SAJET

South Asian Journal of Engineering and Technology Vol.2, No.15 (2016) 124–129

ISSN No: 2454-9614

Virtual Routing Flow Control with Data Compression for Networks Overload

C. Vigundhiya[a], E. Menaka[a*]

[a)] *Department Of Computer Science and Engineering, Vivekananda institute of engineering and technology for women, Tiruchengode , Tamilnadu, India.*
[b)] *Department Of Computer Science and Engineering, Vivekananda institute of engineering and technology for women, Tiruchengode,, Tamilnadu, India.*

*Corresponding Author: C. Vigundhiya

E-mail: vigundhiya93@gmail.com,
Received: 11/11/2015, Revised: 27/12/2015 and Accepted: 5/03/2016

Abstract

Utility maximization in networks where the sources do not make use of flow control and may as a result overload the network. In the deficiency of flow control at the sources, some packets will inevitably have to be dropped when the network is in overload. To that end, we first develop a spread, threshold based packet-dropping policy that maximizes the weighted sum throughput. Next, consider utility maximization and extend a receiver-based flow control scheme that, when combined with threshold-based packet dropping, achieves the optimal utility. The flow control scheme creates virtual queues at the receivers as a push-back mechanism to optimize the amount of data delivered to the destinations via back-pressure routing. A new quality of our scheme is that a utility function can be assigned to a collection of flows, generalizing the traditional approach of optimizing per-flow utilities. Our control policies use finite-buffer queues and are independent of arrival information. Their near-optimal performance is proved and further supported by simulation results.

Keywords: Finite-Buffer Networks, Flow Control, Network Overload, Queuing Analysis, Utility Maximization

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Networking is the construction, design, and use of a network, including the physical (cabling, hub, bridge, switch, router, and so forth), the selection and use of telecommunication protocol and computer software for using and managing the network, and the establishment of operation policies and procedures related to the network.

A process that fosters the exchange of information and ideas among individuals or groups that share a common interest. It may fall into one of 2 categories - social or business. In the latter category, one of the implicit objectives is to form professional relationships that may boost one's future business and employment prospects. Networking is the practice of linking multiple computing devices together in order to share resources.

These resources can be printers, CDs, files, or even electronic communications such as e-mails and instant messages. These networks can be created using several different methods, such as cables, telephone lines, satellites, radio waves, and infrared beams. Without the ability to network, businesses, government agencies, and schools would be unable to operate as efficiently as they do today. The ability for an office or school to connect dozens of computers to a single printer is a seemingly simple, yet extremely useful capability. Perhaps even more valuable is the ability to access the same data files from various computers throughout a building. Flow control in data networks aims to provide fair allocation of resources and regulate the source rates of traffic flows in order to prevent network overload. In recent years, network utility maximization problems have been studied to optimize network performance through a combination of flow control, routing, and scheduling, whose optimal operations are revealed as the solution to the utility maximization problems. In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver.

It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node. Flow control should be distinguished from congestion control, which is used for controlling the flow of data when congestion has actually occurred. Flow control mechanisms can be classified by whether or not the receiving node sends feedback to the sending node. Flow control is important because it is possible for a sending computer to transmit information at a faster rate than the destination computer can receive and process it. This can happen if the receiving computers have a heavy traffic load in comparison to the sending computer, or if the receiving computer has less processing power than the sending computer.

Then, if no measures are taken to restrict the entrance of traffic into the network, queue sizes at bottleneck links will grow and packet delays will increase, possibly violating maximum delay specifications. Furthermore, as queue sizes grow indefinitely, the buffer space at some nodes may be exhausted. When this happens, some of the packets arriving at these nodes will have to be discarded and later retransmitted, thereby wasting communication resources. As a result, a phenomenon similar to a highway traffic jam may occur whereby, as the offered load increases, the actual network throughput decreases while packet delay becomes excessive. It is thus necessary at times to prevent some of the offered traffic from entering the network to avoid this type of congestion.

2. Maximizing the weight sum throughput

Non-persistent TCP connections in transient overload conditions, under the assumption that all connections have the same round-trip times. Goal is to develop theoretical tools that will enable us to relax this assumption and obtain explicit expressions for the rate of growth of the number of connections at the system, the rate at which TCP connections leave the system, as well as the time needed for the completion of a connection. To that end, the system as a DPS (Discriminatory Processor Sharing) system which we analyze under very mild assumptions on the probability distributions related to different classes of arrivals: only assume that the arrival rates of connections

exist, and that the amount of information transmitted during a connection of a given type forms a stationary ergodic sequence. Check through simulations the applicability of our queuing results for modeling TCP connections sharing a bottleneck. model to the analysis of TCP connections with different round trip time sharing a common bottleneck node; using simulations performed with ns simulator , the DPS model is well adapted to the way TCP connections share the bandwidth at overload.

