时; 相比虚拟通道均匀分布技术, VCND 技术能够以较小的吞吐量和网络延时损失获得可观的缓冲单元利用率提升, 并减少了路由器的面积。

关键词 片上网络, 虚拟通道, 路由算法

中图法分类号 TP393 文献标识码 A DOI 10.11896/j.issn.1002-137X.2014.08.036

Routing Algorithm Based on Non-uniform Distribution of Virtual Channel

GUO Lin-lin LI Guang-shun WU Jun-hua

(School of Computer Science, Qufu Normal University, Rizhao 276826, China)

Abstract With increasing integration of system on chip (SoC), communication between IP cores become an urgent problem. In recent years, network on chip (NoC) has been proposed as an effective solution to the complex on-chip communication problems. Virtual channel and routing algorithm play an important role in NoC design. They have great impact on latency, throughput and other performance of NoC. According to the characteristics of load distribution of NoC, we presented a novel non-uniform distribution technology of virtual channel (VCND). The technology of virtual channel is used in the internal Mesh and non-virtual channel is used on the boundary of Mesh. Hence, the amount of buffer unit is reduced. Then a modified deadlock-free routing algorithm was proposed, called combination XY (CXY). Simulation results show that CXY routing algorithm can improve network throughput and keep low message latency compared with XY and XY-YX routing algorithms. And VCND can save router's area and increase the utilization rate of buffer unit obviously with a little losing of network throughput and latency, compared with uniform distribution technology of virtual channel.

Keywords Network on chip, Virtual channel, Routing algorithm

1 引言

随着半导体技术的不断发展, 单个芯片上集成越来越多的 IP 核, 使用片上网络^[1]代替片上总线成为片上系统通信结构设计的理想选择。NoC 是一种基于网络和路由通信的体系结构, 其核心是将宏观网络技术移植到微观网络芯片设计中, 从体系结构上彻底解决片上总线通信带来的带宽局限、单一时钟同步和通信延时的問題。

路由算法设计的好坏直接影响到 NoC 的性能^[2]。文献[1]提出一种简单、无死锁的 XY 路由算法, 其路由选择首先沿 X 维传输, 然后再沿 Y 维传输。当数据包注入率低时, 网络性能优于其它 NoC 路由算法。当数据包注入率高时, NoC

内部流动着大量数据流片, 易产生拥塞, 导致网络性能下降。文献[3]提出一种动态无死锁路由算法(DyXY), 该算法为数据包选择最短路径。如果存在多条最短路径, 则根据每条最短路径的拥塞情况, 选择拥塞程度最轻的那条路径。文献[4]提出一种无死锁容错路由算法(XYX), 数据包采用 XY 路由算法进行传输, 当传输过程发生故障时, 源节点需要重新发送该数据包, 并且采用 YX 路由算法进行重新传输。文献[5]提出一种间歇性路由算法(IX/Y), 在数据包头流片域保留一位, 当其值为 0 时, 数据包选择 XY 路由算法进行传输; 当其值为 1 时, 数据包选择 YX 路由算法进行传输。文献[6]提出在 Mesh 结构上添加额外链路的路由算法, 该算法能有效地降低数据包传输的平均延时, 并且能确保数据包到达目的节

到稿日期: 2013-10-15 返修日期: 2014-01-31 本文受国家自然科学基金项目(61373027), 山东省优秀中青年科学家奖励基金项目(BS2009DX024, BS2010DX013), 山东省自然科学基金项目(ZR2012FM023), 山东省高校科技计划项目(J09LG34)资助。

郭林林(1988—), 女, 硕士, 主要研究领域为片上网络, E-mail: gl_linlin@sina.cn; 李光顺(1977—), 男, 博士, 副教授, 硕士生导师, CCF 高级会员, 主要研究领域为无线传感器网络、片上网络; 吴俊华(1979—), 女, 博士, 副教授, 硕士生导师, 主要研究领域为无线传感器网络、片上网络。

点的路径是最短路径。文献[7]提出一种无死锁路由算法(XY-YX)。该算法根据当前节点与目的节点的相对位置,选择XY路由算法或YX路由算法。上述路由算法都是针对XY路由算法网络负载不均衡的问题而提出的解决方法,目的是在保证网络无死锁的前提下,尽可能均衡网络负载,提高网络性能。

