Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

School of Computer Science and Statistics

Modern Delay-Tolerant Email

Rakesh Lakshmanan

Stephen Farrell
November 24, 2025

Submitted in partial fulfilment of the requirements for the degree of
M.Sc. Computer Science - Future Networked Systems

Abstract

Abstract content

Acknowledgements

I would like to thank my supervisor, Professor Stephen Farrell. Under his supervision, I was able to successfully complete this dissertation. His inspiration and suggestions regarding the project's direction were essential for the progress of this research.

I am also grateful to my family and friends for their support and encouragement throughout this process.

Contents

List of Figures

List of Tables

1 Introduction

Introduction

2 Literature Review

2.1 Introduction

Delay/Disruption-Tolerant Networking (DTN) and Internet email are both store-and-forward communication systems that enable asynchronous message delivery across heterogeneous networks (1, 2). DTN generalizes the store-and-forward concept as a network-layer or overlay architecture for challenged environments, whereas email is a specific application-layer service built on top of relatively well-connected IP networks.(1, 2)

2.2 Delay/Disruption-Tolerant Networking

2.2.1 Concept and Motivation

DTN targets “challenged” networking environments characterized by intermittent connectivity, long or variable delays, high error rates, and constrained resources such as power and storage.(1, 3) In such environments, classical TCP/IP assumptions about continuous end-to-end paths and low round-trip time do not hold, which requires a different architectural approach.(1)

Typical DTN scenarios include deep-space communication, rural and remote connectivity, ad hoc vehicular and mobile networks, and disaster-response deployments where infrastructure is damaged or overloaded.(1, 3) The primary objective is to provide eventual data delivery despite disruptions, using persistent storage and opportunistic forwarding across time-varying connectivity graphs.(1, 4)

2.2.2 DTN Architecture and Bundle Layer

The canonical DTN architecture introduces a new overlay protocol layer, commonly called the bundle layer, which resides above region-specific transports (e.g., TCP, UDP, Licklider Transmission Protocol) and below applications.(1, 3) Applications generate protocol data units called bundles, which encapsulate payload data together with endpoint identifiers, lifetime, priority, and optional security blocks.(1, 5)

Each DTN node maintains persistent storage for bundles and performs a store-carry-forward operation: bundles are stored locally, carried while the node is mobile or idle, and forwarded when a suitable contact becomes available.(1, 6) Convergence-layer adapters map bundle operations onto specific underlying transports (for example, the DTN TCP Convergence-Layer Protocol) so that the bundle layer is insulated from link heterogeneity.(5)

2.2.3 DTN Nodes, Regions, and Security

The architecture partitions the overall system into regions, such as terrestrial IP networks, satellite segments, and deep-space links, which may employ different lower-layer protocols and routing schemes.(3) The bundle layer provides interoperability across these regions using endpoint identifiers and late binding, allowing applications to communicate without being aware of underlying heterogeneity.(3, 6)

Security is addressed using dedicated bundle security mechanisms that provide authentication, integrity protection, and confidentiality over multi-hop, disruption-prone paths.(3) Because DTN nodes may store data for long periods and may replicate messages to improve delivery probability, the security design also considers access control, resistance to resource exhaustion, and key management across regions.(4, 6)

2.2.4 Routing, Scheduling, and Buffer Management

Routing in DTNs differs fundamentally from traditional IP routing because an end-to-end path between source and destination may not exist at any given time.(4, 6) Instead, routing algorithms operate over time-varying or probabilistic contact graphs, taking into account predicted or observed node mobility and contact opportunities.(6)

Existing DTN routing schemes can be broadly classified by the degree of replication and the information they exploit: epidemic and multi-copy protocols maximize delivery probability at the cost of bandwidth and buffer usage, while single-copy or quota-based schemes trade delivery ratio for reduced overhead.(4, 6) Since contacts are intermittent and buffers are limited, joint scheduling and buffer management policies are required to decide which bundles to transmit or drop according to priorities, deadlines, and resource constraints.(6)

