ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Volume 1, Issue 8, October 2013

Delay-Independent Stability and Performance of Distributed Congestion Control

S.Thirunavukkarasu[1] , Dr.K.P.Kaliyamurthie[2]

Assistant Professor, Dept of IT, Bharath University, Chennai, TamilNadu, India.

Professor & Head, Dept of IT, Bharath University, Chennai, TamilNadu, India.

ABSTRACT: Recent research efforts to design better Internet transport protocols combined with scalable Active Queue Management (AQM) have led to significant advances in congestion control. One of the hottest topics in this area is the design of discrete congestion control algorithms that are asymptotically stable under heterogeneous feedback delay and whose control equations do not explicitly depend on the RTTs of end-flows.

Keywords: Active Queue Management,

I. INTRODUCTION

In this paper, we first prove that single-link congestion control methods with a stable radial Jacobian remain stable under arbitrary feedback delay (including heterogeneous directional delays) and that the stability condition of such methods does not involve any of the delays. We then extend this result to generic networks with fixed consistent bottleneck assignments and max–min network feedback. To demonstrate the practicality of the obtained result, we change the original controller in Kelly et al.'s work ["Rate Control for communication]n networks: Shadow prices, proportional fairness and stability," Journal of the Operational Research Society, vol. 49, no. 3, pp. 237–252, March 1998] to become robust under random feedback delay and fixed constants of the control equation. We call the resulting framework Max–min Kelly Control (MKC) and show that it offers smooth sending rate, exponential convergence to efficiency, and fast convergence to fairness, all of which make it appealing for future high-speed networks.

Router

A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located atgateways, the places where two or more networks connect, and are the critical device that keeps data flowing between networks and keeps the networks connected to the Internet. When data is sent between locations on one network or from one network to a second network the data is always seen and directed to the correct location by the router. They accomplish his by using headers and forwarding tables to determine the best path for forwarding the data packets, and they use protocolssuch as ICMP to communicate with each other and configure the best route between any two hosts.
The Internet itself is a global network connecting millions of computers and smaller networks — so you can see how crucial the role of a router is to our way of communicating and computing.

Why Would I Need a Router?

For most home users, they may want to set-up a LAN (local Area Network) or WLAN (wireless LAN) and connect all computers to the Internet without having to pay a full broadband subscription service to their ISP for each computer on the network. In many instances, an ISP will allow you to use a router and connect multiple computers to a single Internet connection and pay a nominal fee for each additional computer sharing the connection. This is when home users will want to look at smaller routers, often called broadband routers that enable two or more computers to share an Internet connection. Within a business or organization, you may need to connect multiple computers to the Internet, but also want to connect multiple private networks — and these are the types of functions arouter is designed for.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Volume 1, Issue 8, October 2013

Routers for Home

Not all routers are created equal since their job will differ slightly from network to network. Additionally, you may look at a piece of hardware and not even realize it is a router. What defines a router is not its shape, color, size or manufacturer, but its job function of routing data packets between computers. A cable modem which routes data between your PC and your ISP can be considered a router. In its most basic form, a router could simply be one of two computers running the Windows 98 (or higher) operating system connected together using ICS (*Internet Connection Sharing*). In this scenario, the computer that is connected to the Internet is *acting as the router* for the second computer to obtain its Internet connection.

Going a step up from ICS, we have a category of hardware routers that are used to perform the same basic task as ICS, albeit with more features and functions. Often called *broadband or Internet connection sharing routers*, these routers allow you to share one Internet connection between multiple computers.

Broadband or ICS routers will look a bit different depending on the manufacturer or brand, but wired routers are generally a small box-shaped hardware device with ports on the front or back into which you plug each computer, along with a port to plug in your broadband modem. These connection ports allow the router to do its job of routing the data packets between each of the the computers and the data going to and from the Internet.

Depending on the type of modem and Internet connection you have, you could also choose a router with phone or fax machine ports. A wired Ethernet broadband router will typically have a built-in Ethernet switch to allow for expansion. These routers also support NAT (*network address translation*), which allows all of your computers to share a single IP address on the Internet. Internet connection sharing routers will also provide users with much needed features such as an SPI firewallor serve as a a DHCP Server.