虚拟通道技术对NoC路由算法的性能有重要的影响^[1]。在数据包注入率较高的情况下,NoC内部容易产生拥塞或死锁,虚拟通道技术能有效地解决该问题。但是虚拟通道技术会额外增加路由器的面积,并且缓冲单元没有被充分利用。因此在保证网络性能的前提下,采用虚拟通道技术时要尽可能减小路由器的面积,提高缓冲单元的利用率。目前虚拟通道研究主要是从网络性能与开销的角度寻求折中点^[8-10],使得网络的整体性能更好。

本文针对NoC负载分布的特点,提出一种新的虚拟通道非均匀分布技术,该技术可提高缓冲单元的利用率,减少路由器的面积;同时提出一种改进的无死锁路由算法CXY,该算法能均衡网络负载,提高网络性能。

2 NoC中VCND技术

2.1 虚拟通道技术

NoC的物理链路实现了路由节点之间的连接,物理链路有两种实现模式:(1)非虚拟通道模式;(2)虚拟通道模式^[7]。非虚拟通道模式的一条物理链路两侧对应一组数据缓冲单元。虚拟通道模式是指多组数据缓冲单元共享一条物理链路,数据缓冲单元之间彼此独立。图1说明了这两种通道模式的不同结构。在非虚拟通道模式下,当一组待传数据占据缓冲单元时,其它组数据不能获得物理链路的使用权。对于虚拟通道模式,当一组待传数据发生阻塞时,其它组数据可以获得物理链路的使用权。因此虚拟通道能提高物理链路的利用率,减轻网络拥塞,提高网络性能,同时也会带来路由器面积的增加以及路由仲裁控制复杂度的增加。为了更好地提高网络整体性能,我们在使用虚拟通道时,要尽可能地根据网络负载分布使用虚拟通道,进而减少路由器面积。减少路由器的缓冲单元数目是降低路由器面积的一种有效方法^[11]。

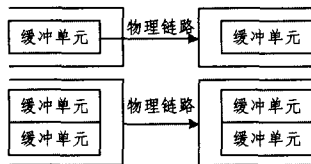


图1 非虚拟通道与虚拟通道结构示意图

NoC所有链路都采用虚拟通道的方法称为虚拟通道均匀分布技术(uniform distribution technology of virtual channel, VCUD)。仅在Mesh内部链路使用虚拟通道,Mesh边界上链路使用非虚拟通道的方法称为虚拟通道非均匀分布技术(non-uniform distribution technology of virtual channel, VCND)。

2.2 VCND技术

基于2D-mesh的NoC,内部链路负载量较大,边界链路负载量较小。根据此负载分布特点,当使用VCUD技术时,边界链路上的缓冲单元利用率会降低,因此我们提出一种VCND技术来解决该问题。该技术能有效地降低NoC的链

路拥塞,提高缓冲单元的利用率,并减少路由器的面积。

图2描述了VCND技术的虚拟通道布局,加粗虚线所围区域的路由节点之间使用虚拟通道,区域外的路由节点之间使用非虚拟通道。在该技术下,数据包传输有下面3种情况。

(1)数据包在内部节点的传输即相邻路由器之间传输采用虚拟通道;当数据包的头流片经过路由节点时,路由控制器和仲裁器确定输出端口和下一跳输入端口的虚拟通道号。

(2)数据包在边界节点的传输即边界相邻路由器之间传输采用非虚拟通道;当数据包的头流片经过路由节点时,路由控制器和仲裁器确定输出端口并检查是否有空闲缓冲单元,如果有空闲缓冲单元就传输,否则等待。

(3)数据包在边界与内部交界处的路由节点之间的传输,存在两种传输形式:一种是从边界到内部的传输,另一种是从内部到边界的传输。由于链路两侧缓冲单元个数不等,因此在传输数据流片时,需要根据先来先服务(first come first service, FCFS)的原则进行仲裁,避免出现饥饿问题。

