Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Lehrstuhl für Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

WS 2009/2010

Seminar

Delay-Tolerant Networks

Volodymyr Goncharov

7. Februar 2010

Abstract

In this paper, I introduce main concepts of delay-tolerant networks and their architecture. Delay-tolerant networks are designed to operate in environments characterized by very long delay paths and frequent network partitions. In the end, I give results of performance evaluation of the DTN store-and-forward approach compared to traditional Internet data transfer protocols.
The paper does not introduce novel approaches created by the author himself but rather should be seen as a summarized review of reference papers.

Keywords: Delay-Tolerant Network, Internet Protocol Suite, Transmission Control Protocol, Internet Protocol, Data Link Layer, Bundle, Bundle Layer

Contents

1 Introduction

TCP/IP Internet works on a principle of providing end-to-end data transfer using a concatenation of potentially dissimilar link-layer technologies. A bunch of data link layer protocols are standardized and worked well on the globe. However, there are many environments where internet assumptions do not hold. Once there is no end-to-end path between source and destination for the duration of a communication session or communication is unreliable and might only exist for short periods of time, a TCP/IP network starts to work inappropriately or even stops to work at all. A good example of such environment is the ”Interplanetary Internet”. The speed-of-light delay from Earth to Mars, for example, is approximately 4 minutes when Earth and Mars are at their closest approach. The one-way light time can exceed 20 minutes when Earth and Mars are in opposition. The speed-of-light delay to the outer planets becomes significantly higher [4]. If one wants to send a file from a base station on Earth to a satellite flying around Mars, it might take about one hour just to initiate the file transfer. File Transfer Protocol requires authorization and authentication commands to be sent before the data transfer starts, TCP uses handshaking mechanism and sends three packets for each FTP command. Considering that round trip of a TCP packet takes at minimum 8 minutes, it becomes clear why one should wait long until the data transfer is initialized.

Delay-tolerant networks (DTN) have been designed to operate in environments where Internet Protocol Suite does not seem to work well. Delay-tolerant networks use a message-oriented overlay that supports intermittent connectivity, overcomes communication disruptions and delays. Transmission of data between source and destination nonexistent for the time of a communication is also allowed. All aforementioned features are achieved by using store-and-forward message method. Services the method provides are very similar to electronic mail, but with improved naming, routing and security capabilities.

2 Challenged networks

Before starting with the concept of delay tolerant networks I would like to introduce examples of so called challenged networks. Challenged networks may violate one or more of the Internet's assumptions and therefore the TCP/IP model is not appropriate for such networks.
According to [2], examples of challenged networks are:

- **Terrestrial Mobile Networks**. Since nodes in such networks are usually vehicles or other moving entities, the network may easily become partitioned. RF interference might also cause network partitions. Mobile networks are characterized by intermittent connectivity and utilize both opportunistic and scheduled contacts.
- **Exotic Media Networks**. These networks are designed to operate in environments with very long-distance links or environments that use acoustic or optical modulation. Communication participants may experience longs delays and connection interruptions. Examples are communication with submarines or low-earth orbiting satellites, deep space RF communication etc.
- **Sensor-based Networks**. These networks consist of a huge number of nodes that are characterized by limited power, memory and CPU capability. Network participants communicate with each other at a scheduled time to save power.

As we can see these kinds of networks suffer from high latency, frequent disconnections, low data rate, bandwidth limitations etc. The Internet would not work well under those assumptions and therefore a model other than TCP/IP should serve challenged networks.

3 Concept

A delay-tolerant network is an overlay on top of existing regional networks. The overlay is called the bundle layer and is intended to operate above the existing protocol stacks in various network architectures and provide a gateway function between them when a node physically touches two or more dissimilar networks [2]. Flexibility and scalability are advantages of using the introduced approach. For example, one may easily link already existing TCP/IP networks with networks that will appear in the future for deep space communication purposes and will probably use their own transport, network and physical layers. A bundle-layer protocol is used overall across the network.
The figure below shows the place of the bundle-layer in a stack of layers:

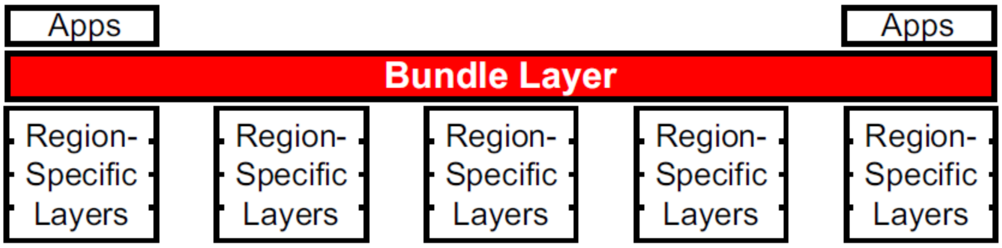

Figure 1 – Bundle-layer in a stack of layers [1]

Bundles are also called messages. Reliable transfer of data is achieved by storing and forwarding entire bundles between nodes that are on the way to a receiver. Besides node-to-node bundle retransmission, custody transfers are done. Custodian node stores a bundle until it is successfully transferred to the next successive node and the next-hope bundle layer accepts custody. In case no another node accepts custody and the bundle's time-to-live expires, the bundle is removed.
Although store-and-forward mechanism is used, custody transfers do not provide guaranteed end-to-end reliability. This can only be attained if a source node keeps a copy of a bundle until getting a return receipt from the receiver, and it will resend the bundle if it does not receive the acknowledgement.

4 Endpoints and types of nodes

A node is an engine for sending and receiving bundles or a communication entity, in whose stack the bundle layer is implemented. According to the RFC 4838 [5], there might be three different types of nodes: host, router and gateway. Nodes may act as source, destination, forwarder (or some combination) depending on the structure of a network.

- **Host** is responsible for sending or/and receiving bundles, but not forwarding them, and therefore may only be a source or destination of a bundle transfer. Since DTN utilize message-oriented approach, nodes should have sufficient persistent storage capacity to queue bundles if the outbound links are not accessible and keep them until links are available again.
- **Router** works within a single DTN region and is responsible for forwarding bundles. Such nodes require persistent storage to queue and keep bundles until outbound

[1] The illustration was taken from [6]

links are available. Routers may optionally work as hosts. They connect neighboring networks that communicate on the same transport, network and physical layers.

- **Gateway** is designed to forward bundles between two or more DTN region networks and may optionally act as a host. The bundle overlay of gateways must have persistent storage and allow custody transfers. Gateways link together networks that operate on different lower-layer protocols.

Both host and router nodes might support custody transfers.
Applications use nodes to send or receive bundles (or messages). Messages are delivered to endpoints that include one or many DTN nodes. A message is deemed to have been successfully delivered when a minimum subset of the nodes in the destination endpoint has received the bundle without errors. The subset is sometimes also called ”minimum reception group” (MRG). RFC 4838 [5] introduced three different types of subsets the nodes may refer to. MRG of an endpoint may consist of only one node (unicast), one of a group of nodes (anycast) or all of a group of nodes (multicast and broadcast). The difference between anycast and multicast is that a message sent to an anycast group should be delivered at least to one node out of the group and not necessarily to all nodes. In case of a multicast message, all nodes in the group must receive a message until it is considered to be successfully delivered. Multicast is a particular case of broadcast. Broadcast is a transmission to all participants of a network and multicast is a transmission to a chosen set of participants only.
A single node may be a part of several endpoints at the same time.

5 Names, addresses and routing

Since delay tolerant networks were designed to couple different networks or regions, it is necessary to have an appropriate mechanism to distinguish regions and single nodes in the regions. For example, these regions might be the Earth’s Internet, a sensor network on the Moon or a military network. According to [5] and [6], a good solution exists using URI format to identify coupled networks. Uniform Resource Identifier or URI is also used to identify endpoints of DTN. URI starts with a scheme name which is maintained by IANA organization. The remaining portion of the URI consists of series of characters and delimiters specified by the syntax, thereby uniquely identifying each endpoint in a network. More detailed information about the syntax and scheme names can be found in the paper [1].
Endpoint Identifier (EID) is a specifically constructed URI which consists of region and

entity ids. Region ids use the same name-space notation as Domain Name System protocol and therefore should be named in the understandable by human beings way. This significantly helps in tracking and monitoring traffic. Good identifiers of regions could be *earth.sol.int*, *mars.sol.int* or *saturn.sol.int* where the first part refers to the planet's name, the second stands for Solar System and the third shows the communication takes place between the planets. Entity ids uniquely describe DTN nodes within a region. At least one unique endpoint identifier must be assigned to each DTN node. Since gateways usually connect two or more regions, they have might have several EIDs. Other regular nodes within a region might also have multiple EIDs.
The figure below shows how region and entity identifiers might be assigned:

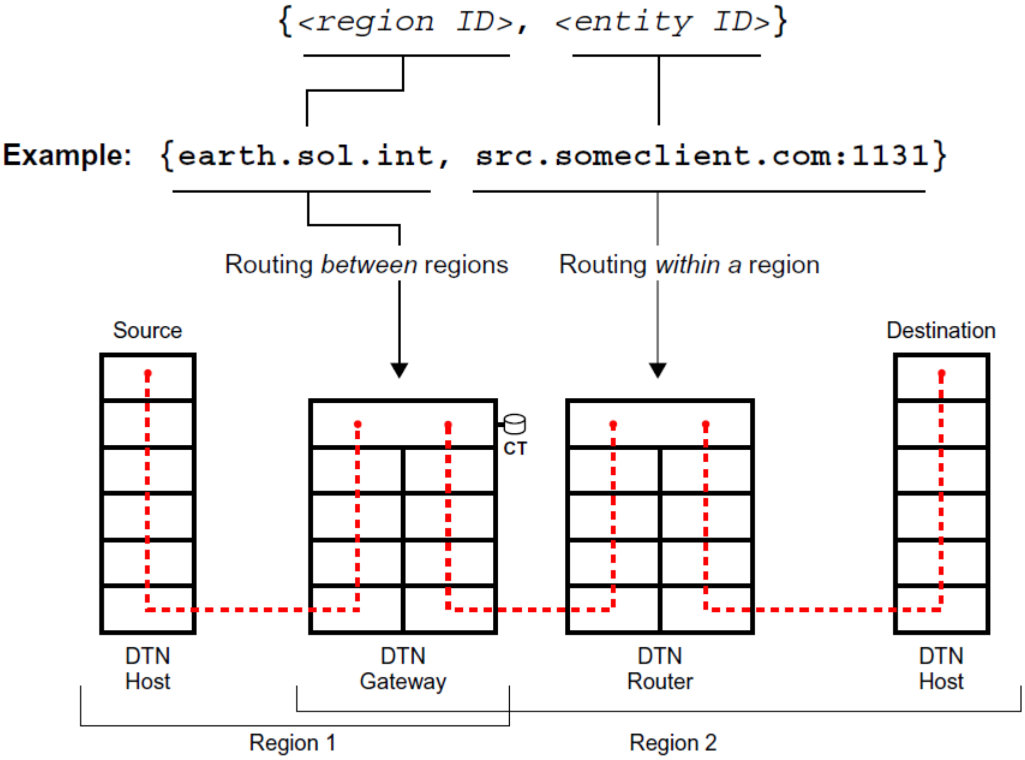
{<region ID>, <entity ID>}
Example: {earth.sol.int, src.someclient.com:1131}
Routing *between* regions
Routing *within a* region
Source
Destination
CT
DTN Host
DTN Gateway
DTN Router
DTN Host
Region 1
Region 2

Figure 1 – Region and entity identifiers [2]

The above mentioned way of node addressing simplifies routing between regions. One can easily recognize the destination region of a packet by only taking a look at its region

[2] The illustration was taken from [6]

id. The routing mechanism used inside DTN depends on the network architecture and therefore might be different in networks. Routing in delay tolerant networks belongs to one of challenging research topics.

6 Security

Most security methods in Internet involve the mutual authentication and further exchange of private data between sender and receiver, leaving the network as a non-participant. This might lead to carrying traffic long distances that is later found to be prohibited. In delay tolerant networks where link capacity is a very costly resource, better security approaches should be implemented.

The security model used in DTN differs from the traditional security model in the way it includes network routers as participants of an authentication process. To carry out the model, each message contains a ”postage stamp” keeping a verifiable identity or signature of the source node. A new identity is created every time the message arrives to a routing node and later is verified on the next consecutive node on the way to a destination.

