



Disruption Tolerant Networking

Kevin Curran & James Knox

University of Ulster, Northern Ireland, UK

Tel: 44-2871 375565 E-mail: kj.curran@ulster.ac.uk

Abstract

Disruption Tolerant Networking (DTN) is a technology that will provide network services for environments so extreme that no end-to-end path exists through a network. Disruption Tolerant Networking hopes to tackle the problem of communicating in areas where due to various factors normal means of communication have limited success and are unreliable. DTN is aimed specifically at networks which are subject to frequent and long lasting disruptions that destroy or severely degrade normal communications. This paper provides an overview.

Keywords: Disruption tolerant networking, Computer networks, Communications, Wireless networks

1. Introduction

Delay Tolerant Networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in mobile or extreme environments that lack continuous network connectivity. In a DTN, asynchronous variable-length messages (called bundles) are routed in a store and forward manner between participating nodes over varied network transport technologies. Disruption Tolerant Networking is important due to the importance of managing network congestion. Congestion is caused by heavy traffic load which can result in long delays in data transmission due to retransmission because of data loss. Currently end to end congestion control is handled by the TCP protocol that prevents the network from collapsing but network degradation does occur when the network becomes congested. TCP/IP works well when there is no disruption to end-to-end communication. Disruption Tolerant Networking addresses weaknesses in TCP such as implementing congestion control mechanisms where each router can make decisions based on local information such as accepting a bundle of data from another router. This local information may include storage availability and the risk of accepting the data bundle based on previous experience, which may have had adverse effects on the network resulting in loss of data. This paper provides a review of Delay Tolerant Networking.

2. Delay Tolerant Networking

Disruption Tolerant Networking allows messages to pass through the network with successive responsibilities, rather than the traditional end-to-end acknowledgement scheme (Riehn, 2004). The main thrust behind Disruption Tolerant Networking is survivability and resilience. The aim is to have a network that will work in environments where continuous end-to-end connectivity cannot be assumed. This could be due to environmental factors, underwater, in desert conditions, deep space, or during warfare. There are many benefits in such a system for example, in places that suffer from disaster or where normal communications are destroyed (Grover and Tipper, 2005).

One of the problems with TCP is that it has a short time-out counter, therefore if no data is sent within a short period the circuit is shut down. This makes it unsuitable as a protocol in deep space as end-to-end connectivity would not be possible. Disruption Tolerant Networking is better suited as it is delay tolerant. Disruption Tolerant networking organises information flow into bundles. Messages pass through networks with successive responsibility unlike the current TCP structure that uses end to end acknowledgements. Intelligence is moved into the network to allow each network to make best choice on delivery of bundles via the optimal path.

Flow control is used to ensure that the destination can handle all incoming data. Congestion control is used when buffers in routers are under pressure due to the limitations of the buffer size. It limits the data loss within a network by inducing flow control which is automatically triggered when there is a difference in the arrival rate and transmission rate of data within the network. When the rates differ TCP will send an acknowledgement to the source which will reduce the transmission rate until transmission rate is equal to the arrival rate. This works well for the internet with end to end connectivity however where end to end connectivity cannot be guaranteed due to external factors this causes problems as automatic flow control and congestion control cannot work under the same set of rules. Unreliable connections make it difficult to ascertain when action is required to limit flow control or when to initialise congestion control (Grover and Tipper, 2005). The only way around this problem with DTN is to initiate congestion control by disregarding bundles due to resource depletion and returning bundles if, the management of local buffer space is under

threat. In this case bundles would be returned to their destination address until the problem was rectified. The management of this system would require the sending application to issue differing TTLs with every bundle being sent depending on their importance and the conveyance of this bundle would be on the basis of the time to live being met. The downside of this would be to accept all bundles with a large TTL; however this has the disadvantage of depleting router buffer space for a long time and all the inherent problems this brings with it.

To help reduce the problems with TTLs and bundles being dropped, DTN implements a custodial transfer system to allocate preference to certain types of bundles that meet certain criteria, allowing for a more efficient system with the conveyance of high priority bundles at the expense of others. As high priority bundles would be forwarded faster than lower priority bundles it would mean that they would have a far better chance of reaching their destination before being timed out, this means that end to end latency would be lower allowing the added benefit of reducing the TTL at every point on the path and therefore increasing the delivery time, and reducing congestion. If a bundle meets the requirements of the congestion control algorithm which is applied to all bundles and if the inbound bundle is flagged for custody transfer then a custody acceptance message is sent back to the current custodian. This causes the bundle to be removed from the custodian's buffer freeing up buffer space and relieving congestion control (see Figure 1).