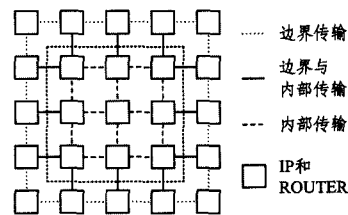


图2 VCND图

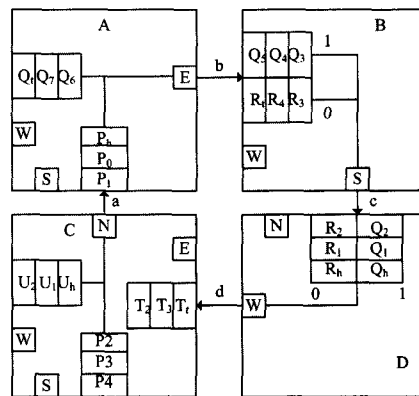


图3 VCND下的数据包传输

图3描述了VCND下的数据包传输。a表示使用非虚拟通道的边界节点之间的传输。数据包P存放在路由器C的缓冲单元,通过N端口传输到路由器A缓冲单元。如果后续数据包U也请求传输,那么它必须等到数据包P传输完,才可以获得物理链路的使用权。c表示使用虚拟通道的内部节点之间的传输。数据包Q和数据包R分别存放在路由器B的1号虚拟通道和0号虚拟通道,通过S端口传输到路由器D的虚拟通道,虚拟通道号要一一对应。当数据包R发生阻塞时,数据包Q就可以获得物理链路的使用权,通过S端口传输到路由器D的1号虚拟通道,降低了网络拥塞。如果数据包R和Q同时请求,则根据FCFS的原则分配链路的使用权,避免出现饥饿问题。b和d表示边界与内部交界处节点之间的传输。b和c的传输形式相似,仅有一点不同,就是b不需要虚拟通道号一一对应。在d形式下,路由器D里的数据包R和Q如果同时请求路由器C的缓冲单元,则根据FCFS原则进行分配。如果路由器C没有空闲缓冲单元,则

必须等待。在 VCND 技术下, NoC 的边界上采用非虚拟通道, 仅在内部采用虚拟通道。因此边界上的路由器内的缓冲单元个数减少, 使得路由器面积减少。当数据包注入率低时, 边界上缓冲单元的利用率大幅度提高。

3 CXY 路由算法

在 XY 路由算法和 XY-YX 路由算法的基础上, 本文提出一种改进的无死锁路由算法 CXY。XY 路由算法是维序路由算法, 先 X 维, 后 Y 维。在负载量较小的情况下, 其性能优于其它路由算法。该算法的缺点是链路负载不均衡。当通信量剧增时, 容易产生拥塞, 网络性能急剧下降^[12,13]。

XY-YX 路由算法主要解决 XY 路由算法带来的链路负载不均衡问题。该算法根据当前节点与目的节点的相对位置, 选择先 X 维传输还是 Y 维传输。缺点是当前节点与目的节点的相对位置具有局部性, 导致选择的 XY 路由算法或 YX 路由算法比较集中, 所以网络负载均衡的效果不明显。

在基于 2D-mesh 的 NoC 中, 当使用 VCND 技术时, 由于边界上不使用虚拟通道, 所以无法避免死锁, 因此设计路由算法时要考虑死锁避免问题。基于以上不足, 本文提出一种改进的无死锁路由算法 CXY。

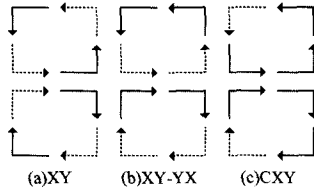


图 4 XY, XY-YX, CXY 路由算法允许的路由转向

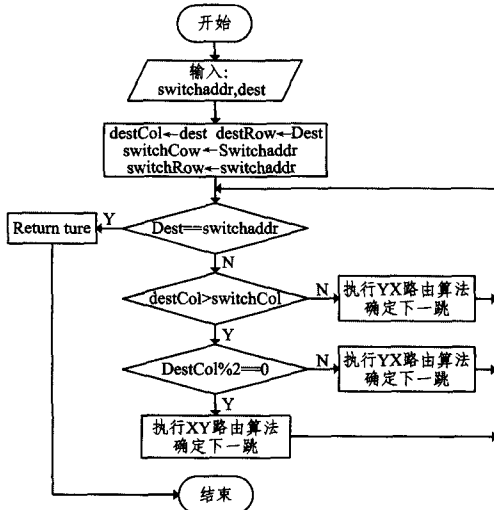


图 5 CXY 路由算法流程图

CXY 路由算法的主要思想是当目的节点位于偶数列且目的节点在当前路由节点的右边时, 采用 XY 路由算法。当目的节点位于奇数列且目的节点在当前路由节点的右边时, 则采用 YX 路由算法。由于边界链路不使用虚拟通道, 为了避免死锁的产生, 当目的节点在当前路由节点的左边时, 仅采用 YX 路由算法, 奇偶位置因素不再参与路由决定。该算法不仅采用 XY 路由算法和 YX 路由算法相结合的方式减轻 X 方向的负载, 而且还利用目的节点的奇偶位置, 使得 XY 路由算法和 YX 路由算法的使用更具均匀性。从 Turn Model 模型^[14-16]的角度分析, 与 XY 路由算法和 XY-YX 路由算法