2.1. Back pressure routing

Backpressure routing refers to an algorithm for dynamically routing traffic over a multi-hop network by using congestion gradients. It usually refers to a data network, but can apply to other types of networks as well. Focus on the data network application, where multiple data streams arrive to a network and must be delivered to appropriate destinations. The backpressure algorithm operates in slotted time, and every slot it seeks to route data in directions that maximize the differential backlog between neighboring nodes. This is similar to how water would flow through a network of pipes via pressure gradients. However, the backpressure algorithm can be applied to multi-commodity networks and to networks where transmission rates can be selected from different (possibly time-varying) options. Attractive features of the backpressure algorithm are:

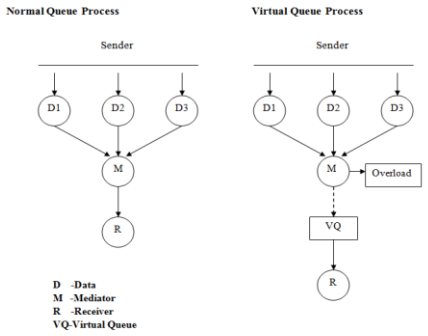

Fig no: 2.1 Virtual Route Creation

2.2 Thresholds-Based

The threshold-based packet-dropping policy, without the use of flow control, suffices to maximize the weighted sum throughput. Moreover, the combined flow control and packet-dropping mechanism has the following properties.

1) It is distributed and only requires information exchange between neighboring nodes.

2) It uses finite-size buffers.

3) It is nearly utility-optimal (throughput-optimal as a special case), and the performance gap from the optimal utility goes to zero as buffer sizes increase.

4) It does not need the knowledge of arrival rates and thus is robust to time-varying arrival rates that can go far beyond the network's stability region.

5) This policy works seamlessly without the need of explicitly deciding whether a network enters or leaves an overload period.
6) The policy can be implemented in parts of a network that include the receivers, treating the rest of the network as exogenous data sources.

3. Utility Optimal Overload Resilient Algorithm

The data packet loss during the data transaction, the proposed method that is Utility-Optimal Overload Resilient Algorithm (UORA) creates a virtual Queue. A Mathematical tool motivated by the earlier work of present a simple rule to design the parameters of the AVQ algorithm.

Then compare its performance through simulation with several well-known AQM schemes such as RED, REM, PI controller and a non adaptive virtual queue algorithm. With a view towards implementation, That AVQ can be implemented as a simple token bucket using only a few lines of code.

ECN marks or drop packets to provide fairness and control queue lengths, the routers have to select packets intelligently in a manner that conveys information about the current state of the network to the users. Algorithms which the routers employ to convey such information are called Active Queue Management *(AQM)* schemes. An AQM scheme might mark or drop packets depending on the policy at the router.

4. Virtual Queue

The large size of file will more from normal data queue to virtual queue and the transaction process will continue as a parallel. So the propose methods execute and send the file very quickly to the receiver. Utility maximization and develop a receiver-based flow control scheme that, when combined with Threshold-based packet dropping, achieves the optimal utility. The flow control scheme creates virtual queues at the receivers as a push-back mechanism to optimize the amount of data delivered to the destinations via back-pressure routing. A new feature of our scheme is that a utility function can be assigned to a collection of flows, generalizing the traditional approach of optimizing per-flow utilities. Our control policies use finite-buffer queues and are independent of arrival statistics.

4.1. Virtual Queue creation

A new virtual queue-based back-pressure scheduling VBR, which re-establishes gradient at each node in a WSN and integrates this gradient when calculating the queue backlog differential between neighbouring nodes when making back-pressure-based scheduling decision. Proved the throughput optimality of VBR. Simulation results show that VBR can significantly improve network performance in terms of packet delivery ratio, average E2E delay, and average queue length at each node as compared with existing work.

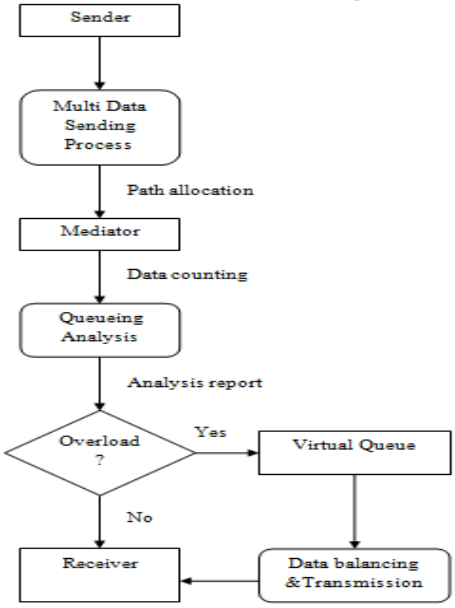

Fig no 4.1 Process Flow

5. Conclusion

A receiver-based flow control and threshold based packet-dropping policy to cope with network overload and achieve optimal utility. Our scheme is robust to uncooperative users who do not employ source-end flow control and to malicious users that intentionally overload the network.