Wireless broadband routers look much the same as a wired router, with the obvious exception of the antenna on top, and the lack of cable running from the PCs to the router when it is all set up. Creating a wireless network adds a bit more security concerns as opposed to wired networks, but wireless broadband routers do have extra levels of embedded security. Along with the features found in wired routers, wireless routers also provide features relevant to wireless security such as Wi-Fi Protected Access (WPA) and wireless MAC address filtering. Additionally, most wireless routers can be configured for "invisible mode" so that your wireless network cannot be scanned by outside wireless clients. Wireless routers will often include ports for Ethernet connections as well. For those unfamiliar with WiFi and how it works, it is important to note that choosing a wireless router may mean you need to beef up your Wi-Fi knowledge-base. After a wireless network is established, you may possibly need to spend more time on monitoring and security than one would with a wired LAN.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

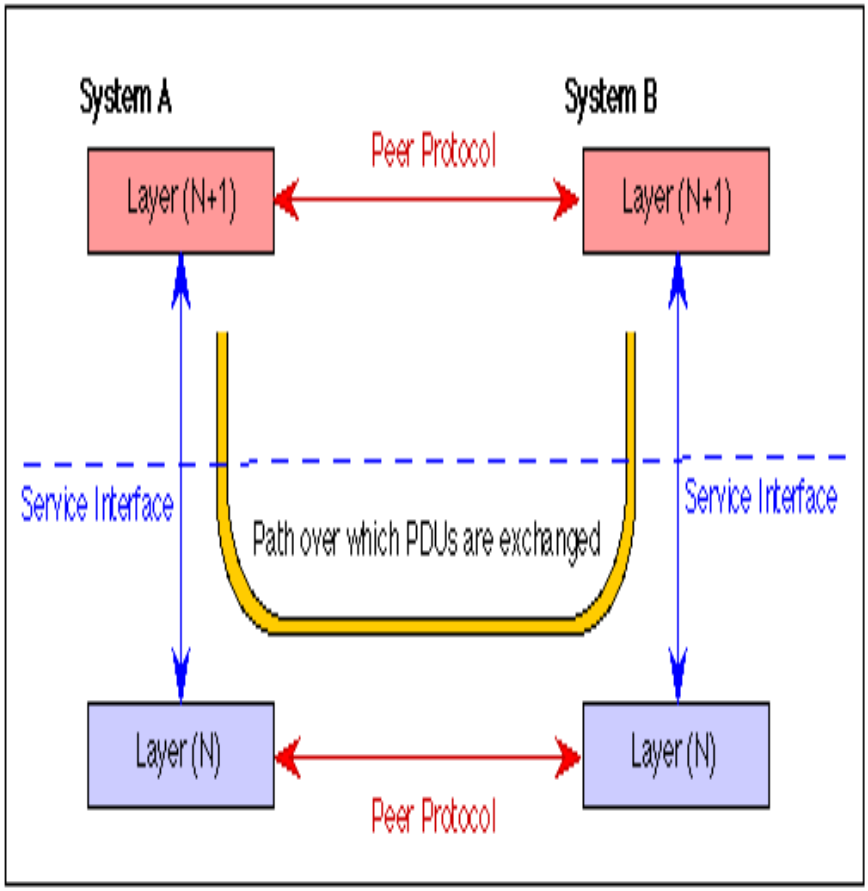
Volume 1, Issue 8, October 2013

Wired and wireless routers and the resulting network can claim pros and cons over each other, but they are somewhat equal overall in terms of function and performance. Both wired and wireless routers have high reliability and reasonably good security (without adding additional products). However —and this bears repeating — as we mentioned you may need to invest time in learning more about wireless security. Generally, going wired will be cheaper overall, but setting up the router and cabling in the computers is a bit more difficult than setting up the wireless network. Of course, mobility on a wired system is very limited while wireless offers outstanding mobility features.

II. PEER-TO-PEER COMMUNICATION

Protocol layers may be defined in such a way that the communications within a layer is independent of the operation of the layer being used. This is known as "peer-to-peer" communication and is an important goal of the OSI Reference Model.