相比, 该算法增加了两个路由转向并且不会产生死锁。图 4 给出了 3 种路由算法允许的路由转向。图 5 给出了 CXY 路由算法选择路径的主要过程。与 XY 路由算法和 XY-YX 路由算法相比, CXY 路由算法能均衡网络链路负载, 提高 NoC 的吞吐量和降低网络平均延时。

算法 1 CXY 路由算法

dest 表示目的节点地址, destRow 表示目的节点的行坐标, destCol 表示目的节点的列坐标。

switchaddr 表示当前路由节点地址, switchRow 表示当前路由节点的行坐标, switchCol 表示当前路由节点的列坐标。

输入: dest, switchaddr

输出: 输出端口 (east, west, north, south)

仅给出确定数据包下一跳的路由算法代码, 如图 6 所示。

```

If (dest == switchaddr) return true;
Else if (destCol > switchCol)
{
  If (destCol % 2 == 0)
    Return east; // 采用 XY 路由算法
  Else
    { // 采用 YX 路由算法
      If (destRow > switchRow)
        Return south;
      Else if (destRow < switchRow)
        Return north;
      Else
        Return east;
    }
}
Else if (destCol < switchCol) // 采用 YX 路由算法
{
  If (destRow > switchRow)
    Return north;
  Else if (destRow < switchRow)
    Return south;
  Else
    Return west;
}
Else
  { // 在同一列
    If (destRow > switchRow)
      Return north;
    Else
      Return south;
  }
}

```

图 6 CXY 路由算法

4 性能仿真分析

本文采用 gpNoCsim1.0 仿真器^[17], 它可以对 NoC 的 Mesh, Torus, Butterfly 和 Fat Tree 等多个拓扑结构进行仿真。该仿真器通过对 NoC 配置一些参数, 实现对 NoC 性能的评估。可配置的参数包括拓扑结构的种类、数据包注入率、缓冲单元大小、虚拟通道个数和运行周期数。评估的性能参数有吞吐量、网络平均延时、链路利用率和缓冲单元利用率。

数据包划分为 3 种流片, 分别是头流片、数据流片和尾流片。头流片中含有该数据包的路由信息, 数据流片包含要传

输的数据,尾流片含有释放缓冲单元的信息。仿真环境中最小单元是流片。本文仿真设定的虚拟通道个数为3,每个虚拟通道对应一个缓冲单元,每个缓冲单元能存放2个流片。仿真每次运行10000个时钟周期,前1000个时钟周期是稳定阶段(warm-up)。

图7给出 5×5 Mesh结构下的仿真结果。(a)、(b)是3种路由算法在VCUD下获得的吞吐量和平均延时。CXY路由算法在VCUD下获得的吞吐量和平均延时优于XY路由算法和XY-YX路由算法。当数据包注入率低时,3种路由算法的平均延时基本一致,随着数据包注入率的增加,XY和XY-YX路由算法的平均延时高于CXY路由算法。当数据包注入率达到0.6时,XY和XY-YX路由算法的平均延时开始迅速增加,而CXY路由算法在数据包注入率为0.7时才迅速增加。CXY路由算法在数据包注入率为0.3之前,获得的吞吐量和另外两种路由算法基本一致。当数据包注入率在0.3和0.7之间时,CXY路由算法获得吞吐量优于其它路由算法。(c)、(d)是3种路由算法在VCND下获得的吞吐量和平均延时。CXY路由算法在VCND下获得的吞吐量和平均延时优于其它两种路由算法,平均延时的优势更明显。由于网络规模较小,使用虚拟通道的链路仅占网络链路总数的30%,与VCUD相比,CXY路由算法在VCND下吞吐量降低了6.3%,网络平均延时增加10.2%。