Below I introduce steps that are usually done to ensure authentication in delay tolerant networks:

- The source node generates its own bundle-specific signature, attaches it to the bundle and sends it to a nearest adjacent node. If the adjacent node does not have a copy of the sender’s public certificate, it gets one either from the sender or a Certificate Authority (CA).
- The forwarding node receives the bundle and verifies the identity field. If the verification fails, the DTN node rejects the bundle. If not, the forwarding node replaces the sender’s signature with its own signature and sends the bundle to the next consecutive forwarder or to a destination node.
- Each subsequent node on the way to a destination verifies only the identification of the previous forwarding node. Then it updates the bundle with its own signature and forwards it.

The described security model identifies and prevents denial-of-service attacks on the very first forwarding node messages are sent to. It has the big benefit as compared with Internet routers.

7 Reducing traffic when using DTN

In this short chapter I want to explain how delay tolerant networks might reduce traffic. In the introduction part we have already seen that the major Internet's transport protocol does not profit in environments with long or variable delays. But not only three way handshaking decreases network traffic.
TCP belongs to reliable transport protocols what means it guaranties consecutive and error-free transmission of packets. It fills the CRC field every time before sending a packet and then checks it on the receiver. If an error occurs then the sender retransmits the packet to the destination point. DTN networks also support retransmission in case of mistakes but as opposite to TCP/IP networks they don't increase network traffic much. This is done by means of store-and-forward approach. In delay tolerant networks retransmissions are performed between neighboring nodes. It is quite obvious that hope-by-hope retransmissions require less time and traffic then end-to-end ones.

8 Evaluation of Delay Tolerant Networking

In the paper [3] authors created a DTN network and then evaluated their implementation. They configured five nodes in a linear topology and ran a set of tests upon them. They tested end-to-end and hop-by-hop configurations of DTN, Mail and SFTP protocols. The end-to-end configuration excluded intermediate storing of a bundle while forwarding it to the destination through all routers. The hop-by-hop approach utilizes custodian transfers and therefore is more appropriate in case of often disconnections and network partitions.
First authors analyzed the bandwidth utilization with no disconnections and both end-to-end and hop-by-hop configurations showed almost the same results. Mail protocol as opposed to DTN had a bit higher per-message header overhead. Then they introduced periodic disconnectivity to each node of the network and ran tests again where disruptions were aligned, shifted, sequential and random. The results were more interesting: Mail, DTN and SFTP of the end-to-end configuration showed very low channel utilization. Due to periodic disruptions, a connection between the source and destination nodes could not be established for the time data is completely sent to the destination. The hop-by-hop Mail and DTN protocols showed very close results. Obviously one would ask why we should reinvent the wheel when the old protocol works as well as the new one. The next test authors performed is about to answer the question.
The experiment was based on network disruptions and enabled reactive fragmentation feature of DTN. As the test showed, DTN was able to deliver one extra message in every

cycle and stayed therefore ahead of sendmail. The reactive fragmentation makes the DTN protocol better than its store-and-forward TCP/IP analogues.

9 Conclusion

The DTN architecture was designed to provide communications between networks that are characterized by long delays and discontinuous end-to-end connectivity. It supports different types of connectivity, including scheduled, predicted and opportunistically connected networks. The store-and-forward approach introduced in DTN is not novel and is widely used in the protocol sendmail. Asynchronous messaging, enhanced security against unauthorized access and reactive fragmentation – these are the features that make DTN an interesting subject to further research.
I, as creators and contributors of the DTN architecture, believe this architecture has future and should be investigated more so that delay tolerant networks can fully utilize it.

References

[1] Berners-Lee T., Fielding R., Masinter L. Uniform Resource Identifier (URI): Generic Syntax. RFC 3986. 2005.

[2] Kevin Fall. A Delay-Tolerant Network Architecture for Challenged Internets. 2003.

[3] Michael Demmer, Eric Brewer, Kevin Fall, Sushant Jain, Melissa Ho, Robin Patra. Implementing Delay Tolerant Networking. 2004.

[4] Robert C. Durst, Patrick D. Feighery, Keith L. Scott. Why not use the Standard Internet Suite for the Interplanetary Internet?

[5] Vinton Cerf, Scott Burleigh, Adrian Hooke, Leigh Torgerson, Robert Durst, Keith Scott, Kevin Fall, Howard Weiss. Delay-Tolerant Network Architecture. RFC 4838. 2007.

[6] Forrest Warthman. Delay-Tolerant Networks (DTNs) - A Tutorial. 2003.