Retrospective on “A Delay-Tolerant Network Architecture for Challenged Internets”

Kevin Fall
Roland Computing Services
kfall@acm.org

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article’s technical content. Comments can be posted through CCR Online.

ABSTRACT

This article provides a brief retrospective on the evolution of Delay Tolerant Networking since 2003.

CCS CONCEPTS

• **Networks → Network architectures**;

KEYWORDS

Delay Tolerant Networking, Disruption Tolerant Networking, DTN

1 INTRODUCTION

The 2003 DTN paper, *A Delay-Tolerant Network Architecture for Challenged Internets* [5], laid out architectural concerns and a design for networks that may lack the low latency performance we are accustomed to in the Internet. A retrospective examined the applicability of the architecture and some remaining issues [6]. Applicable to a wide range of operating environments, including those with poor terrestrial infrastructure, the architecture tried to make very few assumptions on what capabilities underlying networks could provide. Essentially any forward progress in moving data, acknowledged or not, would be considered useful. Given such a wide range of network types that DTN might be applied to, among the early design decisions was to decouple the routing functions (path selection, but also per-hop sending time, message size and protocol/coding selection) from the end-to-end data encapsulation and transport concerns. Significant innovation and exploration were anticipated in the area of routing, and indeed this has been fulfilled.

2 THE EVOLUTION OF DELAY TOLERANT NETWORKING

Work in DTN routing has evolved by exploring several axes, and performance has been assessed using a variety of metrics [8]. First, the degree of knowledge regarding the future topology changes affects the types of routing and forwarding strategies employed. Adopting the terminology of *contacts* to indicate a communication opportunity, when the pattern of future contacts is known, one can pre-compute the paths to be taken, time to transmit and the amount of data to be transferred. This approach is being used with space networks [1], where planetary and orbital dynamics are used to determine the timing and capacity of contacts. At the other extreme, reduced availability of knowledge can lead to variants of MANET-style routing protocols employing non-packet-conserving approaches that allow for controlled flooding and epidemic routing, sometimes combined with techniques such as erasure coding [10].

In addition to topology knowledge, past routing and delivery performance has also been used to predict the potential benefit of forwarding a message to a particular next hop. This has been expressed with utility functions based on history and time, as well as models based on knowledge of the mobility patterns of the nodes tasked with carrying or forwarding in-transit data [2]. Several efforts [15] focus specifically on humans as data carriers and the knowledge of social interaction patterns are used to predict the chance of an end-to-end path over time being achieved.

Other opportunities arise when topologies may be modified to improve routing efficiency. This occurs, for example, when mobile nodes (e.g., drones) can be maneuvered or placed into particular positions to enhance the desired connectivity [3]. An additional variant combines controllable nodes with non-controllable nodes and helps decide which paths are best selected given the hybrid fabric. This may occur in cases of vehicular ad-hoc networks augmented by roadside storage nodes [11]. In some cases, path selection may be based on criteria other than connectivity. For example, a path with reliable storage (what DTN would call a possible ‘custodian’) that could reliably buffer an important message for some period of time might be preferred over a shorter but less reliable or more congested path [14].

While the high level of activity in DTN routing research appears to have diminished since about 2012, there are other issues that have received attention somewhat more recently. Security had been under consideration throughout the entire design [12], but detailed approaches for it were defined later. There are particular challenges in networks where reliable access to a PKI, or CRLs cannot be expected or when time cannot be synchronized [4]. Related, performing integrity checks (e.g., along the delivery path) can be frustrated in cases where connectivity interruption limits the ability to have sufficient data to verify message signatures and hashes. Identity based encryption techniques may provide some degree of enhanced convenience for intermittently-connected DTNs, but there are a variety of tradeoffs and concerns regarding resistance to quantum computing attacks (as with other approaches). More recently, puncturable encryption has been proposed to address forward secrecy in the context of store and forward message networks and DTNs [13].