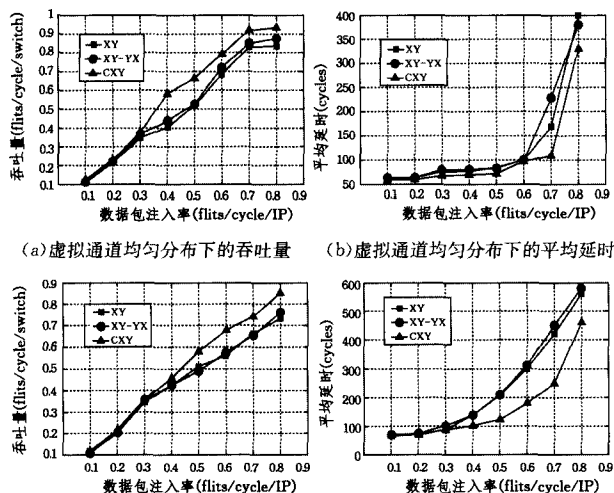


图7 在 5×5 规模下的吞吐量和平均延时

图8给出 8×8 Mesh结构下3种路由算法的仿真结果。从图中可以看出,CXY路由算法在VCUD和VCND下的吞吐量和平均延时都优于其它两种路由算法。3种路由算法在该规模下获得的吞吐量高于在 5×5 规模下获得的吞吐量。当数据包注入率为0.6时,CXY路由算法获得的平均延时低于100个时钟周期。

图9给出 12×12 Mesh结构下3种路由算法的仿真结果。CXY路由算法的吞吐量和平均延时优于XY路由算法和XY-YX路由算法。3种路由算法在VCND下获得的平均延时高于在VCUD下获得的平均延时。因为在VCND下,边界没有采用虚拟通道,所以随着数据包注入率的增加,边界链路容易产生数据包拥塞,导致平均延时增加。在VCUD下,随着数据包注入率的增加,由于边界采用虚拟通道,不易

发生数据包拥塞,因此网络产生的平均延时较小。该规模下,3种路由算法获得的吞吐量高于 5×5 和 8×8 规模下获得的吞吐量,然而网络平均延时随着数据包注入率的增加而增加。

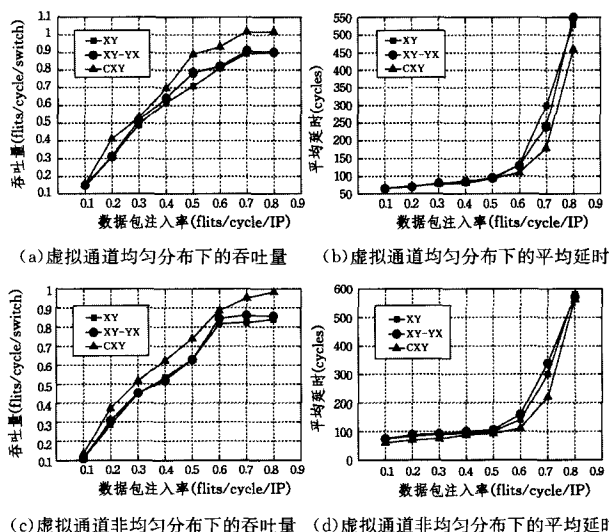


图8 在 8×8 规模下的吞吐量和平均延时

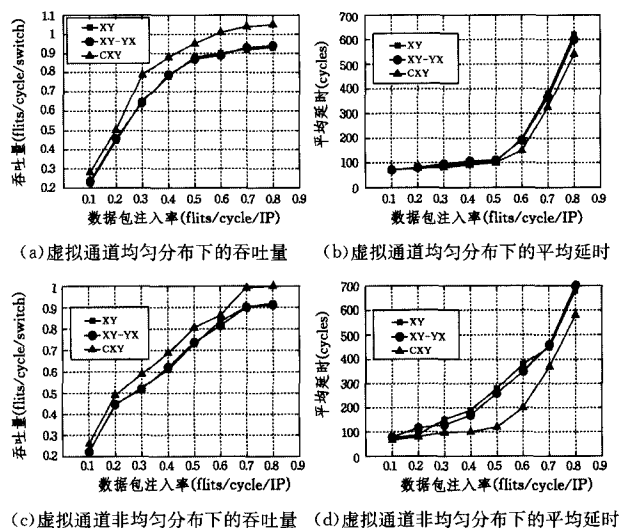


图9 在 12×12 规模下的吞吐量和平均延时

图10和图11描述了不同网络规模下,CXY路由算法在VCND技术下的仿真结果。随着网络规模的增加,CXY路由算法获得的吞吐量也不断地提高。在3个网络规模下,CXY路由算法获得的吞吐量分别为0.8516、0.98、1.00。网络平均延时在数据包注入率达到0.4之前基本一致,随着数据包注入率的增加, 8×8 规模下的CXY路由算法获得的平均延时优于其它两种规模下CXY路由算法获得的平均延时。随着网络规模的不断增大,当数据包注入率高时,VCND下的边界上更容易产生数据包拥塞,导致平均延时增加。

