Chapter 3

Deadlock Prevention with Wormhole Routing: Irregular Topology

Lev Levitin
Boston University, USA

Mark Karpovsky
Boston University, USA

Mehmet Mustafa
Boston University, USA

ABSTRACT

The problem of preventing deadlocks and livelocks in computer communication networks with wormhole routing is considered. The method to prevent deadlocks is to prohibit certain turns (i.e., the use of certain pairs of connected edges) in the routing process, in such a way that eliminates all cycles in the graph. A new algorithm that constructs a minimal (irreducible) set of turns that breaks all cycles and preserves connectivity of the graph is proposed and analyzed. The algorithm is tree-free and is considerably simpler than earlier cycle-breaking algorithms. The properties of the algorithm are proven, and lower and upper bounds for minimum cardinalities of cycle-breaking connectivity preserving sets for graphs of general topology, as well as for planar graphs, are presented. In particular, the algorithm guarantees that not more than 1/3 of all turns in the network become prohibited. Experimental results are presented on the fraction of prohibited turns, the distance dilation, as well as on the message delivery times and saturation loads for the proposed algorithm in comparison with known tree-based algorithms. The proposed algorithm outperforms the tree-based algorithms in all characteristics that were considered.

DOI: 10.4018/978-1-4666-2533-4.ch003
1. INTRODUCTION AND RELATED WORK

With its simplicity, low channel setup times, and its high performance in delivering messages, wormhole routing has been widely investigated (Dally & Seitz, 1987; Boppana & Chalasani, 1993; Chalasani & Boppana, 1995; Duato, Yalamancili, & Ni, 1997; Ni & McKinley, 1993), and recently is being revisited for Networks-on-Chips technologies (Mello, Ost, Moraes, & Calazans, 2004; Hu & Marculescu, 2004). Wormhole routing and its variants, (Gaughan & Yalamanchili, 1995) virtual cut-through and pipelined circuit switching, PCS, have been used in regular topologies from chip-scale networks (Mello et al., 2004; Hu & Marculescu, 2004), to rack-packed Blue Gene (Klepacki, 2003), to irregular topologies formed by interconnecting low-cost workstations in an ad hoc manner, forming what is referred to as Network of Workstations (NOWs) (Libeskind-Hadas, Mazzoni, & Rajagopalan, 1998; Silla, Duato, Sivasubramaniam, & Das, 1998; Silla & Duato, 2000). Nodes in such networks consist of processing element connected to a router or switching element via a channel with full duplex links. Messages originate and are consumed in the processing elements. Messages that are flowing from a router towards a processing element use what is known as the consumption channel and those that are flowing away from the processing element towards the router use the injection channel. The consumption and the injection channels together form the full duplex communication link between the processor and the router. Routers are connected to other routers in the network using full duplex links as well. Messages, also known as ‘worms’, are made up of flits that are transmitted atomically, one flit at a time, from node to node in the network. In contrast to this technique which is known as the wormhole routing, in the store and forward routing technique, the message in its entirety is received by each and every intermediate node, and only then it is transmitted to the next node. Therefore, wormhole routing provides for much faster message delivery. The header flit, containing the destination address is immediately followed by the payload or data flits (Ni & McKinley, 1993). Another aspect that makes wormhole routing and routers attractive is that each channel requires only a few flits deep buffer space (Dally & Seitz, 1986; Glass & Ni, 1992). In wormhole routed networks, messages traverse the network in a pipelined fashion, such that parts of the message occupy different network resources, while the header flit requests yet other resources. Under this policy, when there is no contention, as in lightly loaded networks, the latency of message (average delivery time) varies very slowly with the distance (Ni & McKinley, 1993). However, when a message is blocked, the header and the rest of the message wait until the blockage is removed. As a result, messages could hold up potentially large number of network resources while attempting to reserve others.

In congested networks with high injected traffic, improperly designed routing protocols can lead to a network state, in which no progress can be made in delivering, not only of the current messages but all subsequent messages in the network. This network state, in which worms are in a cyclic dependency of each other’s held-up resources, is known as deadlock. Figure 1 depicts a section of a network in which no measures were taken to prevent deadlock. (The rest of the network where four deadlocked messages have originated is not shown.) The figure shows four-port routers with their local processors presented as circles. Assume that each message \( M_i \) is destined for node \( i \). In the figure communication channels have been occupied by the messages shown juxtaposed next to them. The rest of the messages occupy a number of other channels in the network. It can be seen that four messages, \( M_1, M_2, M_3, \) and \( M_4 \) are blocking each other, so that none of the messages can move forward. For example, message \( M_2 \) has acquired ownership of the vertical com-