It’s worth noting that the DTN protocols are on a path to standardization some 16 years after their discussion with the research community [9]. Standardization through official standards defining organizations such as IETF and CCSDS [7] is not a rapid or simple process. This has been especially true of an entirely different architecture and protocol set than that used with the Internet. Fortunately, multiple generations of researchers, developers, and operators have continued to apply their energy to moving forward on making these capabilities available to users. Many of the initial tests and deployments have been in the aerospace industry, but as the desire to attach VANETs and IoT and other limited-capability devices to the Internet appears to be growing, DTN-like capabilities (e.g., when conventional connectivity is unavailable) appears to remain a compelling fallback capability for important distributed applications.

REFERENCES

[1] Giuseppe Araniti, Nikolaos Bezirgiannidis, Edward Birrane, Igor Bisio, Scott Burleigh, Carlo Caini, Marius Feldmann, Mario Marchese, John Segui, and Kiyohisa Suzuki. 2015. Contact graph routing in DTN space networks: overview, enhancements and performance. *IEEE Communications Magazine* 53, 3 (2015), 38–46.

[2] Aruna Balasubramanian, Brian Levine, and Arun Venkataramani. 2007. DTN routing as a resource allocation problem. *ACM SIGCOMM Computer Communication Review* 37, 4 (2007), 373–384.

[3] Cintia Barroca, António Grilo, and Paulo Rogério Pereira. 2018. Improving Message Delivery in UAV-based Delay Tolerant Networks. In *2018 16th International Conference on Intelligent Transportation Systems Telecommunications (ITST)*. IEEE, 1–7.

[4] Chris Djamaludin, Ernest Foo, S Camtepe, and Peter Corke. 2016. Revocation and update of trust in autonomous delay tolerant networks. *Computers & Security* 60 (2016), 15–36.

[5] Kevin Fall. 2003. A delay-tolerant network architecture for challenged internets. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. ACM, 27–34.

[6] Kevin Fall and Stephen Farrell. 2008. DTN: an architectural retrospective. *IEEE Journal on Selected areas in communications* 26, 5 (2008), 828–836.

[7] The Consultative Committee for Space Data Systems. 2015. CCSDS Bundle Protocol Specification. (Sept. 2015). , Recommended Standard 734.2-B-1, Blue book.

[8] Samo Grasic and Anders Lindgren. 2012. An analysis of evaluation practices for dtn routing protocols. In *Proceedings of the seventh ACM international workshop on Challenged networks*. ACM, 57–64.

[9] IETF. 2019. Delay/Disruption Tolerant Networking (dtn). (2019). https://datatracker.ietf.org/wg/dtn/about/.

[10] Sushant Jain, Michael Demmer, Rabin Patra, and Kevin Fall. 2005. Using redundancy to cope with failures in a delay tolerant network. *ACM SIGCOMM Computer Communication Review* 35, 4 (2005), 109–120.

[11] Hyunwoo Kang, Syed Hassan Ahmed, Dongkyun Kim, and Yun-Su Chung. 2015. Routing protocols for vehicular delay tolerant networks: a survey. *International Journal of Distributed Sensor Networks* 11, 3 (2015), 325027.

[12] Aniket Kate, Gregory M Zaverucha, and Urs Hengartner. 2007. Anonymity and security in delay tolerant networks. In *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*. IEEE, 504–513.

[13] Signe Rüsch, Dominik Schürmann, Rüdiger Kapitza, and Lars Wolf. 2017. Forward secure delay-tolerant networking. In *Proceedings of the 12th Workshop on Challenged Networks*. ACM, 7–12.

[14] Matthew Seligman, Kevin Fall, and Padma Mundur. 2007. Storage routing for DTN congestion control. *Wireless communications and mobile computing* 7, 10 (2007), 1183–1196.

[15] Ying Zhu, Bin Xu, Xinghua Shi, and Yu Wang. 2012. A survey of social-based routing in delay tolerant networks: Positive and negative social effects. *IEEE Communications Surveys & Tutorials* 15, 1 (2012), 387–401.