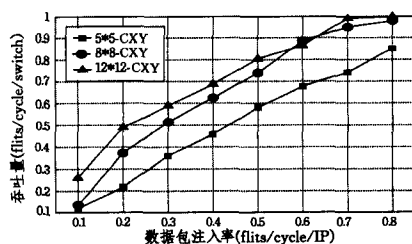


图10 VCND下CXY路由算法的吞吐量

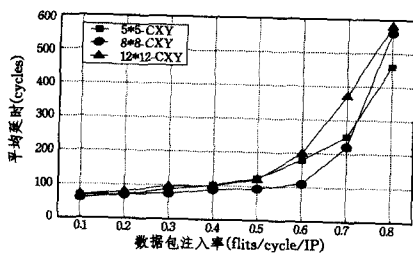


图 11 VCND 下 CXY 路由算法的平均延时

图 12 和图 13 给出 3 种路由算法在 VCUD 和 VCND 下的仿真结果。仿真结果表明,相比 XY 路由算法和 XY-YX 路由算法,CXY 路由算法的网络吞吐量分别提高了 13.12%与 11.54%,网络平均延时分别降低了 12.3%与 9.75%。与 VCUD 相比,CXY 路由算法在 VCND 下获得的吞吐量降低了 4.52%,网络平均延时增加了 3.84%。但是在 VCND 下,路由器面积平均减少了 19.964%,并且缓冲单元利用率也有提升。

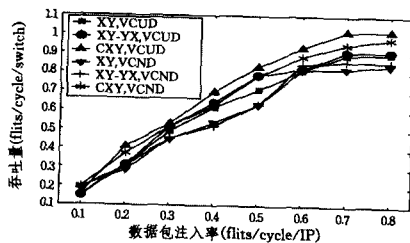


图 12 VCUD 和 VCND 下的吞吐量

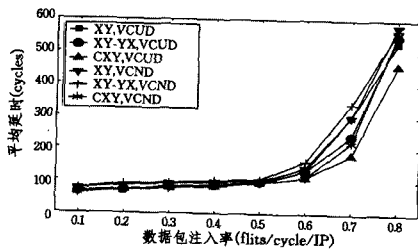


图 13 VCUD 和 VCND 下的平均延时

图 14 给出两种虚拟通道分布下的缓冲单元利用率的仿真结果。在数据包注入率为 0.7 之前,VCND 下的缓冲单元利用率高于 VCUD 下获得的缓冲单元利用率。VCND 技术能根据网络负载的分布特点和实际应用中通信量的估计,合理利用缓冲单元。相比 VCUD 技术,VCND 技术使得缓冲单元利用率平均提高 20.03%。

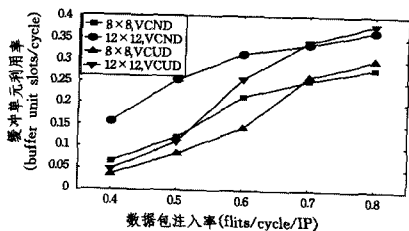


图 14 缓冲单元利用率

表 1 列出两种虚拟通道分布面积消耗的比较。VCUD 表示虚拟通道均匀分布技术所需面积,VCND 表示虚拟通道非均匀分布技术所需面积。从表中可以看出,采用 VCND 技术能大幅度减少路由器面积。当网络规模为 5×5 时,整个芯片上的缓冲单元面积减少 42.6%,路由器面积减少 29.82%。

当网络规模为 8×8 时,缓冲单元面积减少 28.52%,路由器面积减少 19.964%。随着网络规模的增加,NoC 边界上的路由节点数量占网络总路由节点数量的比例逐渐缩小,所以在 VCND 下,整个芯片上的缓冲单元面积减少比例也在不断地下降。当 NoC 规模达到 20×20 时,缓冲单元面积减少 12.56%,路由器面积减少比例仍能达到 8.792%。综上所述,在整个芯片上的缓冲单元面积平均减少了 21.35%,路由器面积平均减少了 19.45%,缓冲单元利用率平均提高了 20.03%。

表 1 NoC 中两种虚拟通道分布面积消耗

NoC 规模	虚拟通道	VCUD 面积 (bit)	VCND 面积 (bit)	缓冲单元面积减少	路由器面积减少
5×5	3	38400	22016	42.6%	29.82%
6×6	3	55296	34816	37.74%	26.418%
7×7	3	75264	50688	32.65%	22.82%
8×8	3	98304	70262	28.52%	19.964%