Each layer provides a protocol to communicate with its peer. When a packet is transmitted by a layer, a header consisting of Protocol Control Information (PCI) is added to the data to be sent. In OSI terminology, the packet data (also known as the Payload) is called a Protocol Data Unit (PDU). The packet so-formed, called a Service Data Unit (SDU) is passed via a service access point to the layer below. This is sent using the service of the next lower protocol layer.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

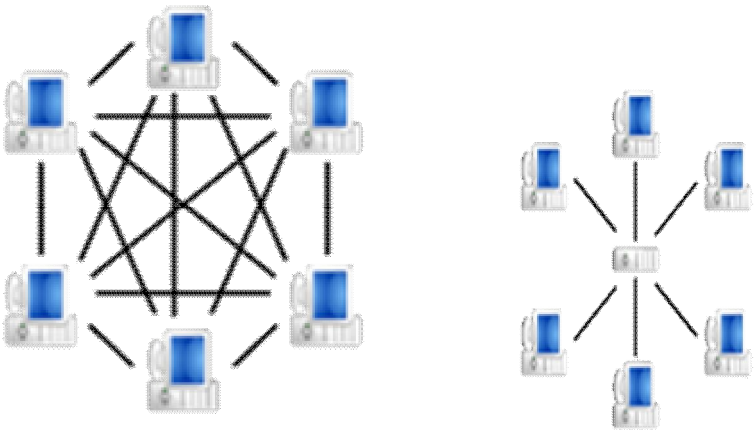
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Volume 1, Issue 8, October 2013

III. CLASSIFICATION OF P2P NETWORKS

P2P networks can be classified by what they can be used for:file



sharing
- telephony
- media streaming (audio, video)
- discussion forums

Other classification of P2P networks is according to their degree of centralization.
In 'pure' P2P networks:
- Peers act as equals, merging the roles of clients and server
- There is no central server managing the network
- There is no central router

Some examples of pure P2P application layer networks designed for file sharing are Gnutella and Free net.
There also exist countless hybrid P2P systems:
- Has a central server that keeps information on peers and responds to requests for that information.
- Peers are responsible for hosting available resources (as the central server does not have them), for letting the central server know what resources they want to share, and for making its shareable resources available to peers that request it.
- Route terminals are used as addresses, which are referenced by a set of indices to obtain an absolute address.

e.g.
- Centralized P2P network such as Napster
- Decentralized P2P network such as KaZaA
- Structured P2P network such as CAN
- Unstructured P2P network such as Gnutella
- Hybrid P2P network (Centralized and Decentralized) such as JXTA (an open source P2P protocol specification)

Networks and protocols

REFERENCES

[1] R. Bronson, *Schaum's Outline of Theory and Problems of Matrix Operations*. New York: McGraw-Hill, 1988.
[2] D.-M. Chiu and R. Jain, "Analysis of the increase and decrease algorithms, for congestion avoidance in computer networks," *Comput. Netw. ISDN Syst.*, vol. 17, no. 1, pp. 1–14, Jun. 1989.
[3] M. Dai and D. Loguinov, "Analysis of rate-distortion functions and, congestion control in scalable internet video streaming," in *Proc. ACM NOSSDAV*, Jun. 2003, pp. 60–69.
[4] S. Deb and R. Srikant, "Global stability of congestion controllers, for the internet," *IEEE Trans. Autom. Control*, vol. 48, no. 6, pp. 1055–1060, Jun. 2003.
ZHANG *et al.*: DELAY-INDEPENDENT STABILITY AND PERFORMANCE OF DISTRIBUTED CONGESTION CONTROL 851

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Volume 1, Issue 8, October 2013

[5] S. Floyd, "High-speed TCP for large congestion windows," IETF RFC 3649, Dec. 2003.
[6] S. Floyd, M. Handley, J. Padhye, and J.Widmer, "Equation-based congestion, control for unicast applications," in *Proc. ACM SIGCOMM*, Aug. 2000, pp. 43–56.
[7] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," *IEEE/ACM Trans. Netw.*, vol. 1, no. 4, pp. 397–413, Jan. 1993.
[8] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1990.
[9] C. Jin, D. Wei, and S. H. Low, "FAST TCP: Motivation, architecture, algorithms, performance," in *Proc. IEEE INFOCOM*, Mar. 2004, pp. 2490–2501.
[10] R. Johari and D. K. H. Tan, "End-to-End congestion control for the internet: Delays and stability," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 818–832, Dec. 2001.