Making “Custody Transfer” historic

Rick Taylor, Aalyria

Introduction

“Custody Transfer” is a concept that has been around since the dawn of DTN research. It is often seen as a panacea for reliability, but it has been under-specified, and many assumptions of effectiveness have been attached to it.

Achieving end-to-end reliability for bundle transfers is a vital capability required by DTNs, but I believe the ‘folklore’ around Custody Transfer is holding us back.

A bit of history

Custody Transfer was a mechanism described in Bundle Protocol version 6, designed to provide some delivery reliability across a DTN, by answering the question:

“Who has the bundle, so I can drop my copy?”

Nodes would acknowledge custody of a bundle, hop-by-hop, ensuring retransmission by the sender did not need to occur.

But the signalling was considered inefficient, the semantics a bit loose, and it was therefore not included in the core BPv7 spec (RFC9171).

The good bit...

The worst performing reliability mechanism for a DTN is anything that requires the bundle *source* to repeatedly retransmit an entire bundle, when it is believed that it has been lost somewhere along the path.

✅ Custody Transfer seems to address this

If a node (A) doesn't drop its copy of a bundle until another node (B) says it has it, then retransmission only needs to occur between A and B.

The bad bit...

It’s not enough - it doesn’t really prevent bundle loss 😞

Just because at time *T0* a node takes custody of a bundle, it doesn’t guarantee that it won’t get dropped before its next transmission opportunity at *T1*.

- “Rapid Unscheduled Disassembly” of platforms happens.
- High radiation environments are tough on storage.
- Queues get full.
- Etc...

And what if two nodes in a row fail?

A Proposal

We need an end-to-end reliability mechanism that minimises the retransmissions of bundles along the path from source to destination, with the following capabilities:

- The ability for a node to signal that it has safely stored the bundle, to avoid pointless retransmission.
- The ability for a node to reaffirm that it still has the bundle stored, to indicate that its previous assertion is still valid or not.
- The ability for a node to signal that it knows another node has the bundle stored, to avoid linking reliability to routing.
- The ability to piggyback the signalling on other traffic that is already flowing in the same direction, to avoid unnecessary signalling overhead.
- The ability to aggregate multiple signals into single control messages, to reduce overall control plane traffic.

Without requiring an end-to-end tunnel encapsulation.

Conclusion

What we need is something more than what we all loosely refer to as “Custody Transfer”.

So let’s stop using those words, and define a BPv7 mechanism that delivers what we need, based on the original good ideas and what we have learned since then.

Questions and Comments?