结束语 NoC 设计的一个关键是如何在性能与成本之间进行折中。本文从网络性能和路由器面积消耗的角度进行探索,使得 NoC 的整体性能更优。根据 NoC 负载分布特点,提出一种在 mesh 边界上使用非虚拟通道,内部使用虚拟通道的 VCND 技术。同时提出一种改进的无死锁路由算法 CXY。该算法根据当前节点与目的节点的相对位置以及目的节点所在列的奇偶性,选择 XY 路由算法或 YX 路由算法。仿真结果表明,在 5×5 、 8×8 、 12×12 等 Mesh 网络下,相比 XY 路由算法和 XY-YX 路由算法,CXY 路由算法的网络吞吐量分别提高了 13.12%与 11.54%,网络平均延时分别降低了 12.3%与 9.75%。相比 VCUD 技术,VCND 技术分别以 4.52%的吞吐量和 3.84%的延时损失获得 20.03%的缓冲单元利用率提升,同时节约了 19.45%的路由器面积。

参考文献

- [1] Dally W J, Towles B. Route packets, not wires: On-chip interconnection networks[C]//Proceedings of IEEE Design Automation Conference. 2001:684-689
- [2] Verbeek F, Schmaltz J. On necessary and sufficient conditions for deadlock-free routing in wormhole networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22 (12):2022-2032
- [3] Li M, Zeng Q A, Jone W B. DyXY: A proximity congestion-aware deadlock-free dynamic routing method for network on chip[C]//Proceedings of the 43rd Annual Design Automation Conference. 2006:849-852
- [4] Patooghy A, Miremadi S G. XYX: A power & performance efficient fault-tolerant routing algorithm for network on chip[C]//Proceedings of the 17th Euromicro International Conference on Parallel, Distributed and Network-based. Weimar, Germany, 2009:245-251
- [5] Tang M, Lin X, Palesi M. Routing Pressure: A Channel-related and Traffic-aware Metric of Routing Algorithm [J]. IEEE transactions on Parallel and Distributed Systems, 2013 (Pre-Prints)
- [6] 蒋明,孟玲珊.一种对片上网络中 mesh 结构的改进策略及路由算法[J]. 计算机科学,2012,39(6):40-43