2.3 Internet Email Architecture

2.3.1 Service Model and Roles

Internet email is an asynchronous application-layer service that delivers messages between users identified by email addresses of the form `local-part@domain`.(2, 7) The system is decomposed into functional roles including Message User Agents (MUAs), Message Submission Agents (MSAs), Message Transfer Agents (MTAs), Message Delivery Agents (MDAs), and Mail Access Agents.(2)

MUAs (such as desktop clients or webmail front-ends) are responsible for message composition, display, and user interaction, but they offload submission, relay, and storage to server-side agents.(2) MSAs accept messages from MUAs, apply initial checks, and hand them to MTAs, which relay messages between domains until they reach an MDA that deposits them into per-user mailboxes.(2, 7)

2.3.2 Protocol Suite: SMTP, POP, IMAP, MIME

The Simple Mail Transfer Protocol (SMTP) defines the submission and relay of messages between MSAs and MTAs, including envelope commands and response codes for reliable transfer (7). Originally designed for clear text operation and implicit trust between servers, SMTP has been extended with authentication and encryption mechanisms such as SMTP AUTH and STARTTLS.(7)

For mailbox access, the Post Office Protocol version 3 (POP3) supports simple download-and-delete retrieval, while the Internet Message Access Protocol (IMAP) offers folder hierarchies, server-side search, and synchronization across multiple clients and devices.(8) At the message format level, the Internet Message Format standard and Multipurpose Internet Mail Extensions (MIME) specify headers, structure, multiple body parts, and attachments, enabling rich content and internationalization.(9)

2.3.3 Security and Anti-Abuse Mechanisms

Traditional email architecture did not include end-to-end confidentiality, strong sender authentication, or robust abuse controls, making it vulnerable to spoofing, spam, and phishing (2). In practice, deployments mitigate these weaknesses by combining transport-layer security (TLS), server and user authentication, and extensive content-based filtering, often using machine learning to classify spam and malicious messages.(2, 10)

Domain-level authentication and policy mechanisms such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and DMARC enable domains to assert which hosts may send mail on their behalf and to specify handling rules for authentication failures.(2) Additional secure application architectures have been proposed that overlay existing email infrastructure with stronger identity, integrity, and legal guarantees, while preserving compatibility with standard protocols.(10)

2.4 Comparison of DTN and Email Architectures

Both DTN and Internet email rely on asynchronous, store-and-forward operation, with intermediate nodes temporarily buffering data before forwarding it to the destination.(1, 2) However, DTN is conceived as a general-purpose network-layer architecture for environments with extreme delay and disruption, while email is a specific application protocol suite designed for relatively stable IP networks (1, 7).

DTN introduces a unified bundle layer to integrate heterogeneous underlying networks and explicitly models time-varying connectivity and contact opportunities (1, 3). On the contrary, the email architecture builds on existing IP transport and focuses on application-level roles, standardized message formats, and security mechanisms for addressing and content-level

3 System Design

System design content

4 | Implementation

Implementation content

5 Results and Discussion

Results

6 | Conclusions and Future Work

Conclusions

Bibliography

[1] Kevin Fall. A delay-tolerant network architecture for challenged internets. In *ACM SIGCOMM*, 2003.

[2] Dave Crocker. Internet mail architecture. *RFC 5598*, 2009.

[3] Vinton G. Cerf, Scott C. Burleigh, Adrian J. Hooke, et al. Delay-tolerant networking architecture. *RFC 4838*, 2007.

[4] Aruna Balasubramanian, Brian N. Levine, and Arun Venkataramani. Dtn routing as a resource allocation problem. *ACM SIGCOMM Computer Communication Review*, 2007.

[5] Scott Burleigh et al. Delay-tolerant networking tcp convergence-layer protocol version 4. *RFC 9174*, 2022.

[6] C. C. Sobin et al. A survey of routing and data dissemination in delay tolerant networks. *Ad Hoc Networks*, 2012.

[7] John C. Klensin. Simple mail transfer protocol. *RFC 5321*, 2008.

[8] Mark R. Crispin. Internet message access protocol - version 4rev1. *RFC 3501*, 2003.

[9] Pete Resnick. Internet message format. *RFC 5322*, 2008.

[10] Francesco Buccafurri et al. Secure application email architecture. In *CEUR Workshop Proceedings*, 2023.