If a custody transfer bundle is refused then a custody refusal message is sent back to the current custodian along the original sender route, this retriggers the resending of the bundle usually via a different route. At the same time, the absence of a custodial acceptance message triggers congestion control. Here congestion pressure at the current custodian remains unrelieved because the custodial bundle remains in the custodian's buffers, causing net space to increase over time (Burleigh et al., 2004). The problem with this is how one decides on the custodial timeout because unlike TCP/IP that has an end to end connection it is far harder to gauge the time of a round trip using the custodian method. However the benefit of the DTN based network systems is that unlike the protocol TCP/IP which requires a continuous end to end connection in order to work, the Custodial transfer system allows for breaks to occur in the connection of the end to end path which will not affect the data transmission as illustrated in Figure 2.

For example, if node A was trying to communicate with node E through nodes B, C and D then with the TCP/IP protocol this would not be possible as there is no continuous connection. However with DTN node C acts like a waterwheel first scooping the data from node B then releasing it to node D. This allows for there to be a break in connection between nodes C and D while the connection between B & C is open. Therefore it allows connections to be maintained even though connections to B & C and C & D were not opened concurrently. Thus the network integrity is maintained for bundle transfer to take place without the need for continuous end to end connection.

3. Conclusion

DTN based network systems are ideal for Interplanetary Networks which allow for long-haul communication capabilities where a continuous end to end link is not sustainable. Other places where DTN can be used include spacecraft, military/tactical, some forms of disaster response, underwater, and some form of ad-hoc sensor/actuator networks (Akyildiz, 2003). It may also include Internet connectivity in places where performance may suffer such as developing parts of the world.

References

- Akyildiz, I., Akan, O., Chen, C., Fang, J., and Su, W. (2003). InterPlanetary Internet: State-of-the-Art and Research Challenges, *Computer Networks Journal*, Vol. 43, Issue 2, pp. 75-113, October 2003.
- Riehn, M. (2004). Disruption Tolerant Networking. Available at: <http://www.darpa.mil/sto/solicitations/DTN/proposers.htm> Accessed [10th March 2007].
- Burleigh, S., Jennings, E. and Schoolcraft, J. (2007) Autonomous Congestion Control in Delay-Tolerant Networks, American Institute of Aeronautics and Astronautics. http://pdf.aiaa.org/preview/CDReadyMSPOPS06_1317/PV2006_5970.pdf [15th March 2007].
- Grover, W. and Tipper, D. (2005). Design and Operation of Survivable Networks, *Journal of Network and Systems Management, Special Issue on Designing and Managing Networks and Service Reliability*, Vol. 13, No. 1, pp. 7-13.

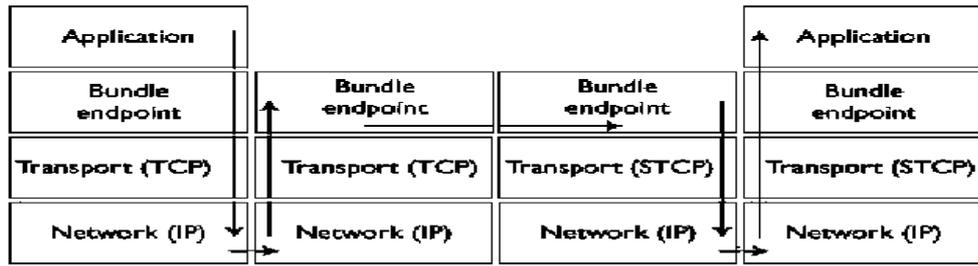


Figure 1. High priority

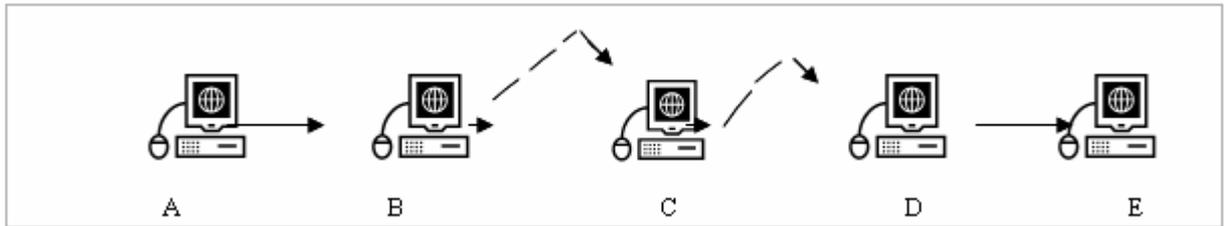


Figure 2. Custodial Transfer System