# COL334 Assignment 5
# A Delay-Tolerant Network Architecture for Challenged Internets
A Review and Summary

Jai Javeria 2018CS10340

January 15, 2021

## 1 Abstract

The paper addresses the problem and assumptions that the TCP/IP based internet service model makes, which some "challenged" network conditions might not satisfy. Some of them being

- Existence of end to end path while sending data between 2 points.
- Packet losses are low and mainly occur due to congestion.
- Maximum RTT is not excessive.
- The enpoints do not have strict power and memory constraints.

The paper gives the examples of Mobile, Interplanetary, Military and Sensor Networks where some of these assumptions are violated. In section 2, the paper discusses in detail the the characteristics of such networks where traditional protocols like TCP/IP cannot be used.
Section 3 discusses about the existent technology (at the time of the publication of the paper) that handle some of the problems with challenged networks. These were:

- Performance Enhancing Proxies (PEPs): Its use is not recommended. They change connection endpoints, violating end-to-end reliability. Mobile internets lead to increase in complexity of the whole system.
- Protocol Booster: They are not able to gain a lot of performance improvements.
- Proxies: These are application specific.
- E-Mail: It lacks dynamic routing and relies on mail relays which do not work efficiently during a network failure.

After identifying and discussing about the flaws of the available technology, the paper motivates the need for additional architecture and proposes the Delay Tolerant Networking (DTN) Architecture. The salient features of this architecture are:

- **DTN Gateway and Regions**: A network with similar protocols and address spaces is regarded as a region. A DTN Gateway is a bridge between 2 regions to ensure interoperability. It also stores packets when reliable data transfer is required.
- **Name Tuples**: Using DNS service in a delay prone network is inefficient since there would be long waiting time just for connection to start. Thus the paper suggest a new routing mechanism consisting of a name tuple {Region Name, Entity Name}. The region name is a globally unique id for identification of a region. The entity name is unique within a region and identifies nodes in it. For inter region routing, only the first part of the tuple is used.

- **Custody Transfer**: Since nodes in challenged networks might not be active till the time the sent message reliably reaches the destination, the responsibility of reliably sending the message is given to each node with memory (persistent node) on the way. When a message passes from one persistent node to the other, the new node takes the "custody" of the packet and it is now its responsibility to ensure reliability of message transfer. Thus this transfer takes place until the packet reaches its destination.
- **Security**: We would not like challenged networks to carry prohibited messages all over to the destination. Thus the paper proposes a hop by hop checking mechanism. The routers would drop illegitimate traffic whenever they find one.
- **Congestion and Flow Control**: Some mechanisms to control congestion are through rejecting incoming custody transfers when buffer is full, routing packets to sub-optimal routes because of buffer constraints and dropping non custody messages in favour of those requiring custody.

# 2 Advantages

- The mechanism presented in the paper is a generalized overlay architecture which can work with any underlying protocol stack.
- The paper recognises the heterogeneity of different regions and provides a way for communication to happen across all these networks. The architecture proposed is also compatible with the TCP/IP based internet.
- The paper successfully addresses the drawback of end to end reliability and security in challenged networks with hop by hop versions.

# 3 Limitations

- The paper does not talk about rural area networks as a use case of the above architecture. Thus the paper did not discuss the use of a mix of name tuple and DNS service for routing. This can arise when a rural user wants to connect to, say www.cse.iitd.ac.in. One way to resolve this is to defer the DNS name resolution to the DTN gateway and let the end user only be worried to approach the gateway.
- The paper does not discuss about how the congestion notifications would be sent in a delay and disconnection aware way. Sending the data to a router only to figure out that the router cannot take the custody of the packet is wastage of precious bandwidth.
- The paper does not talk about transfer of custody in cases where the next hop does not have the capability to take custody i.e. cannot store message (non-persistent). One trivial way is for every persistent node to calculate its nearest persistent neighbours and open connections directly to them, via the non persistent hops.
- The paper assumes that entity and region name resolutions can happen automatically without a DNS service. This may not always we true. Say a user wants to connect to www.cse.iitd.ac.in and say the entity name is the same as the URL but how does the user find the region name.

# 4 Relevance in Present Day

With the pandemic, most of our day to day essential activities like classes have move online, thus making the internet a necessity and a right rather than a luxury. Thus it becomes extremely important that we are able to connect each and everyone to it. Many people still have less connectivity in their place of residence, so using such an architecture is essential for democratizing the access to the internet.
The same paper, if written today would definitely look it from the "internet for all" perspective and include a lot of insights particular to connecting remote areas like villages.