好地支持了敌手的询问。新协议在计算量方面的优势并不明显,如何在安全假设和安全目标不变的情况下提出计算量更小的认证密钥交换协议,是下一步值得研究的问题。

参 考 文 献

- [1] Bellare M, Rogaway P. Entity authentication and key distribution [C]//Stinson D R. Crypto'93, Lecture Notes in Computer Science 773. Berlin: Springer, 1993: 232-249
- [2] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels [C] // EUROCRYPT 2001, LNCS. vol. 2045, Springer-Verlag, 2001: 453-474
- [3] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange [C]//ProvSec 2007, LNCS, vol. 4784. Springer-Verlag, 2007: 1-16
- [4] Lee J, Park J H. Authenticated Key Exchange Secure under the Computational Diffie-Hellman Assumption [R]. Report 2008/344. Cryptology ePrint Archive, 2008
- [5] 秦波, 伍前红, 王育民, 等. 密钥协商协议进展[J]. 计算机科学, 2008, 35(9): 9-12
- [6] 任勇军, 王建东, 王箭, 等. 标准模型下基于身份的认证密钥协商协议[J]. 计算机研究与发展, 2010, 47(9): 1604-1610
- [7] 赵建杰, 谷大武. eCK 模型下可证明安全的双方认证密钥协商协议[J]. 计算机学报, 2011, 34(1): 47-54
- [8] Zhou Qing-lei, Yang Zeng-fu. TUP: A New eCK-Secure AKE Protocol under the CDH Assumption [J]. Int. J. Communications, Network and System Sciences, 2012, 5: 332-336
- [9] Bian Shi-zhu, Wang Jian-dong, Ren Yong-jun. Strongly-secure and Efficient Authenticated Key Exchange Protocol [J]. Computer Engineering, 2010, 36(7)
- [10] Nishide T, Yoneyama K, Ohta K. Attribute-based encryption with partially hidden encryptor-specified access structures [C]//Proceedings of the 6th international conference on Applied cryptography and network security, 2008. New York, USA, 2008: 111-129
- [11] Kim M B, Fujioka A, Ustaoglu B. Strongly Secure Authenticated Key Exchange without NAXOS' Approach [C]//Proc. of the fourth International Workshop on Security, IWSEC09 Lecture Notes in Computer Science. vol. 5824, Springer-Verlag, 2009: 174-191
- [12] Cremers C J F. Formally and practically relating the ck, ck-hmqv, and eCK security models for authenticated key exchange [OL]. Cryptology ePrint Archive, August 2009
- [13] Cheng Qing-feng, Ma Chuan-gui, Wei Fu-shan. A modified eCK model with stronger security for tripartite authenticated key exchange [C]//Zhengzhou information Science and Technology Institute, Zhengzhou, China, 2010
- [14] McCullagh N, Barreto S L. A new two-party identity-based authenticated key agreement [C]//Proceedings of CT-RSA 2005, Lecture Notes in Computer Science 3376. Springer-Verlag, 2005: 262-274
- [15] Lauter K, Mityagin A. Security analysis of KEA authenticated key exchange [C]//Public Key Cryptography PKC2006, LNCS 3958, 2006: 378-394
- [16] Krawczyk H. HMQV: A high-performance secure Diffie-Hellman protocol, Advances in Cryptology CRYPTO 2005 [C] // LNCS 3621. 2005: 546-566
- [17] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange [C]//ProvSec2007, Lecture Notes in Computer Science 4784, 2007: 1-16
- [18] Ustaoglu B. Obtaining a secure and efficient key agreement protocol from (H)MQV and NAXOS [J]. Designs, Codes and Cryptography, 2008, 46(3): 329-342
- [19] Kudla C, Paterson K. Modular security proofs for key agreement protocols [C]//Advances in Cryptology-Asia crypt 2005, LNCS 3788. Springer-Verlag, 2005: 549-565
- [20] Jeong I R, Katz J, Lee D H. One-round protocols for two-party authenticated key exchange [C]//Applied Cryptography and Network Security, Second International Conference, ACNS 2004, volume 3089 of Lecture Notes in Computer Science. Springer, 2004: 220-232
- [21] Okamoto T. Authenticated key exchange and key encapsulation in the standard model [C]//Advances in Cryptology-ASIA-CRYPT 2007, volume 4833 of Lecture Notes in Computer Science. Springer, 2007: 474-484
- [22] Boyd C, Cliff Y, Nieto J G, et al. Efficient one-round key exchange in the standard model [C]//Information Security and Privacy 2008, Volume 5107 of Lecture Notes in Computer Science. Springer, 2008: 69-83
-
- (上接第 168 页)
- [7] 欧阳一鸣, 董少周, 梁华国. 基于 2DMesh 的 NoC 路由算法设计与仿真 [J]. 计算机工程, 2009, 35(22): 227-229
- [8] 朱红雷, 彭元喜, 尹亚明, 等. 一种动态分配虚拟通道输出队列结构的片上路由器 [J]. 计算机研究与发展, 2012, 49(1): 183-192
- [9] 周芳, 吴宁, 周磊, 等. 面向低功耗的片上网络虚拟通道分配算法 [J]. 东南大学学报: 自然科学版, 2013, 43(2): 263-267
- [10] 胡哲琨, 陈杰. 完全自适应路由算法的虚拟通道分配优化策略 [J]. 微电子学与计算机, 2013, 30(8): 1-7
- [11] Yoon Y J, Concer N, Petracca M, et al. Virtual channels vs. multiple physical networks: A comparative analysis [C]//Proceedings of the 47th ACM/IEEE Design Automation Conference. 2010: 162-165
- [12] Lin J, Lin X, Tang L. Making-a-stop: A new bufferless routing algorithm for on-chip network [J]. Journal of Parallel and Distributed Computing, 2012, 72(4): 515-524
- [13] Chawade S D. Review of XY routing Algorithm for Network-on-chip Architecture [J]. International Journal of Computer Applications, 2012, 43(21): 48-52
- [14] Chiu Ge-ming. The Odd-Even Turn Model for Adaptive Routing [J]. IEEE Transactions on Parallel and Distributed Systems, 2000, 11(7): 729-736
- [15] Hu S, Lin X. A Symmetric Odd-Even Routing Model in Network-on-Chip [C]//Proceedings of the 11th International Conference on Computer and Information Science, Shanghai, China, 2012: 457-462
- [16] Moosavi S R, Chang C-Y, Rahmani A, et al. An efficient history-based routing algorithm for interconnection networks [C]//Proceedings of the International SoC Design Conference. 2012: 277-280
- [17] Al-Nayem A, Zerin T. gpNoCsim 1.0 User's Guide 2006 [OL]. <http://www.buet.ac.bd/cse/research/noc/>