A novel feature of our policy is a receiver-based backpressure/push-back mechanism that regulates data flows at the granularity of traffic classes, where packets can be classified based on their types. This is in contrast to source-based schemes that can only differentiate between source–destination pairs.

The receiver-based flow control scheme has a wide range of potential applications, including preventing denial-of-service attacks in Web servers, mitigating overload conditions that may arise when the network is experiencing significant degradation due to a disaster or attack, and even regulating traffic flows in the Internet. This framework also gives rise to a number of future research directions, such as accounting for the "cost" of packet dropping (e.g., due to the need to retransmit the dropped packets). A closely related problem involves the interaction between TCP-based flow control and the receiver-based flow control scheme, e.g., TCP's response to the packet-dropping mechanism.

In this context, it would also be interesting to develop a mathematical model to study optimal overload control in a network serving TCP flows. Another interesting future research direction is to use our framework to study traffic offloading problems in wire line and wireless networks, where traffic offloading is analogous to "dropping" data from the overloaded network to an alternative backup network.

References

[1] M. Chiang, S. H. Low, A. R. Calderbank, and J. C. Doyle, "Layering as optimization decomposition: A mathematical theory of network architectures,"Proc. IEEE, vol. 95, no. 1, pp. 255–312, Jan. 2007.
[2] F. P. Kelly, A. K. Maulloo, and D. K. H. Tan, "Rate control in communication networks: Shadow prices, proportional fairness and stability,"J. Oper. Res., vol. 49, pp. 237–252, 1998.
[3] F. P. Kelly, "Charging and rate control for elastic traffic," Eur. Trans. Telecommun., vol. 8, pp. 33–37, 1997.
[4] S. H. Low and D. E. Lapsley, "Optimization flow control—I: Basic algorithm and convergence," IEEE/ACM Trans. Netw., vol. 7, no. 6,pp. 861–874, Dec. 1999.
[5] A. L. Stolyar, "Maximizing queueing network utility subject to stability: Greedy primal-dual algorithm," Queueing Syst., vol. 50, no. 4,pp. 401–457, 2005.
[6] M. J. Neely, E. Modiano, and C.-P. Li, "Fairness and optimal stochastic control for heterogeneous networks," IEEE/ACM Trans. Netw., vol. 16, no. 2, pp. 396–409, Apr. 2008.
[7] A. Eryilmaz and R. Srikant, "Joint congestion control, routing, and MAC for stability and fairness in wireless networks," IEEE J. Sel.Areas Commun., vol. 24, no. 8, pp. 1514–1524, Aug. 2006.
[8] A. Eryilmaz and R. Srikant, "Fair resource allocation in wireless networks using queue-length-based scheduling and congestion control,"IEEE/ACM Trans. Net., vol. 15, no. 6, pp. 1333–1344, Dec. 2007.
[9] X. Lin and N. B. Shroff, "Joint rate control and scheduling in multihop wireless networks," in Proc. IEEE CDC, Dec. 2004, pp. 1484–1489.
[10] R. K. C. Chang, "Defending against flooding-based distributed denialof- service attacks: A tutorial," IEEE Commun. Mag., vol. 40, no. 10,pp. 42–51, Oct. 2002.
[11] A. Srivastava, B. B. Gupta, A. Tyagi, A. Sharma, and A. Mishra, "A recent survey on DDoS attacks and defense mechanisms," in Advances in Parallel Distributed Computing, ser. Communications in Computerand Information Science. Berlin, Germany: Springer, 2011, vol. 203,pp. 570–580.
[12] J. Borland, "Net video not yet ready for prime time," Feb. 1999 [Online]. Available: http://news.cnet.com/2100-1033-221271.html
[13] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network,"Comput. Commun. Rev., vol. 32, pp. 62–73, 2002.
[14] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resource allocation and cross-layer control in wireless networks," Found. Trends Netw., vol. 1,no. 1, pp. 1–144, 2006.
[15] M. J. Neely, Stochastic Network Optimization with Application to Communication and Queuing Systems. San Francisco, CA, USA:Morgan & Claypool, 2010.